NIST Special Publication 800-60 Volume I
Revision 1

National Institute of
Standards and Technology
U.S. Department of Commerce

# Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories

**Kevin Stine**
**Rich Kissel**
**William C. Barker**
**Jim Fahlsing**
**Jessica Gulick**

INFORMATION SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

**August 2008**

**U.S. DEPARTMENT OF COMMERCE**
*Carlos M. Gutierrez, Secretary*

**NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY**
*James M. Turner, Deputy Director*

## Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the nation’s measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof-of-concept implementations, and technical analyses to advance the development and productive use of information technology. ITL’s responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. This Special Publication 800-series reports on ITL’s research, guidelines, and outreach efforts in information system security and its collaborative activities with industry, government, and academic organizations.

## Authority

This document has been developed by the National Institute of Standards and Technology (NIST) to further its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, P.L. 107-347. NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), *Securing Agency Information Systems*, as analyzed in A-130, Appendix IV: *Analysis of Key Sections*. Supplemental information is provided in A-130, Appendix III.

This guideline has been prepared for use by federal agencies. It may also be used by nongovernmental organizations on a voluntary basis and is not subject to copyright. (Attribution would be appreciated by NIST.)

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official.

NIST Special Publication 800-60 Volume I, Revision 1, 53 pages

**(Date) CODEN: NSPUE2**

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There are references in this publication to documents currently under development by NIST in accordance with responsibilities assigned to NIST under the Federal Information Security Management Act of 2002. The methodologies in this document may be used even before the completion of such companion documents. Thus, until such time as each document is completed, current requirements, guidelines, and procedures (where they exist) remain operative. For planning and transition purposes, agencies may wish to closely follow the development of these new documents by NIST. Individuals are also encouraged to review the public draft documents and offer their comments to NIST. All NIST documents mentioned in this publication, other than the ones noted above, are available at http://csrc.nist.gov/publications.

COMMENTS MAY BE SUBMITTED TO THE COMPUTER SECURITY DIVISION, INFORMATION TECHNOLOGY
LABORATORY, NIST VIA ELECTRONIC MAIL AT SEC-CERT@NIST.GOV OR VIA REGULAR MAIL AT
100 BUREAU DRIVE (MAIL STOP 8930), GAITHERSBURG, MD 20899-8930

## Acknowledgements

The authors, Kevin Stine, Rich Kissel, and William C. Barker, wish to thank their colleagues, Jim Fahlsing and Jessica Gulick from Science Applications International Corporation (SAIC), who helped update this document, prepare drafts, and review materials. In addition, special thanks are due to our reviewers, Arnold Johnson (NIST), Karen Quigg (Mitre Corporation), and Ruth Bandler (Food and Drug Administration), who greatly contributed to the document's development. A special note of thanks goes to Elizabeth Lennon for her superb technical editing and administrative support. NIST also gratefully acknowledges and appreciates the many contributions from individuals in the public and private sectors whose thoughtful and constructive comments improved the quality and usefulness of this publication.

# Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories

## Table of Contents

# EXECUTIVE SUMMARY

Title III of the E-Government Act (Public Law 107-347), titled the Federal Information Security Management Act (FISMA), tasked the National Institute of Standards and Technology (NIST) to develop:

- Standards to be used by all Federal agencies to categorize all information and information systems collected or maintained by or on behalf of each agency based on the objectives of providing appropriate levels of information security according to a range of risk levels;
- Guidelines recommending the types of information and information systems to be included in each such category; and
- Minimum information security requirements (i.e., management, operational, and technical security controls), for information and information systems in each such category.

In response to the second of these tasks, this guideline has been developed to assist Federal government agencies to categorize information and information systems. The guideline's objective is to facilitate application of appropriate levels of information security according to a range of levels of impact or consequences that might result from the unauthorized disclosure, modification, or use of the information or information system. This guideline assumes that the user is familiar with *Standards for Security Categorization of Federal Information and Information Systems* (Federal Information Processing Standard [FIPS] 199). The guideline and its appendices:

- Review the security categorization terms and definitions established by FIPS 199;
- Recommend a security categorization process;
- Describe a methodology for identifying types of Federal information and information systems;
- Suggest provisional[1] security impact levels for common information types;
- Discuss information attributes that may result in variances from the provisional impact level assignment; and
- Describe how to establish a system security categorization based on the system's use, connectivity, and aggregate information content.

This document is intended as a reference resource rather than as a tutorial and not all of the material will be relevant to all agencies. This document includes two volumes, a basic guideline and a volume of appendices. Users should review the guidelines provided in Volume I, then refer to only that specific material from the appendices that applies to their own systems and applications. The provisional impact assignments are provided in Volume II, Appendix C and D. The basis employed in this guideline for the identification of information types is the Office of

[1] Provisional security impact levels are the initial or conditional impact determinations made until all considerations are fully reviewed, analyzed, and accepted in the subsequent categorization steps by appropriate officials.

Management and Budget’s Federal Enterprise Architecture (FEA) Program Management Office (PMO) October 2007 publication, *The Consolidated Reference Model Document Version 2.3*.

# 1.0 INTRODUCTION

The identification of information processed on an information system is essential to the proper selection of security controls and ensuring the confidentiality, integrity, and availability of the system and its information. The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60 has been developed to assist Federal government agencies to categorize information and information systems.

## 1.1 Purpose and Applicability

NIST SP 800-60 addresses the FISMA direction to develop guidelines recommending the types of information and information systems to be included in each category of potential security impact. This guideline is intended to help agencies consistently map security impact levels to types of: (i) information (e.g., privacy, medical, proprietary, financial, contractor sensitive, trade secret, investigation); and (ii) information systems (e.g., mission critical, mission support, administrative). This guideline applies to all Federal information systems other than *national security systems*. *National security systems* store, process, or communicate *national security* information.[2]

## 1.2 Target Audience

This publication is intended to serve a diverse federal audience of information system and information security professionals including: (i) individuals with information system and information security management and oversight responsibilities (e.g., chief information officers, senior agency information security officers, authorizing officials); (ii) organizational officials having a vested interest in the accomplishment of organizational missions (e.g., mission and business area owners, information owners); (iii) individuals with information system development responsibilities (e.g., program and project managers, information system developers); and (iv) individuals with information security implementation and operational responsibilities (e.g., information system owners, information owners, information system security officers).

## 1.3 Relationship to Other Documents

NIST Special Publication (SP) 800-60 is a member of the NIST family of security-related publications including:

- FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems;*
- FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*;

[2] FISMA defines a *national security system* as any information system (including telecommunications system) used or operated by an agency or by a contractor on behalf of an agency, or any other organization on behalf of an agency – (i) the function, operation, or use of which: involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapon system; or is critical to the direct fulfillment of military or intelligence missions (excluding a routine administrative or business system used for applications such as payroll, finance, logistics, and personnel management); or (ii) that processes classified information. [See Public Law 107-347, Section 3542 (b)(2)(A).]

- NIST SP 800-30, *Risk Management Guide for Information Technology Systems;*[3]
- NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems;*
- NIST Draft SP 800-39, *Managing Risk from Information Systems: An Organization Perspective;*
- NIST SP 800-53, *Recommended Security Controls for Federal Information Systems;*
- NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*; and
- NIST SP 800-59, *Guideline for Identifying an Information System as a National Security System*.

This series of nine documents is intended to provide a structured, yet flexible framework for selecting, specifying, employing, evaluating, and monitoring the security controls in Federal information systems—and thus, makes a significant contribution toward satisfying the requirements of the Federal Information Security Management Act (FISMA) of 2002. While the publications are mutually reinforcing and have some dependencies, in most cases, they can be effectively used independently of one another.

The SP 800-60 information types and associated security impact levels are based on the Office of Management and Budget (OMB) Federal Enterprise Architecture Program Management Office's October 2007 *FEA Consolidated Reference Model Document*, *Version 2.3*, inputs from participants in previous NIST SP 800-60 workshops, and FIPS 199. Rationale for the example impact-level recommendations provided in the appendices has been derived from multiple sources and, as such, will require several iterations of review, comment, and subsequent modification to achieve consistency in terminology, structure, and content.

## 1.4 Organization of this Special Publication

This is Volume I of two volumes. It contains the basic guidelines for mapping types of information and information systems to security categories. The appendices, including security categorization recommendations for mission-based information types and rationale for security categorization recommendations, are published as a separate Volume II.

**Volume I** provides the following background information and mapping guidelines:

- Section 2: Provides an overview of the value of the categorization process to agency missions, security programs and overall information technology (IT) management and the publication's role in the system development lifecycle, the certification and accreditation process, and the NIST Risk Management Framework.
- Section 3: Provides the security objectives and corresponding security impact levels identified in the Federal Information Processing Standard 199, *Standards for Security Categorization of Federal Information and Information Systems* [FIPS 199];

[3] This document is currently under revision and will be reissued as Special Publication 800-30, Revision 1, *Guide for Conducting Risk Assessments*.

- Section 4: Identifies the process including guidelines for identification of *mission-based* and *management and support* information types and the process used to select security impact levels, general considerations relating to security impact assignment, guidelines for system security categorization, and considerations and guidelines for applying and interrelating system categorization results to the agency's enterprise, large supporting infrastructures, and interconnecting systems;
- Appendix A: Glossary; and
- Appendix B: References.

**Volume II** includes the following appendices:

- Appendix A: Glossary [Repeated];
- Appendix B: References [Repeated];
- Appendix C: Provisional security impact level assignments and supporting rationale for *management and support* information (administrative, management, and service information);
- Appendix D: Provisional security impact level assignments and supporting rationale for *mission-based* information (mission information and services delivery mechanisms); and
- Appendix E: Legislative and executive sources that specify sensitivity/criticality properties.

# 2.0 PUBLICATION OVERVIEW

Security categorization provides a vital step in integrating security into the government agency's business and information technology management functions and establishes the foundation for security standardization amongst their information systems. Security categorization starts with the identification of what information supports which government lines of business, as defined by the Federal Enterprise Architecture (FEA). Subsequent steps focus on the evaluation of the need for security in terms of confidentiality, integrity, and availability. The result is strong linkage between missions, information, and information systems with cost effective information security.

## 2.1 Agencies Support the Security Categorization Process

Agencies support the categorization process by establishing mission-based information types for the organization. The approach to establishing mission-based information types at an agency begins by documenting the agency's mission and business areas. In the case of mission-based information, the responsible individuals, in coordination with management, operational, enterprise architecture, and security stakeholders, should compile a comprehensive set of the agency's lines of business and mission areas. In addition, responsible individuals should identify the applicable sub-functions necessary to accomplish the organization's mission. For example, one organization's mission might be related to economic development. Sub-functions that are part of the organization's economic development mission might include business and industry development, intellectual property protection, or financial sector oversight. Each of these sub-functions represents an information type.

Agencies should conduct FIPS 199 security categorizations of their information systems as an agency-wide activity with the involvement of the senior leadership and other key officials within the organization (e.g., mission and business owners, authorizing officials, risk executive, chief information officer, senior agency information security officer, information system owners, and information owners) to ensure that each information system receives the appropriate management oversight and reflects the needs of the organization as a whole. Senior leadership oversight in the security categorization process is essential so that the next steps in the NIST Risk Management Framework[4] (e.g., security control selection) can be carried out in an effective and consistent manner throughout the agency.

## 2.2 Value to Agency Missions, Security Programs and IT Management

Federal agencies are heavily dependent upon information and information systems to successfully conduct critical missions. With an increasing reliability on and growing complexity of information systems as well as a constantly changing risk environment, information security has become a mission-essential function. This function must be conducted in a manner that reduces the risks to the information entrusted to the agency, its overall mission, and its ability to do business and to serve the American public. In the end, information security, as a function, becomes a business enabler through diligent and effective management of risk to information confidentiality, integrity, and availability.

[4] See Section 2.5, Figure 1: NIST Risk Management Framework

Therefore, the value of information security categorization is to enable agencies to proactively implement appropriate information security controls based on the assessed potential impact to information confidentiality, integrity, and availability and in turn to support their mission in a cost-effective manner. An incorrect information system impact analysis (i.e., incorrect FIPS 199 security categorization) can result in the agency either over protecting the information system thus wasting valuable security resources, or under protecting the information system and placing important operations and assets at risk. The aggregation of such mistakes at the enterprise level can further compound the problem.

In contrast, conducting FIPS 199 impact analyses as an agency-wide exercise with the participation of key officials (e.g., Chief Information Officer [CIO], Senior Agency Information Security Officer [SAISO], Authorizing Officials, Mission/System Owners) at multiple levels can enable the agency to leverage economies of scale through the effective management and implementation of security controls at the enterprise level. A resulting value of consistently implementing this systematic process for determining the security categorization and the application of appropriate security protection is an improved overall understanding of the agency's mission, business processes, and information and system ownership.

*Implementation Tip*

To enable an appropriate level of mission support and the diligent implementation of current and future information security requirements, each agency should establish a formal process to validate system level security categorizations in terms of agency priorities. This will not only promote comparable evaluation of systems, but also yield added benefits to include leveraging common security controls and establishing defense-in-depth.

## 2.3 Role in the System Development Lifecycle

An initial security categorization should occur early in the agency's system development lifecycle (SDLC). The resulting security categorization would feed into security requirements identification (later to evolve into security controls) and other related activities such as privacy impact analysis or critical infrastructure analysis. Ultimately, the identified security requirements and selected security controls are introduced to the standard systems engineering process to effectively integrate the security controls with the information systems functional and operational requirements, as well as other pertinent system requirements (e.g., reliability, maintainability, supportability).

## 2.4 Role in the Certification and Accreditation Process

Security categorization establishes the foundation of the certification and accreditation (C&A) activity by determining the levels of rigor required for certification and overall assurance testing of security controls, as well as additional activities that may be needed (i.e., privacy and critical infrastructure protection (CIP)). Thus, it assists in determining C&A level of effort and associated activity duration.

Security categorization is a prerequisite activity for the C&A process. The categorization should be revisited at least every three years or when significant change occurs to the system or supporting business lines. Situational changes outside the system or agency may require a reevaluation of the categorization (i.e., directed mission changes, changes in governance, elevated or targeted threat activities). For more information, see NIST SP 800-64, *Security Considerations in the Information System Development Life Cycle* and NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*.

*Implementation Tip*

It is important to routinely revisit the security categorization as the mission/ business changes because it is likely the impact levels or even information types may change as well.

## 2.5 Role in the NIST Risk Management Framework

Security Categorization is the key first step in the Risk Management Framework[5] because of its effect on all other steps in the framework from selection of security controls to level of effort in assessing security control effectiveness.

Figure 1, NIST Risk Management Framework, depicts the role of NIST security standards and guidelines for information system security.

[5] NIST SP 800-39, *Managing Risk from Information Systems: An Organizational Perspective*, (Initial Public Draft), October 2007.

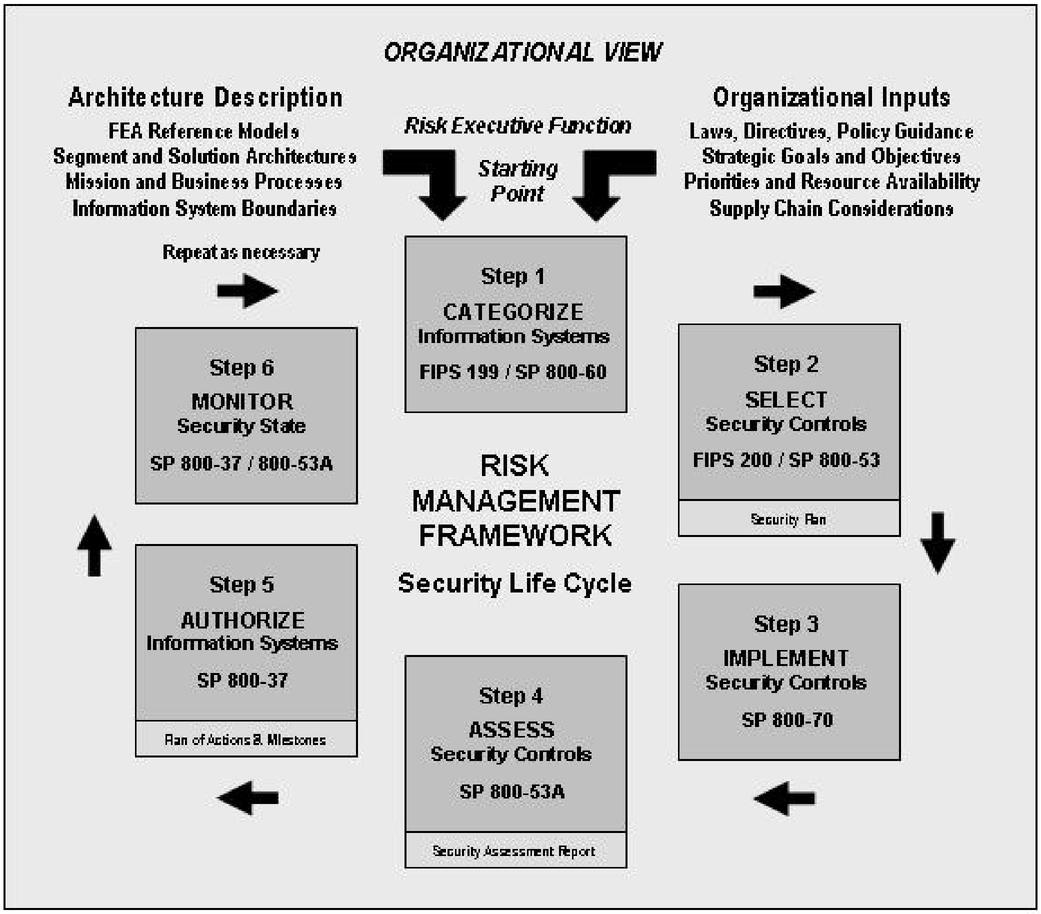


**Figure 1: NIST Risk Management Framework**

The security categorization process documented in this publication provides input into the following processes:

- Step 2: Select an initial set of security controls for the information system based on the FIPS 199 security categorization and apply tailoring guidance as appropriate, to obtain a starting point for required controls as specified in FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems* and NIST SP 800-53, *Recommended Security Controls for Federal Information Systems.* Utilizing NIST SP 800-53 and SP 800-30, *Risk Management Guide for Information Technology Systems, s*upplement the initial set of tailored security controls based on an assessment of risk and local conditions including organization-specific security requirements, specific threat information, cost-benefit analyses, or special circumstances.

- Step 3: Implement the security controls in the information system.

- Step 4: Assess the security controls using appropriate methods and procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. (Reference NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*).

- Step 5: Authorize information system operation based upon a determination of the risk to organizational operations, organizational assets, or to individuals resulting from the operation of the information system and the decision that this risk is acceptable as specified in NIST SP 800-37*, Guide for the Security Certification and Accreditation of Federal Information Systems.*

- Step 6: Monitor and assess selected security controls in the information system on a continuous basis including documenting changes to the system, conducting security impact analyses of the associated changes, and reporting the security status of the system to appropriate organizational officials on a regular basis. (Reference NIST SP 800-37 and SP 800-53A).

# 3.0 SECURITY CATEGORIZATION OF INFORMATION AND INFORMATION SYSTEMS

Federal Information Processing Standard 199 (FIPS 199), *Standards for Security Categorization of Federal Information and Information Systems*, defines the security categories, security objectives, and impact levels to which SP 800-60 maps information types. FIPS 199 establishes security categories based on the magnitude of harm expected to result from compromises rather than on the results of an assessment that includes an attempt to determine the probability of compromise. FIPS 199 also describes the context of use for this guideline. Some of the content of FIPS 199 is included in this section in order to simplify the use of this guideline.

## 3.1 Security Categories and Objectives

### 3.1.1 Security Categories

FIPS 199 establishes security categories for both information[6] and information systems. The security categories are based on the potential impact on an organization should certain events occur. The potential impacts could jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization.

FIPS 199 establishes three potential levels of impact (low, moderate, and high) relevant to securing Federal information and information systems for each of three stated security objectives (confidentiality, integrity, and availability).

### 3.1.2 Security Objectives and Types of Potential Losses

As reflected in Table 1, FISMA and FIPS 199 define three security objectives for information and information systems.

**Table 1: Information and Information System Security Objectives**

| Security Objectives | FISMA Definition [44 U.S.C., Sec. 3542] | FIPS 199 Definition |
|---|---|---|
| **Confidentiality** | "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" | A loss of *confidentiality* is the unauthorized disclosure of information. |
| **Integrity** | "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…" | A loss of *integrity* is the unauthorized modification or destruction of information. |
| **Availability** | "Ensuring timely and reliable access to and use of information…" | A loss of *availability* is the disruption of access to or use of information or an information system. |

[6] Information is categorized according to its *information type*. An information type is a specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or, in some instances, by a specific law, Executive Order, directive, policy, or regulation.

## 3.2 Impact Assessment

FIPS 199 defines three levels of *potential impact* on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability). The application of these definitions must take place within the context of each organization and the overall national interest. Table 2 provides FIPS 199 potential impact definitions.

**Table 2: Potential Impact Levels**

| Potential Impact | Definitions |
|---|---|
| **Low** | The potential impact is **low** if—The loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.[7]<br>A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals. |
| **Moderate** | The potential impact is **moderate** if—The loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.<br>A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries. |
| **High** | The potential impact is **high** if—The loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.<br>A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries. |

In FIPS 199, the security category of an information type can be associated with both user information and system information[8] and can be applicable to information in either electronic or non-electronic form. It is also used as input in considering the appropriate security category for a system. Establishing an appropriate security category for an information type simply requires determining the *potential impact* for each security objective associated with the particular information type. The generalized format for expressing the security category, or *SC*, of an information type is:

[7] Adverse effects on individuals may include, but are not limited to, loss of the privacy to which individuals are entitled under law.

[8] System information (e.g., network routing tables, password files, cryptographic key management information) must be protected at a level commensurate with the most critical or sensitive user information being processed by the information system to ensure confidentiality, integrity, and availability.

$$\text{Security Category}_{\text{information type}} = \{(\text{confidentiality, impact}), (\text{integrity, impact}), (\text{availability, impact})\}$$

where the acceptable values for potential *impact* are low, moderate, high, or not applicable.[9]

[9] The potential impact value of *not applicable* may be applied only to the confidentiality security objective.

## 4.0 Assignment of Impact Levels And Security Categorization

This section provides a methodology for assigning security impact levels and security categorizations for information types and information systems consistent with the organization's assigned mission and business functions based on FIPS 199, Standards for Security Categorization of Federal Information and Information Systems. This document assumes that the user has read and is familiar with FIPS 199. Figure 2 illustrates the four-step security categorization process and how it drives the selection of baseline security controls.

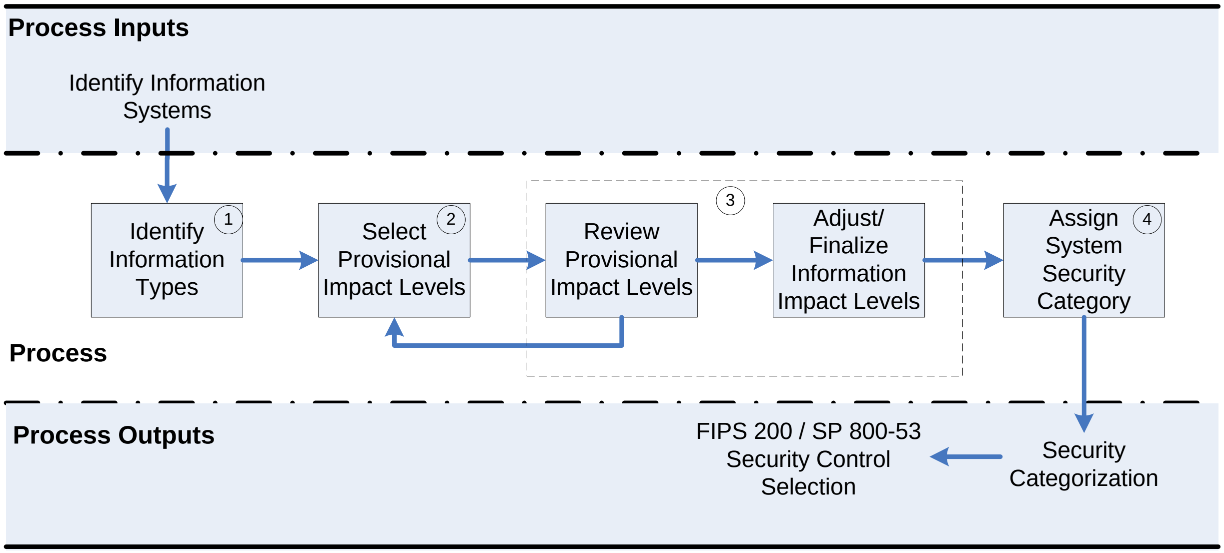
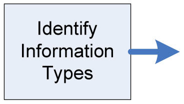
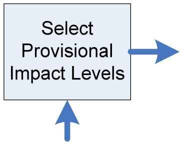
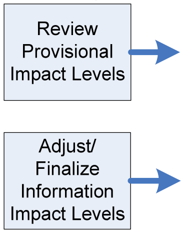
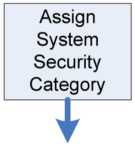

Process Inputs
Identify Information Systems
Process
Identify Information Types
1
Select Provisional Impact Levels
2
3
Review Provisional Impact Levels
Adjust/ Finalize Information Impact Levels
Assign System Security Category
4
Process Outputs
FIPS 200 / SP 800-53 Security Control Selection
Security Categorization

**Figure 2: SP 800-60 Security Categorization Process Execution**

Table 3 provides a step-by-step roadmap for identifying information types, establishing security impact levels for loss of confidentiality, integrity, and availability of information types, and assigning security categorization for the information types and for the information systems. Security categorization is the basis for identifying an initial baseline set of security controls for the information system.[10] Each functional step in the process is explained in detail in Sections 4.1 through 4.4.

[10] An information system is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information [Source: SP 800-53; FIPS 200; FIPS 199; 44 U.S.C., Sec. 3502; OMB Circular A-130, App. III]

**Table 3: SP 800-60 Process Roadmap**

| Process Step | Activities | Roles |
|---|---|---|
| Input: Identify information systems | • Agencies should develop their own policies regarding information system identification for security categorization purposes. The system is generally bounded by a security perimeter[11]. | CIO; SAISO; Mission Owners |
| Step 1<br><br> | • Document the agency's business and mission areas<br>• Identify all of the information types that are input, stored, processed, and/or output from each system [Section 4.1]<br>o Identify *Mission–based* Information Type categories based on supporting FEA Lines of Business [Section 4.1.1]<br>o As applicable, identify *Management and Support* Information Type categories based on supporting FEA Lines of Business [Section 4.1.2]<br>o Specify applicable sub-functions for the identified *Mission-based* and *Management and Support* categories [Volume II, Appendices C and D]<br>o As necessary, identify other required information types [Sections 4.1.3, 4.1.4]<br>• Document applicable information types for the identified information system along with the basis for the information type selection [Section 4.5] | Mission Owners; Information Owners |
| Step 2<br><br> | • Select the security impact levels for the identified information types<br>o from the recommended provisional impact levels for each identified information type [Volume II, Appendices C and D)<br>o or, from FIPS 199 criteria provided in Table 7 Section 4.2.1, and Section 4.2.2<br>• Determine the security category (SC) for each information type: $SC_{\text{information type}}$ = {(confidentiality, impact), (integrity, impact), (availability, impact)}<br>• Document the provisional impact level of confidentiality, integrity, and availability associated with the system's information type [Section 4.5] | Information System Security Officer (ISSO) |
| Step 3<br><br> Review<br>Provisional<br>Impact Levels<br>Adjust/<br>Finalize<br>Information<br>Impact Levels | • Review the appropriateness of the provisional impact levels based on the organization, environment, mission, use, and data sharing [Section 4.3]<br>• Adjust the impact levels as necessary based on the following considerations:<br>o Confidentiality, integrity, and availability factors [Section 4.2.2]<br>o Situational and operational drivers (timing, lifecycle, etc.) [Section 4.3]<br>o Legal or statutory reasons<br>• Document all adjustments to the impact levels and provide the rationale or justification for the adjustments [Section 4.5] | SAISO; ISSO; Mission Owners; Information Owners |
| Step 4<br><br> | • Review identified security categorizations for the aggregate of information types.<br>• Determine the system security categorization by identifying the security impact level high water mark for each of the security objectives (confidentiality, integrity, availability): $SC_{\text{System X}}$ = {(confidentiality, impact), (integrity, impact), (availability, impact)}<br>• Adjust the security impact level high water mark for each system security objective, as necessary, by applying the factors discussed in section 4.4.2.<br>• Assign the overall information system impact level based on the highest impact level for the system security objectives (confidentiality, integrity, availability)<br>• Follow the agency's oversight process for reviewing, approving, and documenting all determinations or decisions [Section 4.5] | CIO, SAISO; ISSO; Mission Owners; Information Owners |
| Output: Security Categorization | • Output that can be used as input to the selection of the set of security controls necessary for each system and the system risk assessment<br>• The minimum security controls recommended for each system security category can be found in NIST SP 800-53, as updated | CIO; ISSO; Authorizing Officials; Developers |

[11] Security perimeter is synonymous with the term accreditation boundary and includes all components of an information system to be accredited by an authorizing official and excludes separately accredited systems to which the information system is connected.

## 4.1 Step 1: Identify Information Types

In accordance with FIPS 199, agencies shall identify all of the applicable information types that are representative of input, stored, processed, and/or output data from each system. The initial activity in mapping types of Federal information and information systems to security objectives and impact levels is the development of an information taxonomy, or creation of a catalog of information types.[12] The basis for the identification of information types is the OMB's Business Reference Model (BRM) described in the October 2007 publication, *FEA Consolidated Reference Model Document, Version 2.3*. The *BRM* describes four business areas containing 39 FEA lines of business.[13] The four business areas separate government operations into high-level categories relating:

- The purpose of government (*services for citizens*);
- The mechanisms the government uses to achieve its purpose (*mode of delivery*);
- The support functions necessary to conduct government operations (*support delivery of services*); and
- The resource management functions that support all areas of the government's business (*management of government resources*).

The first two business areas, *services for citizens* and the *mode of delivery* represent the NIST SP 800-60 Mission-based Information Types and will be discussed first in the following section, while *support delivery of services* and *management of government resources* represent Management and Support Information Types and will be presented in Section 4.1.2.

Although this guideline identifies a number of information types and bases its taxonomy on the *BRM*, only a few of the types identified are likely to be processed by any single system. Also, each system may process information that does not fall neatly into one of the listed information types. Once a set of information types identified in this guideline has been selected, it is prudent to review the information processed by each system under review to see if additional types need to be identified for impact assessment purposes. Also, it is recommended that organizational officials maintain proper documentation of identified information types per information system along with the basis for the information type selection. Guidance for documenting information types is provided in Section 4.5.

### 4.1.1 Identification of Mission-based Information Types

This section describes a process for identifying mission-based information types and for specifying the impact of unauthorized disclosure, modification, or unavailability of this information. Mission-based information types are, by definition, specific to individual departments and agencies or to specific sets of departments and agencies. The BRM *services for citizens* business area provides the primary frame of reference for determining the security

[12] One issue associated with the taxonomy activity is the determination of the degree of granularity. If the categories are too broad, then the guidelines for assigning impact levels are likely to be too general to be useful. On the other hand, if an attempt is made to provide guidelines for each element of information processed by each government agency, the guideline is likely to be unwieldy and to require excessively frequent changes.

[13] Definitions are provided in SP 800-60 Appendix A for the BRM terms such as "Business Areas", "Lines of Businesses" and "Sub-functions".

objectives impact levels for mission-based information and information systems. The consequences or impact of unauthorized disclosure of information, modification or destruction of information, and disruption of access to or use of information are defined by the nature and beneficiary of the service being provided or supported. The BRM establishes 26 direct services and delivery support lines of business with 98 associated information types (reference Table 4). Two additional information types were included to address Executive Functions of the Executive Office of the President and Trade Law Enforcement. These additions are identified by italics in Table 4.

**Table 4: Mission-Based Information Types and Delivery Mechanisms**[14]

**Mission Areas and Information Types [Services for Citizens]**

**D.1 Defense & National Security**
Strategic National & Theater Defense
Operational Defense
Tactical Defense

**D.2 Homeland Security**
Border and Transportation Security
Key Asset and Critical Infrastructure Protection
Catastrophic Defense
*Executive Functions of the Executive Office of the President (EOP)*

**D.3 Intelligence Operations**
Intelligence Planning
Intelligence Collection
Intelligence Analysis & Production
Intelligence Dissemination
Intelligence Processing

**D.4 Disaster Management**
Disaster Monitoring and Prediction
Disaster Preparedness and Planning
Disaster Repair and Restoration
Emergency Response

**D.5 International Affairs & Commerce**
Foreign Affairs
International Development and Humanitarian Aid
Global Trade

**D.6 Natural Resources**
Water Resource Management
Conservation, Marine and Land Management
Recreational Resource Management and Tourism
Agricultural Innovation and Services

**D.7 Energy**
Energy Supply
Energy Conservation and Preparedness
Energy Resource Management
Energy Production

**D.8 Environmental Management**
Environmental Monitoring and Forecasting
Environmental Remediation
Pollution Prevention and Control

**D.9 Economic Development**
Business and Industry Development
Intellectual Property Protection
Financial Sector Oversight
Industry Sector Income Stabilization

**D.10 Community & Social Services**
Homeownership Promotion
Community and Regional Development
Social Services
Postal Services

**D.11 Transportation**
Ground Transportation
Water Transportation
Air Transportation
Space Operations

**D.12 Education**
Elementary, Secondary, and Vocational Education
Higher Education
Cultural and Historic Preservation
Cultural and Historic Exhibition

**D.13 Workforce Management**
Training and Employment
Labor Rights Management
Worker Safety

**D.14 Health**
Access to Care
Population Health Mgmt & Consumer Safety
Health Care Administration
Health Care Delivery Services
Health Care Research and Practitioner Education

**D.15 Income Security**
General Retirement and Disability
Unemployment Compensation
Housing Assistance
Food and Nutrition Assistance
Survivor Compensation

**D.16 Law Enforcement**
Criminal Apprehension
Criminal Investigation and Surveillance
Citizen Protection
Leadership Protection
Property Protection
Substance Control
Crime Prevention
*Trade Law Enforcement*

**D.17 Litigation & Judicial Activities**
Judicial Hearings
Legal Defense
Legal Investigation
Legal Prosecution and Litigation
Resolution Facilitation

**D.18 Federal Correctional Activities**
Criminal Incarceration
Criminal Rehabilitation

**D.19 General Sciences & Innovation**
Scientific and Technological Research and Innovation
Space Exploration and Innovation

[14] The recommended information types provided in NIST SP 800-60 are established from the "business areas" and "lines of business" from OMB's Business Reference Model (BRM) section of Federal Enterprise Architecture (FEA) Consolidated Reference Model Document Version 2.3, October 2007.

**Table 4: Mission-Based Information Types and Delivery Mechanisms**[14]

| Services Delivery Mechanisms and Information Types [Mode of Delivery] | | |
|---|---|---|
| **D.20 Knowledge Creation & Management**<br>Research and Development<br>General Purpose Data and Statistics<br>Advising and Consulting<br>Knowledge Dissemination<br>**D.21 Regulatory Compliance & Enforcement**<br>Inspections and Auditing<br>Standards Setting/Reporting Guideline Development<br>Permits and Licensing | **D.22 Public Goods Creation & Management**<br>Manufacturing<br>Construction<br>Public Resources, Facility and Infrastructure Management<br>Information Infrastructure Management<br>**D.23 Federal Financial Assistance**<br>Federal Grants (Non-State)<br>Direct Transfers to Individuals<br>Subsidies<br>Tax Credits | **D.24 Credit and Insurance**<br>Direct Loans<br>Loan Guarantees<br>General Insurance<br>**D.25 Transfers to State/ Local Governments**<br>Formula Grants<br>Project/Competitive Grants<br>Earmarked Grants<br>State Loans<br>**D.26 Direct Services for Citizens**<br>Military Operations<br>Civilian Operations |

The approach to establishing mission-based information types at an agency level begins by documenting the agency's business and mission areas. The owner, or designee, of each information system is responsible for identifying the information types stored in, processed by, or generated by that information system. In the case of mission-based information, the responsible individuals, in coordination with management, operational, and security stakeholders, should compile a comprehensive set of lines of business and mission areas conducted by the agency. In addition, the responsible individuals should identify the applicable sub-functions necessary to conduct agency business and in turn accomplish the agency's mission. For example, one mission conducted by an agency might be law enforcement. Sub-functions that are part of the agency's law enforcement mission might include criminal investigation and surveillance, criminal apprehension, criminal incarceration, citizen protection, crime prevention, and property protection. Each of these sub-functions would represent an information type.

Recommended mission-based lines of business and constituent sub-functions that may be processed by information systems are identified in Table 4 with details provided in Volume II, Appendix D, "Examples of Impact Determination for Mission-based Information and Information Systems."

*Implementation Tip*

At the agency level, all government agencies perform at least one of the *mission areas* and employ at least one of the *services delivery mechanisms* described in Table 4. However, some information systems may only provide a supporting role to the agency's mission and not directly process any of the *mission-based* information types.

### 4.1.2 Identification of Management and Support Information

Much Federal government information and many supporting information systems are not employed directly to provide direct mission-based services, but are primarily intended to support delivery of services or to manage resources. The *support delivery of services* and *management of resources* business areas are together composed of 13 lines of business (Tables 5 and 6). The

*BRM* subdivides the lines of business into 72 sub-functions. The *support delivery of services* and *management of resource* business areas are common to most Federal government agencies, and the information associated with each of their sub-functions is identified in this guideline as a *management and support* information type. Four additional *management and support* sub-factor information types have been defined to address privacy information. One additional *management and support* sub-factor information type has been defined to address General Information as a catch-all information type that may not be defined by the FEA BRM. As such, agencies may find it necessary to identify additional information types not defined in the BRM and assign associated security impact levels to those types.

#### 4.1.2.1 Services Delivery Support Information

Most information systems employed in both service delivery support and resource management activities engage in one or more of the eight *support delivery of services* lines of business. Each of the information types associated with *support delivery of services* sub-functions is provided in Table 5. Volume II, Appendix C.2, "Services Delivery Support Functions," recommends provisional impact levels for confidentiality, integrity, and availability security objectives. These service support functions are the day-to-day activities necessary to provide the critical policy, programmatic, and managerial foundation that support Federal government operations. The direct service missions and constituencies ultimately being supported by service support functions comprise a significant factor in determining the security impacts associated with compromise of information associated with the *support delivery of services* business area.

**Table 5: Services Delivery Support Functions and Information Types**[15]

**C.2.1 Controls and Oversight**
Corrective Action (Policy/Regulation)
Program Evaluation
Program Monitoring

**C.2.2 Regulatory Development**
Policy & Guidance Development
Public Comment Tracking
Regulatory Creation
Rule Publication

**C.2.3 Planning & Budgeting**
Budget Formulation
Capital Planning
Enterprise Architecture
Strategic Planning
Budget Execution
Workforce Planning
Management Improvement
Budgeting & Performance Integration
Tax & Fiscal Policy

**C.2.4 Internal Risk Management & Mitigation**
Contingency Planning
Continuity of Operations
Service Recovery

**C.2.5 Revenue Collection**
Debt Collection
User Fee Collection
Federal Asset Sales

**C.2.6 Public Affairs**
Customer Services
Official Information Dissemination
Product Outreach
Public Relations

**C.2.7 Legislative Relations**
Legislation Tracking
Legislation Testimony
Proposal Development
Congressional Liaison Operations

**C.2.8 General Government**
Central Fiscal Operations
Legislative Functions
Executive Functions
Central Property Management
Central Personnel Management
Taxation Management
Central Records & Statistics Management
*Income Information*
*Personal Identity and Authentication*
*Entitlement Event Information*
*Representative Payee Information*
*General Information*

#### 4.1.2.2 Government Resource Management Information

The *government resource management information* business area includes the back office support activities enabling the Federal government to operate effectively. The five *government resource management information* lines of business and the sub-functions associated with each

[15] The recommended information types provided in NIST SP 800-60 are established from the "business areas" and "lines of business" from OMB's Business Reference Model (BRM) section of Federal Enterprise Architecture (FEA) Consolidated Reference Model Document Version 2.3, October 2007.

information type are identified in Table 6. Volume II, Appendix C.3, "Government Resource Management Information," recommends provisional impact levels for confidentiality, integrity, and availability security objectives. Many departments and agencies operate their own support systems. Others obtain at least some support services from other organizations. Some agencies' missions are primarily to support other government departments and agencies in the conduct of direct service missions. As indicated above, security objectives and associated security impact levels for administrative and management information and systems are determined by the nature of the supported direct services and constituencies being supported.

**Table 6: Government Resource Management Functions and Information Types**[16]

| **C.3.1 Administrative Management** | **C.3.3 Human Resource Management** | **C.3.5 Information & Technology Management** |
|---|---|---|
| Facilities, Fleet, and Equipment Management<br>Help Desk Services<br>Security Management<br>Travel<br>Workplace Policy Development & Management | HR Strategy<br>Staff Acquisition<br>Organization & Position Mgmt<br>Compensation Management<br>Benefits Management<br>Employee Performance Mgmt<br>Employee Relations<br>Labor Relations<br>Separation Management<br>Human Resources Development | System Development<br>Lifecycle/Change Management<br>System Maintenance<br>IT Infrastructure Maintenance<br>Information Security<br>Record Retention<br>Information Management<br>System and Network Monitoring<br>Information Sharing |
| **C.3.2 Financial Management** | **C.3.4 Supply Chain Management** | |
| Accounting<br>Funds Control<br>Payments<br>Collections and Receivables<br>Asset and Liability Management<br>Reporting and Information<br>Cost Accounting/ Performance Measurement | Goods Acquisition<br>Inventory Control<br>Logistics Management<br>Services Acquisition | |

### 4.1.3 Legislative and Executive Information Mandates

During the identification of information types within an information system, agency personnel should afford special consideration for applicable governances addressing the information processed and the agency's supported mission. Volume II, Appendix E lists legislative and executive mandates establishing sensitivity and criticality guidelines for specific information types.

### 4.1.4 Identifying Information Types Not Listed in this Guideline

The FEA BRM Information Types are provided only as a taxonomy guideline. Not all information processed by an information system may be identified from Tables 4 through 6. Therefore, an agency may identify unique information types not listed in this guideline or may choose not to select provisional impact levels from Volume II, Appendix C (for management and support information types) or Volume II, Appendix D (for mission-based information types). Sections 4.2.1 through 4.2.3 of this guideline provide assistance to agencies in assigning provisional security categories to agency-identified information types and information systems.

Additionally, SP 800-60 provides a *management and support* sub function, General Information Type, which can be used by agencies as a means to identify and categorize information not

[16] The recommended information types provided in NIST SP 800-60 are established from the "business areas" and "lines of business" from OMB's Business Reference Model (BRM) section of Federal Enterprise Architecture (FEA) Consolidated Reference Model Document Version 2.3, October 2007.

contained in the FEA BRM. A complete description of the General Information Type information should be captured in the agency's collection and documentation process.

## 4.2 Step 2: Select Provisional Impact Level

In Step 2, organizations should establish provisional impact levels[17] based on the identified information types in Step 1. The provisional impact levels are the original impact levels assigned to the confidentiality, integrity, and availability security objectives of an information type from Volume II before any adjustments are made. Also in this step, the initial security categorization for the information type is established and documented.

Volume II, Appendix C suggests provisional confidentiality, integrity, and availability impact levels for management and support information types, and Volume II, Appendix D provides examples of provisional impact level assignments for mission-based information types. Using the impact assessment criteria identified in Section 3.2 for the security objectives and types of potential losses identified in Section 3.1.2, the organizational entity responsible for impact determination must assign impact levels and consequent security categorization for the *mission-based* and *management and support* information types identified for each information system.

### 4.2.1 FIPS 199 Security Categorization Criteria

Where an information type processed by an information system is not categorized by this guideline [based on information types identified in Volume II, Appendices C and D], an initial impact determination will need to be made based on FIPS 199 categorization criteria (cited in Table 7).

Agencies can assign security categories to information types and information systems by selecting and adjusting appropriate Table 7 values for the potential impact of compromises of confidentiality, integrity, and availability security objectives. Those responsible for impact level selection and subsequent security categorization should apply the criteria provided in Table 7 to each information type received by, processed in, stored in, and/or generated by each system for which they are responsible. The security categorization will generally be determined based on the most sensitive or critical information received by, processed in, stored in, and/or generated by the system under review.

[17] Impact levels (plural), as used here, refers to *low*, *moderate*, *high*, or *not applicable* values assigned to each security objective (i.e., confidentiality, integrity, and availability) used in expressing the security category of an information type or information systems. The value of *not applicable* only applies to information types and not to information systems.

**Table 7: Categorization of Federal Information and Information Systems**

| Security Objective | Potential Impact | | |
|---|---|---|---|
| | Low | Moderate | High |
| ***Confidentiality***<br>Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.<br>[44 U.S.C., Sec. 3542] | The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals. |
| ***Integrity***<br>Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.<br>[44 U.S.C., Sec. 3542] | The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals. |
| ***Availability***<br>Ensuring timely and reliable access to and use of information.<br>[44 U.S.C., Sec. 3542] | The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. | The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals. | The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals. |

### 4.2.2 Common Factors for Selection of Impact Levels

Where an agency determines security impact levels and security categorization based on local application of FIPS 199 criteria, it is recommended that the following factors be considered with respect to security impacts for each information type.

#### 4.2.2.1 Confidentiality Factors

Using the FIPS 199 potential impact criteria summarized in Table 7, each information type should be evaluated for confidentiality with respect to the impact level associated with unauthorized disclosure of (i) each known variant of the information belonging to the type and (ii) each use of the information by the system under review. Answers to the following questions will help in the evaluation process:

- How can a malicious adversary use the unauthorized disclosure of information to do limited/serious/severe harm to agency operations, agency assets, or individuals?
- How can a malicious adversary use the unauthorized disclosure of information to gain control of agency assets that might result in unauthorized modification of information, destruction of information, or denial of system services that would result in limited/serious/severe harm to agency operations, agency assets, or individuals?

- Would unauthorized disclosure/dissemination of elements of the information type violate laws, executive orders, or agency regulations?

#### 4.2.2.2 Integrity Factors

Using the FIPS 199 potential impact criteria summarized in Table 7, each information type should be evaluated for integrity with respect to the impact level associated with unauthorized modification or destruction of (i) each known variant of the information belonging to the type and (ii) each use of the information by the system under review. Answers to the following questions will help in the evaluation process:

- How can a malicious adversary use the unauthorized modification or destruction of information to do limited/serious/severe harm to agency operations, agency assets, or individuals?
- Would unauthorized modification/destruction of elements of the information type violate laws, executive orders, or agency regulations?

Unauthorized modification or destruction of information can take many forms. The changes can be subtle and hard to detect, or they can occur on a massive scale. One can construct an extraordinarily wide range of scenarios for modification of information and its likely consequences. Just a few examples include forging or modifying information to:

- Reduce public confidence in an agency;
- Fraudulently achieve financial gain;
- Create confusion or controversy by promulgating a fraudulent or incorrect procedure;
- Initiate confusion or controversy through false attribution of a fraudulent or false policy;
- Influence personnel decisions;
- Interfere with or manipulate law enforcement or legal processes;
- Influence legislation; or
- Achieve unauthorized access to government information or facilities.

In most cases, the most serious impacts of integrity compromise occur when some action is taken that is based on the modified information or the modified information is disseminated to other organizations or the public.

Undetected loss of integrity can be catastrophic for many information types. The consequences of integrity compromise can be either direct (e.g., modification of a financial entry, medical alert, or criminal record) or indirect (e.g., facilitation of unauthorized access to sensitive or private information or deny access to information or information system services). Malicious use of write access to information and information systems can do enormous harm to an agency's mission and can be employed to use an agency system as a proxy for attacks on other systems.

In many cases, the consequences of unauthorized modification or destruction of information to agency mission functions and public confidence in the agency can be expected to be limited. In other cases, integrity compromises can result in the endangerment of human life or other severe consequences. The impact can be particularly severe in the case of time-critical information.

#### 4.2.2.3 Availability Factors

Using the FIPS 199 potential impact criteria summarized in Table 7, each information type should be evaluated for availability with respect to the impact level associated with the disruption of access to or use of information of (i) each known variant of the information belonging to the type and (ii) each use of the information by the system under review. Answers to the following questions will help in the evaluation process:

- How can a malicious adversary use the disruption of access to or use of information to do limited/serious/severe harm to agency operations, agency assets, or individuals?
- Would disruption of access to or use of elements of the information type violate laws, executive orders, or agency regulations?

For many information types and information systems, the availability impact level depends on how long the information or system remains unavailable. Undetected loss of availability can be catastrophic for many information types. For example, permanent loss of budget execution, contingency planning, continuity of operations, service recovery, debt collection, taxation management, personnel management, payroll management, security management, inventory control, logistics management, or accounting information databases would be catastrophic for almost any agency. Complete reconstruction of such databases would be time consuming and expensive.

In most cases, the adverse effects of a limited-duration availability compromise on an organization's mission functions and public confidence will be limited. In contrast, for time-critical information types, availability is less likely to be restored before serious harm is done to agency assets, operations, or personnel (or to public welfare). In such instances, the documented availability impact level recommendations should indicate the information is time-critical and the basis for criticality.

### 4.2.3 Examples of FIPS 199-Based Selection of Impact Levels

FIPS 199-based examples of security objective impact selection and security categorization for sample information types follow:

EXAMPLE 1: An organization managing *public information* on its web server determines that there is no potential impact from a loss of confidentiality (i.e., confidentiality requirements are not applicable), a moderate potential impact from a loss of integrity, and a moderate potential impact from a loss of availability. The resulting security category of this information type is expressed as:

> Security Category $_{\text{public information}}$ = {(confidentiality, n/a), (integrity, moderate), (availability, moderate)}.

EXAMPLE 2: A law enforcement organization managing extremely sensitive *investigative information* determines that the potential impact from a loss of confidentiality is high, the potential impact from a loss of integrity is moderate, and the potential impact from a loss of availability is moderate. The resulting security category for this type of information is expressed as:

Security Category $_{\text{investigative information}}$ = {(confidentiality, high), (integrity, moderate), (availability, moderate)}.

EXAMPLE 3: A financial organization managing routine *administrative information* (not privacy-related information) determines that the potential impact from a loss of confidentiality is low, the potential impact from a loss of integrity is low, and the potential impact from a loss of availability is low. The resulting security category of this information type is expressed as:

Security Category $_{\text{administrative information}}$ = {(confidentiality, low), (integrity, low), (availability, low)}.

In general, security objective impact assessment is independent of mechanisms employed to mitigate the consequences of a compromise.

## 4.3 Step 3: Review Provisional Impact Levels and Adjust/Finalize Information Type Impact Levels

In Step 3, organizations should review and adjust the provisional security impact levels for the security objectives of each information type and arrive at a finalized state. To accomplish this, organizations should: (i) review the appropriateness of the provisional impact levels based on the organization, environment, mission, use, and data sharing; (ii) adjust the security objective impact levels as necessary using the special factors[18] guidance found in Volume II, Appendices C and D; and (iii) document all adjustments to the impact levels and provide the rationale or justification for the adjustments.

When security categorization impact levels recommended in Section 4.2 or Volume II, Appendices C and D are adopted as provisional security impact levels, the agency should review the appropriateness of the provisional impact levels in the context of the organization, environment, mission, use, and data sharing associated with the information system under review. This review should include the agency's mission importance; lifecycle and timeliness implications; configuration and security policy related information; special handling requirements; etc. The FIPS 199 factors presented in Section 4.2.2 of this document should be used as the basis for decisions regarding adjustment or finalization of the provisional impact levels. The confidentiality, integrity, and availability impact levels may be adjusted one or more times in the course of the review. Once the review and adjustment process is complete, the mapping of impact levels by information type can be finalized.

The impact of information compromise of a particular type can vary in different agencies or in dissimilar operational contexts. Also, the impact for an information type may vary throughout the life cycle. For example, contract information that has a ***moderate*** confidentiality impact level during the life of the contract may have a ***low*** impact level when the contract is completed. Policy information may have ***moderate*** confidentiality and integrity impact levels during the policy development process, ***low*** confidentiality and ***moderate*** integrity impact levels when the policy is implemented, and ***low*** confidentiality and integrity impact levels when the policy is no longer used.

[18] The special factor guidance in NIST SP 800-60, Volume II, provides specific guidance on considerations for adjusting each security objective (confidentiality, integrity, and availability) for each information type. The special factor guidance is applied to each information type, based on how the information type is used, the organization's mission, or the system's operating environment.

The impact levels associated with the *management and support* information common to many agencies are strongly affected by the *mission-based* information with which it is associated. That is, agency-common management and support information used with very sensitive or critical mission-based information types may have higher impact levels than the same agency-common information used with less critical mission-based information types.

Further, information systems process many types of information. Not all of these information types are likely to have the same security impact levels. The compromise of some information types will jeopardize system functionality and agency mission more than the compromise of other information types. System security impact levels must be assessed in the context of system mission and function as well as on the basis of the aggregate of the component information types.

Additionally, configuration and security policy enforcement information should be reviewed and adjusted considering the information processed on the system. Configuration and security policy information includes password files, network access rules, other hardware and software configuration settings, and documentation affecting access to the information system's data, programs, and/or processes. At a minimum, a low confidentiality and integrity impact level will apply to this set of information and processes due to a potential for corruption, misuse, or abuse of system information and processes.

A factor specific to the confidentiality objective is information subject to special handling (e.g., information subject to the Privacy Act of 1974, 5 U.S.C. § 552A). Regardless of other considerations, some minimum confidentiality impact level must be assigned to any information system that stores, processes, or generates such information. Examples of such information include information subject to the Trade Secrets Act, the Privacy Act, Department of Energy Safeguards Information, Internal Revenue Service Official Use Only Information, and Environmental Protection Agency Confidential Business Information (e.g., subject to Toxic Substances Control Act; Resource Conservation and Recovery Act; Comprehensive Environmental Response, Compensation, and Liability Act). Some of these statutory and regulatory specifications are listed in Volume II, Appendix E, "Legislative and Executive Sources Establishing Sensitivity/Criticality."

## 4.4 Step 4: Assign System Security Category

Once the security impact levels have been selected, reviewed and adjusted as necessary for the security objectives of each individual information type processed by an information system, it is necessary to assign a system security category based on the aggregate of information types. The Step 4 activities include the following: (i) review identified security categorizations for the aggregate of information types; (ii) determine the system security categorization by identifying the high water mark for each of the security objectives (confidentiality, integrity, availability) based on the aggregate of the information types; (iii) adjust the high water mark for each system security objective, as necessary, by applying the factors discussed in section 4.4.2; (iv) assign the overall information system impact level based on the highest impact level for the system security objectives; and (v) document all security categorization determinations and decisions.

### 4.4.1 FIPS 199 Process for System Security Categorization

FIPS 199 recognizes that determining the security category of an information system requires additional analysis and must consider the security categories of all information types resident on the information system. For an information system, the potential security impact levels assigned to each of the respective security objectives (confidentiality, integrity, availability) are the highest level (i.e., high water mark) for any one of these objectives that has been determined for the types of information resident on the information system.

Information systems are composed of both computer programs and information. Programs in execution within an information system (i.e., system processes) facilitate the processing, storage, and transmission of information and are necessary for the organization to conduct its essential business functions and operations. These system-processing functions also require protection and could be subject to security categorization as well. However, in the interest of simplification, it is assumed that the security categorization of all information types associated with the information system provide an appropriate worst case potential for the overall information system—thereby obviating the need to consider the system processes in the security categorization of the information system. This is in recognition of:

- The fundamental requirement to protect the integrity, availability, and, for key information such as passwords and encryption keys, the confidentiality of system-level processing functions and information at the high water mark; and
- The strong interdependence between confidentiality, integrity, and availability.

For this reason, FIPS 199 notes that, while the value (i.e., level) of *not applicable* can apply to a security objective for specific information types processed by systems, this value cannot be assigned to any security objective for an information system. There is a minimum provisional impact (i.e., low water mark) for a compromise of confidentiality, integrity, and availability for an information system. This is necessary to protect the system-level processing functions and information critical to the operation of the information system.

The generalized format for expressing the security category, or *SC*, of an information system is:

SC $_{\text{information system}}$ = {(confidentiality, *impact*), (integrity, *impact*), (availability, *impact*)},

where the acceptable values for potential impact are LOW, MODERATE, or HIGH.

The following examples illustrate the system security categorization process described in FIPS 199.

SYSTEM EXAMPLE 1: An information system used for large acquisitions in a contracting organization contains both sensitive, pre-solicitation phase contract information and routine administrative information. The management within the contracting organization determines that: (i) for the sensitive contract information, the potential impact from a loss of confidentiality is moderate, the potential impact from a loss of integrity is moderate, and the potential impact from a loss of availability is low; and (ii) for the routine administrative information (non-privacy-related information), the potential impact from a loss of confidentiality is low, the potential impact from a loss of integrity is low, and the potential impact from a loss of availability is low. The resulting security categories, or *SC*, of these information types are expressed as:

$SC_{\text{contract information}} =$ {(confidentiality, MODERATE), (integrity, MODERATE), (availability, LOW)}, and

$SC_{\text{administrative information}} =$ {(confidentiality, LOW), (integrity, LOW), (availability, LOW)}.

The resulting security category of the information system is expressed as:

$SC_{\text{acquisition system}} =$ {(confidentiality, MODERATE), (integrity, MODERATE), (availability, LOW)},

representing the high water mark or maximum potential impact values for each security objective from the information types resident on the acquisition system.

SYSTEM EXAMPLE 2: A power plant contains a SCADA (supervisory control and data acquisition) system controlling the distribution f electric power for a large military installation. The SCADA system contains both real-time sensor data and routine administrative information. The management at the power plant determines that: (i) for the sensor data being acquired by the SCADA system, there is no potential impact from a loss of confidentiality, a high potential impact from a loss of integrity, and a high potential impact from a loss of availability; and (ii) for the administrative information being processed by the system, there is a low potential impact from a loss of confidentiality, a low potential impact from a loss of integrity, and a low potential impact from a loss of availability. The resulting security categories, or *SC*, of these information types are expressed as:

$SC_{\text{sensor data}} =$ {(confidentiality, NA), (integrity, HIGH), (availability, HIGH)}, and

$SC_{\text{administrative information}} =$ {(confidentiality, LOW), (integrity, LOW), (availability, LOW)}.

The resulting security category of the information system is initially expressed as:

$SC_{\text{SCADA system}} =$ {(confidentiality, LOW), (integrity, HIGH), (availability, HIGH)},

representing the high water mark or maximum potential impact values for each security objective from the information types resident on the SCADA system. The management at the power plant chooses to increase the potential impact from a loss of confidentiality from low to moderate reflecting a more realistic view of the potential impact on the information system should there be a security breach due to the unauthorized disclosure of system-level information or processing functions. The final security category of the information system is expressed as:

$SC_{\text{SCADA system}} =$ {(confidentiality, MODERATE), (integrity, HIGH), (availability, HIGH)}.

### 4.4.2 Guidelines for System Categorization

In some cases, the impact level for a system security category will be higher than any security objective impact level for any information type processed by the system.

The primary factors that most commonly raise the impact levels of the system security category above that of its constituent information types are aggregation and critical system functionality. Additionally, variations in sensitivity/criticality with respect to time may need to be factored into the impact assignment process. Some information loses its sensitivity in time (e.g., economic/commodity projections after they’ve been published). Other information is particularly critical at some point in time (e.g., weather data in the terminal approach area during aircraft landing operations). This section provides some general guidelines regarding how aggregation, critical functionality, and other system factors may affect system security categorization.

*Implementation Tip*

Agency personnel should be aware that there are several factors that should be considered during the aggregation of system information types. When considering these factors, previously unforeseen concerns may surface affecting the confidentiality, integrity, and/or availability impact levels at the system level. These factors include data aggregation, critical system functionality, extenuating circumstances, and other system factors.

In order to effectively accomplish this step, various stakeholders (e.g., management, operational personnel, or security experts) may need to be involved in decisions regarding system-level impact assessments. The following sections provide factors to consider in adjusting the system security objective impact levels.

#### 4.4.2.1 Aggregation

Some information may have little or no sensitivity in isolation but may be highly sensitive in aggregation. In some cases, aggregation of large quantities of a single information type can reveal sensitive patterns and plans, or facilitate access to sensitive or critical systems. In other cases, aggregation of information of several different and seemingly innocuous types can have similar effects. In general, the sensitivity of a given data element is likely to be greater in context than in isolation (e.g., association of an account number with the identity of an individual and/or institution). The availability, routine operational employment, and sophistication of data aggregation and inference tools are all increasing rapidly. If review reveals increased sensitivity or criticality associated with information aggregates, then the system security objective impact levels may need to be adjusted to a higher level than would be indicated by the security impact levels associated with any individual information type. This could be implemented by incorporating a statement that explains the aggregation and potential security objective affected as well as the modification to impact levels.

#### 4.4.2.2 Critical System Functionality

Compromise of some information types may have low impact in the context of a system’s primary function but may have much more significance when viewed in the context of the potential impact of compromising:

- Other systems to which the system in question is connected, or
- Other systems which are dependent on that system’s information.

Access control information for a system that processes only low impact information might initially be thought to have only low impact security objectives. However, if access to that system might result in some form of access to other systems (e.g., over a network), the sensitivity and criticality attributes of all systems to which such indirect access can result needs to be considered. Similarly, some information may, in general, have low sensitivity and/or criticality security objectives. However, that information may be used by other systems to enable extremely sensitive or critical functions (e.g., air traffic control use of weather information or use of commercial flight information to identify military combat transport systems). Loss of data integrity, availability, temporal context, or other context can have catastrophic consequences.

#### 4.4.2.3 Extenuating Circumstances

This publication focuses on categorizing an information system based on its information types and associated security objective impacts. There are times when a system security objective impact level should be elevated based on reasons other than its information. For example, the information system provides critical process flow or security capability, the visibility of the system to the public, the sheer number of other systems reliant on its operation or possibly its overall cost of replacement. These examples, given a specific situation, may provide reason for the system owner to increase the overall security impact level of a system.

An elevation based on extenuating circumstances can be more apparent by comparing the original security categorization to the business impact analysis. If the system was categorized based on FIPS 199 at a Moderate overall impact level but the system owner has determined it needs to be operational within 4-8 hours of a disruption irrespective of the aggregated information type availability security impact level assigned, then there is a disconnect that might be caused by the system's extenuating circumstances.  Agencies must customize the information system availability security impact level as appropriate to obtain full value and accuracy.

#### 4.4.2.4 Other System Factors

***Public Information Integrity***

Most Federal agencies maintain web pages that are accessible to the public.  The vast majority of these public web pages permit interaction between the site and the public.  In some cases, the site provides only information.  In other cases, forms may be submitted via the website (e.g., applications for service or job applications).  In some cases, the site is a medium for business transactions.  Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency.  In most cases, the damage can be corrected within a relatively short period of time, and the damage is limited (impact level is ***low***).  In other cases (e.g., very large fraudulent transactions or modification of a web page belonging to an intelligence/security community component), the damage to mission function and/or public confidence in the agency can be serious.  In such cases, the integrity impact associated with unauthorized modification or destruction of a public web page would be at least ***moderate***.

***Catastrophic Loss of System Availability***

Either physical or logical destruction of major assets can result in very large expenditures to restore the assets and/or long periods of time for recovery.  Permanent loss/unavailability of information system capabilities can seriously hamper agency operations and, where direct services to the public are involved, have a severe adverse effect on public confidence in Federal agencies.  Particularly in the case of large systems, FIPS 199 criteria suggest that catastrophic loss of system availability may result in a ***high*** availability impact level.  Whether or not the impact level of system availability should be ***high*** (and subsequent ***high*** system security impact level) is dependent on other factors, such as cost and criticality of the system, rather than on the security impact levels for the information types being processed by the system.

***Large Supporting and Interconnecting Systems***

Large or complex information systems composed of multiple lower level systems often require additional consideration regarding assignment of system security categorization. This section will provide guidelines for applying and interrelating individual system security categorization results to enterprise organizations, large supporting infrastructures (such as general support systems, data warehouse applications, large data storage units, server farms, and information repositories), and interconnecting systems.

Upon security categorization identification for all information systems interacting with large infrastructure systems, senior IT and security officials have possession of valuable information that can now enable an enterprise wide security perspective. One significant activity includes levying an overall security categorization for the agency's supporting network infrastructures. Since networks, as well as other general support systems, do not inherently "own" mission-based or management and support information types, the infrastructure's categorization is based on the aggregation of the information systems' security categorizations. In other words, the infrastructure's security categorization is the high water mark of the supported information systems and is based on the information types processed, flowed, or stored on the network or general support system. Together, the top down enterprise wide threat assessment and bottom up security assessment derived by aggregation will allow an organization to look at its risk profile from a comprehensive and balanced view. Further, this analysis will ensure the proper application of common security controls supporting the multiple information systems and the protection provided by those controls are inherited by the individual systems.

### *Critical Infrastructures and Key Resources*

Where the mission served by an information system, or the information that the system processes, affects the security of critical infrastructures and key resources, the harm that results from a compromise requires particularly close attention. In this case, an effect on security might include a significant reduction in the effectiveness of physical or cyber security protection mechanisms, or facilitation of a terrorist attack on critical infrastructures and key resources. Accordingly, the system security categorization should be carefully determined when a loss of confidentiality, integrity, or availability will result in a negative impact on the critical infrastructures and key resources.

The *Critical Information Infrastructure Act of 2002*, Public Law 107-296 §§ 211-215 of November 25, 2002 (codified as 6 U.S.C. 131-134), defines the term "critical infrastructure information" to mean information not customarily in the public domain and related to the security of critical infrastructure or protected systems. Should information types be aligned with Critical Infrastructures, then action should be taken to ensure compliance with Homeland Security Presidential Directive No. 7 (HSPD 7) and to initiate an interdependency analysis.

### *Privacy Information*

*The E-Government Act of 2002* complements privacy protection requirements of the *Privacy Act of 1974*. Under the terms of these public laws, Federal government agencies have specific responsibilities regarding collection, dissemination or disclosure of information regarding individuals.[19]

The September 26, 2003 OMB Memorandum M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," puts the privacy provisions of the E-Government Act of 2002 into effect. The guidance applies to information that identifies individuals in a recognizable form, including name, address, telephone number, Social Security Number, and e-mail addresses. OMB instructed agency heads "to describe how the government handles information that individuals provide electronically, so that the American public has assurances that personal information is protected." Under these public laws and executive policies, it is necessary to broaden the definition of "unauthorized disclosure" to encompass *any* access, use, disclosure, or sharing of privacy-protected information among Federal government agencies when such actions are prohibited by privacy laws and policies. Since most privacy regulations focus on access, use, disclosure, or sharing of information, privacy considerations are dealt with in this guideline as special factors affecting the confidentiality impact level. In establishing confidentiality impact levels for each information type, responsible parties must consider the consequences of unauthorized disclosure of privacy information (with respect to violations of Federal policy and/or law).

Agencies are required to conduct Privacy Impact Assessments (PIAs) before developing IT systems that contain personally identifiable information or before collecting personally identifiable information electronically. The impact of privacy violations should consider any adverse effects experienced by individuals or organizations as a result of the loss of PII confidentiality. Examples of adverse effects experienced by individuals may include blackmail, identity theft, discrimination, or emotional distress. Examples of adverse effects experienced by organizations may include administrative burden, financial losses, loss of public reputation and confidence, and the penalties associated with violation of the relevant statutes and policies.

Categorizations should be reviewed to ensure that the adverse effects of a loss of PII confidentiality have been adequately factored into impact determinations. The confidentiality impact level should generally fall into the ***moderate*** range.

***Trade Secrets***

There are several laws that specifically prohibit unauthorized disclosure of trade secrets (e.g., 7 U.S.C., Chapter 6, Subchapter II, Section 136h and 42 U.S.C., Chapter 6A, Subchapter XII, Part E, Section 300j-4(d)(1)). Systems that store, communicate, or process trade secrets will generally be assigned at least a ***moderate*** confidentiality impact level.

#### 4.4.3 Overall Information System Impact

Since the impact values (i.e., levels) for confidentiality, integrity, and availability may not always be the same for a particular information system, the high water mark concept[20] is used to

[19] The OMB definition of an individual is, "a citizen of the United States or an alien lawfully admitted for permanent residence." Agencies may choose to extend the protections of the Privacy Act and E-Government Act to businesses, sole proprietors, aliens, etc.

determine the overall impact level of the information system. The security impact level for an information system will generally be the highest impact level for the security objectives (confidentiality, integrity, and availability) associated with the aggregate of system information types. Thus, a low-impact system is defined as an information system in which all three of the security objectives are low. A moderate-impact system is an information system in which at least one of the security objectives is moderate and no security objective is greater than moderate. And finally, a high-impact system is an information system in which at least one security objective is high.

## 4.5 Documenting the Security Categorization Process

Essential to the security categorization process is documenting the research, key decisions and approvals, and supporting rationale driving the information system security categorization. This information is key to supporting the security life cycle and will need to be included in the information system's security plan.

Figure 3 provides an example of information details that should be collected.

[20] The high water mark concept is employed because there are significant dependencies among the security objectives of confidentiality, integrity, and availability. In most cases, a compromise in one security objective ultimately affects the other security objectives as well.

| **Information System Name: SCADA System [and Agency specific identifier]** | | | |
|---|---|---|---|
| **Business and Mission Supported:** The SCADA (supervisory control and data acquisition) system provides real-time control and information supporting the main power plant. The power plant provides critical distribution of electric power to the military installation. | | | |
| **Information Types** | | | |
| [D.7.1] Energy Supply | Sensor data monitoring the availability of energy for the Military installation and its soldiers and command authority. This function includes control of distribution and transfer of power. The SCADA remote control capabilities can take action such as initiating necessary switching actions to alleviate an overloading power condition. The impacts to this information and the SCADA system may affect the installation's critical infrastructures. | | |
| [C.2.8.12]General Information | The SCADA information system processes routine administrative information. | | |
| **Step 1** | **Step 2 [Provisional] / Step 3a [Adjustments]** | | |
| **Identify Information Types** | **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| | **Step 3b- Impact Adjustment Justification** | | |
| Energy Supply | L / M | L / H | L / H |
| | Disclosure of sensor information may seriously impact the missions if indications & warnings of overall capability are provided to an adversary. | Severe impacts or consequences may occur if adversarial modification of information results in incorrect power system regulation or control actions. | Due to loss of availability, severe impact to the mission capability may result and may in-turn have overall catastrophic consequences for the facility's critical infrastructures and possible loss of human life. |
| General Information | L | L | L |
| | No adjustments | No adjustments | No adjustments |
| **Step 4 System Categorization:** | **Moderate** | **High** | **High** |
| | **Overall Information System Impact: High** | | |

**Figure 3: Security Categorization Information Collection**

In addition, agencies may consider enhancing their SSPs with other analyses, decisions, assignments, and or approvals that were used in the categorization process. Examples may include:

- Agency's business and mission areas (Step 1 in Table 1)
- Legislative and executive information mandates affecting the information impact assignment or adjustment (Section 4.1.3)
- Indicating whether the information is time-critical in rationales for assigning availability impact levels (Section 4.2.2.3)
- Rationales for assigning information to the General Information Type (Section 4.1.2, Implementation Tip)
- Results of reviews of the appropriateness of the provisional impact levels for information (Section 4.3)

- Results of considering the potential impacts to other organizations and considering, “in accordance with the USA Patriot Act of 2001 and Homeland Security Presidential Directives, potential national-level impacts in categorizing the information system” (NIST SP 800-53 security control RA-2)
- Results of reviewing the identified security categorizations for the aggregate of information types (Step 4 in Table 1)
- Effects of various factors and circumstances (e.g., data aggregation, critical system functionality, privacy, trade secrets, critical infrastructure, aggregation, critical system functionality, extenuating circumstances) on the system category (Section 4.4.2)
- Whether and why the agency determined that the system impact level must be higher than any of the levels of the information types that the system processes (Section 4.4)
- Approvals of all determinations or decisions (Step 4 in Table 1)

## 4.6 Uses of Categorization Information

The results of system security categorization can and should be used by, or made available to, appropriate agency personnel to support agency activities including:

- Business Impact Analysis (BIA): Agency personnel should consider the cross-utilization of security categorization and BIA information in the performance of each activity. Their common objectives enable agencies to mutually draw from them, thus, providing checks and balances to ensure accuracy for each information system. Conflicting information and anomalous conditions, such as a low availability impact and a BIA three-hour recovery time objective, should trigger a reevaluation by the mission and data owners.
- Capital Planning and Investment Control (CPIC) and Enterprise Architecture (EA): Just as no IT investment should be made without a business-approved architecture,[21] the security categorization that begins the security life cycle is a business-enabling activity directly feeding the enterprise architecture and CPIC processes for new investments, as well as migration and upgrade decisions. Specifically, the security categorization can provide a firm basis for justifying certain capital expenditures and also can provide analytical input to avoid unnecessary investments.
- System Design: Understanding and designing the system architecture with varying information sensitivity levels in mind may assist in achieving economies of scale with security services and protection through common security zones within the enterprise. For example, an information system containing privacy information may be located in one security zone with other information systems containing similar sensitive information. Each zone may have varying levels of security. For instance, the more critical zones may require 3-factor authentication where the open area may only require normal access controls. This type of approach requires a solid understanding of an agency’s information and data types gained through the security categorization process.

[21] FEA Consolidated Reference Model Document Version 2.3, October 2007

- Contingency and Disaster Recovery Planning: Contingency and disaster recovery planning personnel should review information systems that have multiple data types of varying impact levels and consider grouping applications with similar information system impact levels with sufficiently protected infrastructures. This ensures efficient application of the correct contingency and disaster protection security controls and avoids the over protection of lower impact information systems.
- Information Sharing and System Interconnection Agreements: Agency personnel should utilize aggregated and individual security categorization information when assessing interagency connections. For example, knowing that information processed on a high impact information system is flowing to another agency's moderate impact information system should cause both agencies to evaluate the security categorization information, the implemented or resulting security controls, and the risk associated with interconnecting systems. The results of this evaluation may substantiate the need for additional security controls in the form of a Service Level Agreement, information systems upgrades, additional mitigating security controls, or alternative means of sharing the required information.

# APPENDIX A: GLOSSARY OF TERMS

Accreditation

The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. [FIPS 200, NIST SP 800-37]

Accreditation Boundary

All components of an information system to be accredited by an authorizing official and excludes separately accredited systems to which the information system is connected. Synonymous with the term security perimeter defined in CNSS Instruction 4009 and DCID 6/3. [NIST SP 800-37]

Accrediting Authority

See Authorizing Official.

Agency

An executive department specified in 5 U.S.C., Sec. 101; a military department specified in 5 U.S.C., Sec. 102; an independent establishment as defined in 5 U.S.C., Sec. 104(1); and a wholly owned Government corporation fully subject to the provisions of 31 U.S.C., Chapter 91. [41 U.S.C., Sec. 403]

Authentication

Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. [FIPS 200]

Authenticity

The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. See authentication.

Authorizing Official

Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. Synonymous with Accreditation Authority. [FIPS 200, NIST SP 800-37]

Availability

Ensuring timely and reliable access to and use of information. [44 U.S.C., Sec. 3542]

Business Areas

"Business areas" separate government operations into high-level categories relating to the purpose of government, the mechanisms the government uses to achieve its purposes, the support functions necessary to conduct government operations, and resource management functions that support all areas of the government's business. "Business areas" are subdivided into "areas of operation" or "lines of business." The recommended information types provided in NIST SP 800-60 are established from the "business areas" and "lines of business" from OMB's Business Reference Model (BRM) section of *Federal Enterprise Architecture (FEA) Consolidated Reference Model Document Version 2.3*

Certification

A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. [FIPS 200, NIST SP 800-37]

Chief Information Officer

Agency official responsible for:
(i) Providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, Executive Orders, directives, policies, regulations, and priorities established by the head of the agency;
(ii) Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and
(iii) Promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency. [PL 104-106, Sec. 5125(b)]

Classified Information

Information that has been determined pursuant to Executive Order (E.O.) 13292 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

Command and Control
The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission.

Confidentiality
Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., Sec. 3542]

Counterintelligence
Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities.

Criticality
A measure of the degree to which an organization depends on the information or information system for the success of a mission or of a business function.

Cryptologic
Of or pertaining to cryptology.

Cryptology
The science that deals with hidden, disguised, or encrypted communications. It includes communications security and communications intelligence.

Executive Agency
An executive department specified in 5 U.S.C., Sec. 101; a military department specified in 5 U.S.C., Sec.102; an independent establishment as defined in 5 U.S.C., Sec. 104(1); or a wholly owned government corporation fully subject to the provisions of 31 U.S.C., Chapter 91. [41 U.S.C., Sec. 403]

Federal Enterprise Architecture [FEA Program Management Office]
A business-based framework for government-wide improvement developed by the Office of Management and Budget that is intended to facilitate efforts to transform the federal government to one that is citizen-centered, results-oriented, and market-based.

Federal Information System
An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency. [40 U.S.C., Sec. 11331]

General Support System

An interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people. [OMB Circular A-130, Appendix III]

High-Impact System

An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of high. [FIPS 200]

Impact

The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.

Independent Regulatory Agency

The Board of Governors of the Federal Reserve System, the Commodity Futures Trading Commission, the Consumer Product Safety Commission, the Federal Communications Commission, the Federal Deposit Insurance Corporation, the Federal Energy Regulatory Commission, the Federal Housing Finance Board, the Federal Maritime Commission, the Federal Trade Commission, the Interstate Commerce Commission, the Mine Enforcement Safety and Health Review Commission, the National Labor Relations Board, the Nuclear Regulatory Commission, the Occupational Safety and Health Review Commission, the Postal Rate Commission, the Securities and Exchange Commission, and any other similar agency designated by statute as a Federal independent regulatory agency or commission.

Individual

A citizen of the United States or an alien lawfully admitted for permanent residence. Agencies may, consistent with individual practice, choose to extend the protections of the Privacy Act and E-Government Act to businesses, sole proprietors, aliens, etc.

Information

An instance of an information type. [FIPS 199]

Information Owner

Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. [CNSS Inst. 4009]

Information Resources

Information and related resources, such as personnel, equipment, funds, and information technology. [44 U.S.C., Sec. 3502]

Information Security

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. [44 U.S.C., Sec. 3542]

Information System

A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. [44 U.S.C., Sec. 3502; OMB Circular A-130, Appendix III]

Information System Owner (or Program Manager)

Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. [CNSS Inst. 4009, Adapted]

Information System Security Officer

Individual assigned responsibility by the senior agency information security officer, authorizing official, management official, or information system owner for maintaining the appropriate operational security posture for an information system or program. [CNSS Inst. 4009, Adapted]

Information Technology

Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources. [40 U.S.C., Sec. 1401]

Information Type

A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or in some instances, by a specific law, Executive Order, directive, policy, or regulation. [FIPS 199]

Integrity

Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., Sec. 3542]

Intelligence

(i) the product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas; or

(ii) information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding. The term 'intelligence' includes foreign intelligence and counterintelligence.

Intelligence Activities

The term 'intelligence activities' includes all activities that agencies within the Intelligence Community are authorized to conduct pursuant to Executive Order 12333, United States Intelligence Activities.

Intelligence Community

The term 'intelligence community' refers to the following agencies or organizations:

(i) The Central Intelligence Agency (CIA);
(ii) The National Security Agency (NSA);
(iii) The Defense Intelligence Agency (DIA);
(iv) The offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs;
(v) The Bureau of Intelligence and Research of the Department of State;
(vi) The intelligence elements of the Army, Navy, Air Force, and Marine Corps, the Federal Bureau of Investigation (FBI), the Department of the Treasury, and the Department of Energy; and
(vii) The staff elements of the Director of Central Intelligence.

Lines of Business

“Lines of business” or “areas of operation” describe the purpose of government in functional terms or describe the support functions that the government must conduct in order to effectively deliver services to citizens. *Lines of business* relating to the purpose of government and the mechanisms the government uses to achieve its purposes tend to be mission-based. *Lines of business* relating to support functions and resource management functions that are necessary to conduct government operations tend to be common to most agencies. The recommended information types provided in NIST SP 800-60 are established from the “business areas” and “lines of business” from OMB’s Business Reference Model (BRM) section of *Federal Enterprise Architecture (FEA) Consolidated Reference Model Document Version 2.3*

Low-Impact System

An information system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS 199 potential impact value of low. [FIPS 200]

Mission Critical

Any telecommunications or information system that is defined as a *national security system* (FISMA) or processes any information the loss, misuse, disclosure, or unauthorized access to or modification of, would have a debilitating impact on the mission of an agency.

Moderate-Impact System

An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of moderate and no security objective is assigned a FIPS 199 potential impact value of high. [FIPS 200]

National Security Information

Information that has been determined pursuant to Executive Order 12958 as amended by Executive Order 13292, or any predecessor order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status.

National Security System

Any information system (including any telecommunications system) used or operated by an agency or by a contractor on behalf of an agency, or any other organization on behalf of an agency –

(i) the function, operation, or use of which: involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapon system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example payroll, finance, logistics, and personnel management applications); or

(ii) is protected at all times by procedures established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. [44 U.S.C., Sec. 3542]

Non-repudiation

Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender’s identity, so neither can later deny having processed the information. [CNSS Inst. 4009 Adapted]

Potential Impact

The loss of confidentiality, integrity, or availability could be expected to have: (i) a limited adverse effect (FIPS 199 low); (ii) a serious adverse effect (FIPS 199 moderate); or (iii) a severe or catastrophic adverse effect (FIPS 199 high) on organizational operations, organizational assets, or individuals. [FIPS 199]

Privacy Impact Assessment (PIA)

An analysis of how information is handled:

(i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy;

(ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and

(iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. [OMB Memorandum 03-22]

Public Information

Any information, regardless of form or format that an agency discloses, disseminates, or makes available to the public.

Risk

The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring. [FIPS 200, Adapted]

Security Category

The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, individuals, other organizations, or the Nation. [FIPS 199, Adapted]

Security Controls

The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. [FIPS 199]

Security Objectives

Confidentiality, integrity, and availability.[FIPS 199]

Senior Agency Information Security Officer

Official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers. [44 U.S.C., Sec. 3544]

Sensitivity

Used in this guideline to mean a measure of the importance assigned to information by its owner, for the purpose of denoting its need for protection.

Sub-functions

*Sub-functions* are the basic operations employed to provide the system services within each area of operations or line of business. The recommended information types provided in NIST SP 800-60 are established from the “business areas” and “lines of business” from OMB’s Business Reference Model (BRM) section of *Federal Enterprise Architecture (FEA) Consolidated Reference Model Document Version 2.3*

System

See Information System.

Telecommunications

The transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received.

Threat

Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets,  individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. [CNSS Inst. 4009, Adapted]

Vulnerability

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. [CNSS Inst. 4009, Adapted]

Weapons System

A combination of one or more weapons with all related equipment, materials, services, personnel, and means of delivery and deployment (if applicable) required for self-sufficiency.

# APPENDIX B: REFERENCES

S. 3418 [5 U.S.C. § 552A through Public Law 93-579], 93rd U.S. Cong., 2d Sess., *The Privacy Act of 1974,* December 31, 1974 (effective September 27, 1975).

S. 244 [Public Law 104-13], 104th U.S. Cong., 1t Sess., *Paperwork Reduction Act of 1995*, May 22, 1995.

S. 1124, Division E [Public Law 104-106], 104th U.S. Cong., 2d Sess., *Information Technology Management Reform Act of 1996,* February 10, 1996.

H.R. 3162, Titles VII and Title IX [Public Law 107-56], 107th U.S. Cong., 1t Sess., *The USA PATRIOT Act of 2001,* October 26, 2001.

Public Law 107-296, *Critical Information Infrastructure Act of 2002*, §§211-215, November 25, 2002.

H.R. 2458 [Public Law 107-347], 107th U.S. Cong., 2d Sess., *E-Government Act of 2002*, December 17, 2002.

H.R. 2458, Title III [Public Law 107-347], 107th U.S. Cong., 2d Sess., *Federal Information Security Management Act of 2002*, December 17, 2002.

Executive Office of the President, *Presidential Decision Directive 63, Protecting America's Critical Infrastructures,* May 22, 1998.

United States Office of Management and Budget, Circular No. A-130, Appendix III, Transmittal Memorandum #4, *Management of Federal Information Resources*, November 2000.

United States Office of Management and Budget, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, September 29, 2003.

United States Office of Management and Budget (OMB), Federal Enterprise Architecture (FEA) Program Management Office (PMO), *FEA Consolidated Reference Model 2.3*, October 2007.

United States Department of Commerce, National Institute of Standards and Technology, Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, December 2003.

United States Department of Commerce, National Institute of Standards and Technology, Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.

United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-18, *Guide for Developing Security Plans for Federal Information Systems*, Revision 1, February 2006.

United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, July 2002.

United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-34, *Contingency Planning Guide for Information Technology Systems*, June 2002.

United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004.

United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-39, *Draft Managing Risk from Information Systems: An Organizational Perspective*, April 2008.

United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, Revision 2, December 2007.

United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems,* July 2008.

United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003.

United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-64, *Security Considerations in the Information System Development Life Cycle,* June 2004.

NIST Special Publication 800-60 Volume II
Revision 1

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

# Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories

**Kevin Stine**
**Rich Kissel**
**William C. Barker**
**Annabelle Lee**
**Jim Fahlsing**

## INFORMATION SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

**August 2008**

U.S. DEPARTMENT OF COMMERCE
*Carlos M. Gutierrez, Secretary*

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
*James M. Turner, Deputy Director*

## Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. This Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

## Authority

This document has been developed by the National Institute of Standards and Technology (NIST) to further its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, P.L. 107-347. NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems, as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in A-130, Appendix III.

This guideline has been prepared for use by federal agencies. It may also be used by nongovernmental organizations on a voluntary basis and is not subject to copyright. (Attribution would be appreciated by NIST.)

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official.

NIST Special Publication 800-60 Volume II, Revision 1, 304 pages
**(Date) CODEN: NSPUE2**

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There are references in this publication to documents currently under development by NIST in accordance with responsibilities assigned to NIST under the Federal Information Security Management Act of 2002. The methodologies in this document may be used even before the completion of such companion documents. Thus, until such time as each document is completed, current requirements, guidelines, and procedures (where they exist) remain operative. For planning and transition purposes, agencies may wish to closely follow the development of these new documents by NIST. Individuals are also encouraged to review the public draft documents and offer their comments to NIST. All NIST documents mentioned in this publication, other than the ones noted above, are available at http://csrc.nist.gov/publications.

## Acknowledgements

The authors wish to thank their colleagues who helped update this document, prepare drafts, and review materials.  In addition, special thanks are due to our reviewers who greatly contributed to the document’s development.  The authors also gratefully acknowledge and appreciate the many comments from the public and private sectors whose thoughtful and constructive comments improved the quality and usefulness of this publication.

## Note

NIST Special Publication (SP) 800-60 may be used by organizations in conjunction with a family of security-related publications including:

- FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems;*
- FIPS Publication 200, *Minimum Security Controls for Federal Information Systems*;
- NIST SP 800-30, *Risk Management Guide for Information Technology Systems*[1];
- NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems;*
- NIST Draft SP 800-39, *Managing Risk from Information Systems: An Organizational Perspective;*
- NIST SP 800-53, *Recommended Security Controls for Federal Information Systems;*
- NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*; and
- NIST SP 800-59, *Guideline for Identifying an Information System as a National Security System*.

This series of nine documents is intended to provide a structured, yet flexible framework for selecting, specifying, employing, and evaluating the security controls in Federal information systems—and thus, make a significant contribution toward satisfying the requirements of the Federal Information Security Management Act (FISMA) of 2002. While the publications are mutually reinforcing and have some dependencies, in most cases, they can be effectively used independently of one another.

This is Volume II of two volumes. Volume I contains the basic guidelines for mapping types of information and information systems to security categories. The appendices contained in Volume II include security categorization recommendations and rationale for mission-based and management and support information types.

The SP 800-60 information types and security impact levels are based on the OMB Federal Enterprise Architecture Program Management Office's October 2007 *FEA Consolidated Reference Model Document, Version 2.3* inputs from participants in NIST SP 800-60 workshops, and FIPS 199. Rationale for the example security impact level recommendations provided in the appendices have been derived from multiple sources, and as such, will require several iterations of review, comment, and subsequent modification to achieve consistency in terminology, structure, and content.

[1] This document is currently under revision and will be reissued as Special Publication 800-30, Revision 1, *Guide for Conducting Risk Assessments*.

# EXECUTIVE SUMMARY

Title III of the E-Government Act (Public Law 107-347), titled the Federal Information Security Management Act (FISMA), tasked the National Institute of Standards and Technology (NIST) to develop:

- Standards to be used by all Federal agencies to categorize all information and information systems collected or maintained by or on behalf of each agency based on the objectives of providing appropriate levels of information security according to a range of risk levels;
- Guidelines recommending the types of information and information systems to be included in each such category; and
- Minimum information security requirements (i.e., management, operational, and technical security controls), for information and information systems in each such category.

In response to the second of these tasks, this guideline has been developed to assist Federal government agencies to categorize information and information systems. The guideline's objective is to facilitate provision of appropriate levels of information security according to a range of levels of impact or consequences that might result from the unauthorized disclosure, modification, or loss of availability of the information or information system. This guideline assumes that the user is familiar with *Standards for Security Categorization of Federal Information and Information Systems* (FIPS 199). The guideline and its appendices:

- Review the security categorization terms and definitions established by FIPS 199;
- Recommend a security categorization process;
- Describe a methodology for identifying types of Federal information and information systems;
- Suggest provisional security impact levels for common information types;
- Discuss information attributes that may result in variances from the provisional security impact level assignment; and
- Describe how to establish a system security categorization based on the system's use, connectivity, and aggregate information content.

This document is intended as a reference resource rather than as a tutorial. Not all of the material will be relevant to all agencies. This document includes two volumes, a basic guideline and a volume of appendices. Users should review the guidelines provided in Volume I, then refer to only that specific material from the appendices that applies to their own systems and applications.

The provisional security impact level assignments contained in appendices C and D are only the first step in impact assignment and subsequent risk assessment processes. The impact assignments are not intended to be used by auditors as a definitive checklist for information types and impact assignments.

The basis employed in this guideline for the identification of information types is the Office of Management and Budget's Federal Enterprise Architecture (FEA) Program Management Office (PMO) October 2007 publication, *The Consolidated Reference Model Document Version 2.3*.

# GUIDE FOR MAPPING TYPES OF INFORMATION AND INFORMATION SYSTEMS TO SECURITY CATEGORIES

## Volume II: Appendices

## Table of Contents

## APPENDIX A: GLOSSARY OF TERMS

Accreditation
The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. [FIPS 200, NIST SP 800-37]

Accreditation Boundary
All components of an information system to be accredited by an authorizing official and excludes separately accredited systems to which the information system is connected. Synonymous with the term security perimeter defined in CNSS Instruction 4009 and DCID 6/3. [NIST SP 800-37]

Accrediting Authority
See Authorizing Official.

Agency
An executive department specified in 5 U.S.C., Sec. 101; a military department specified in 5 U.S.C., Sec. 102; an independent establishment as defined in 5 U.S.C., Sec. 104(1); and a wholly owned Government corporation fully subject to the provisions of 31 U.S.C., Chapter 91. [41 U.S.C., Sec. 403]

Authentication
Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. [FIPS 200]

Authenticity
The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. See authentication.

Authorizing Official
Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. Synonymous with Accreditation Authority. [FIPS 200, NIST SP 800-37]

Availability
Ensuring timely and reliable access to and use of information. [44 U.S.C., Sec. 3542]

Business Areas

"Business areas" separate government operations into high-level categories relating to the purpose of government, the mechanisms the government uses to achieve its purposes, the support functions necessary to conduct government operations, and resource management functions that support all areas of the government's business. "Business areas" are subdivided into "areas of operation" or "lines of business." The recommended information types provided in NIST SP 800-60 are established from the "business areas" and "lines of business" from OMB's Business Reference Model (BRM) section of *Federal Enterprise Architecture (FEA) Consolidated Reference Model Document Version 2.3*

Certification

A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. [FIPS 200, NIST SP 800-37]

Chief Information Officer

Agency official responsible for:
(i) Providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, Executive Orders, directives, policies, regulations, and priorities established by the head of the agency;
(ii) Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and
(iii) Promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency. [PL 104-106, Sec. 5125(b)]

Classified Information

Information that has been determined pursuant to E.O. 13292 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

Command and Control

The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission.

Confidentiality

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., Sec. 3542]

Counterintelligence

Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities.

Criticality

A measure of the degree to which an organization depends on the information or information system for the success of a mission or of a business function.

Cryptologic

Of or pertaining to cryptology.

Cryptology

The science that deals with hidden, disguised, or encrypted communications. It includes communications security and communications intelligence.

Executive Agency

An executive department specified in 5 U.S.C., Sec. 101; a military department specified in 5 U.S.C., Sec.102; an independent establishment as defined in 5 U.S.C., Sec. 104(1); or a wholly owned government corporation fully subject to the provisions of 31 U.S.C., Chapter 91. [41 U.S.C., Sec. 403]

Federal Enterprise Architecture
[FEA Program Management Office]

A business-based framework for government-wide improvement developed by the Office of Management and Budget that is intended to facilitate efforts to transform the federal government to one that is citizen-centered, results-oriented, and market-based.

Federal Information System

An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency. [40 U.S.C., Sec. 11331]

General Support System

An interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people. [OMB Circular A-130, Appendix III]

High-Impact System

An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of high. [FIPS 200]

Impact

The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.

Independent Regulatory Agency

The Board of Governors of the Federal Reserve System, the Commodity Futures Trading Commission, the Consumer Product Safety Commission, the Federal Communications Commission, the Federal Deposit Insurance Corporation, the Federal Energy Regulatory Commission, the Federal Housing Finance Board, the Federal Maritime Commission, the Federal Trade Commission, the Interstate Commerce Commission, the Mine Enforcement Safety and Health Review Commission, the National Labor Relations Board, the Nuclear Regulatory Commission, the Occupational Safety and Health Review Commission, the Postal Rate Commission, the Securities and Exchange Commission, and any other similar agency designated by statute as a Federal independent regulatory agency or commission.

Individual

A citizen of the United States or an alien lawfully admitted for permanent residence. Agencies may, consistent with individual practice, choose to extend the protections of the Privacy Act and E-Government Act to businesses, sole proprietors, aliens, etc.

Information

An instance of an information type. [FIPS 199]

Information Owner

Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. [CNSS Inst. 4009]

Information Resources

Information and related resources, such as personnel, equipment, funds, and information technology. [44 U.S.C., Sec. 3502]

Information Security

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. [44 U.S.C., Sec. 3542]

Information System

A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. [44 U.S.C., Sec. 3502; OMB Circular A-130, Appendix III]

Information System Owner (or Program Manager)

Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. [CNSS Inst. 4009, Adapted]

Information System Security Officer

Individual assigned responsibility by the senior agency information security officer, authorizing official, management official, or information system owner for maintaining the appropriate operational security posture for an information system or program. [CNSS Inst. 4009, Adapted]

Information Technology

Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources. [40 U.S.C., Sec. 1401]

Information Type

A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or in some instances, by a specific law, Executive Order, directive, policy, or regulation. [FIPS 199]

Integrity

Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., Sec. 3542]

Intelligence

(i) the product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas; or
(ii) information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding. The term 'intelligence' includes foreign intelligence and counterintelligence.

Intelligence Activities

The term 'intelligence activities' includes all activities that agencies within the Intelligence Community are authorized to conduct pursuant to Executive Order 12333, United States Intelligence Activities.

Intelligence Community

The term 'intelligence community' refers to the following agencies or organizations:
(i) The Central Intelligence Agency (CIA);
(ii) The National Security Agency (NSA);
(iii) The Defense Intelligence Agency (DIA);
(iv) The offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs;
(v) The Bureau of Intelligence and Research of the Department of State;
(vi) The intelligence elements of the Army, Navy, Air Force, and Marine Corps, the Federal Bureau of Investigation (FBI), the Department of the Treasury, and the Department of Energy; and
(vii) The staff elements of the Director of Central Intelligence.

Lines of Business

“Lines of business” or “areas of operation” describe the purpose of government in functional terms or describe the support functions that the government must conduct in order to effectively deliver services to citizens. *Lines of business* relating to the purpose of government and the mechanisms the government uses to achieve its purposes tend to be mission-based. *Lines of business* relating to support functions and resource management functions that are necessary to conduct government operations tend to be common to most agencies. The recommended information types provided in NIST SP 800-60 are established from the “business areas” and “lines of business” from OMB’s Business Reference Model (BRM) section of *Federal Enterprise Architecture (FEA) Consolidated Reference Model Document Version 2.3*

Low-Impact System

An information system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS 199 potential impact value of low. [FIPS 200]

Mission Critical

Any telecommunications or information system that is defined as a *national security system* (FISMA) or processes any information the loss, misuse, disclosure, or unauthorized access to or modification of, would have a debilitating impact on the mission of an agency.

Moderate-Impact System

An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of moderate and no security objective is assigned a FIPS 199 potential impact value of high. [FIPS 200]

National Security Information

Information that has been determined pursuant to Executive Order 12958 as amended by Executive Order 13292, or any predecessor order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status.

National Security System

Any information system (including any telecommunications system) used or operated by an agency or by a contractor on behalf of an agency, or any other organization on behalf of an agency –

(i) the function, operation, or use of which: involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapon system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example payroll, finance, logistics, and personnel management applications); or

(ii) is protected at all times by procedures established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. [44 U.S.C., Sec. 3542]

Non-repudiation

Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender’s identity, so neither can later deny having processed the information. [CNSS Inst. 4009 Adapted]

Potential Impact

The loss of confidentiality, integrity, or availability could be expected to have: (i) a limited adverse effect (FIPS 199 low); (ii) a serious adverse effect (FIPS 199 moderate); or (iii) a severe or catastrophic adverse effect (FIPS 199 high) on organizational operations, organizational assets, or individuals. [FIPS 199]

Privacy Impact Assessment (PIA)

An analysis of how information is handled:

(i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy;

(ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and

(iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. [OMB Memorandum 03-22]

Public Information

Any information, regardless of form or format that an agency discloses, disseminates, or makes available to the public.

Risk

The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring. [FIPS 200, Adapted]

Security Category

The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, individuals, other organizations, or the Nation. [FIPS 199, Adapted]

Security Controls

The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. [FIPS 199]

Security Objectives

Confidentiality, integrity, and availability.[FIPS 199]

Senior Agency Information Security Officer

Official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer’s primary liaison to the agency’s authorizing officials, information system owners, and information system security officers. [44 U.S.C., Sec. 3544]

Sensitivity
Used in this guideline to mean a measure of the importance assigned to information by its owner, for the purpose of denoting its need for protection.

Sub-functions
*Sub-functions* are the basic operations employed to provide the system services within each area of operations or line of business. The recommended information types provided in NIST SP 800-60 are established from the “business areas” and “lines of business” from OMB’s Business Reference Model (BRM) section of *Federal Enterprise Architecture (FEA) Consolidated Reference Model Document Version 2.3*

System
See Information System.

Telecommunications
The transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received.

Threat
Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. [CNSS Inst. 4009, Adapted]

Vulnerability
Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. [CNSS Inst. 4009, Adapted]

Weapons System
A combination of one or more weapons with all related equipment, materials, services, personnel, and means of delivery and deployment (if applicable) required for self-sufficiency.

# APPENDIX B: REFERENCES

S. 3418 [5 U.S.C. § 552A through Public Law 93-579], 93rd U.S. Cong., 2d Sess., *The Privacy Act of 1974*, December 31, 1974 (effective September 27, 1975).

S. 244 [Public Law 104-13], 104th U.S. Cong., 1t Sess., *Paperwork Reduction Act of 1995*, May 22, 1995.

S. 1124, Division E [Public Law 104-106], 104th U.S. Cong., 2d Sess., *Information Technology Management Reform Act of 1996*, February 10, 1996.

H.R. 3162, Titles VII and Title IX [Public Law 107-56], 107th U.S. Cong., 1t Sess., *The USA PATRIOT Act of 2001*, October 26, 2001.

Public Law 107-296, *Critical Information Infrastructure Act of 2002*, §§211-215, November 25, 2002.

H.R. 2458 [Public Law 107-347], 107th U.S. Cong., 2d Sess., *E-Government Act of 2002*, December 17, 2002.

H.R. 2458, Title III [Public Law 107-347], 107th U.S. Cong., 2d Sess., *Federal Information Security Management Act of 2002*, December 17, 2002.

Executive Office of the President, *Presidential Decision Directive 63, Protecting America's Critical Infrastructures*, May 22, 1998.

United States Office of Management and Budget, Circular No. A-130, Appendix III, Transmittal Memorandum #4, *Management of Federal Information Resources*, November 2000.

United States Office of Management and Budget, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, September 29, 2003.

United States Office of Management and Budget (OMB), Federal Enterprise Architecture (FEA) Program Management Office (PMO), *FEA Consolidated Reference Model 2.3*, October 2007.

United States Department of Commerce, National Institute of Standards and Technology, Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, December 2003.

United States Department of Commerce, National Institute of Standards and Technology, Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.

United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-18, *Guide for Developing Security Plans for Federal Information Systems*, Revision 1, February 2006.

United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, July 2002.

United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-34, *Contingency Planning Guide for Information Technology Systems*, June 2002.

United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems,* May 2004.

United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-39, *Draft Managing Risk from Information Systems: An Organizational Perspective*, April 2008.

United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, Revision 2, December 2007.

United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems,* July 2008.

United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003.

United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-64, *Security Considerations in the Information System Development Life Cycle,* June 2004.

# APPENDIX C: MANAGEMENT AND SUPPORT INFORMATION AND INFORMATION SYSTEMS IMPACT LEVELS

Much Federal government information and many systems are not employed directly to provide services to citizens, but are primarily intended to provide administrative or business services that support mission accomplishment. Volume I, Section 4.1.2, "Identification of Management and Support Information," suggests a set of information types for *management and support* information as based on Office of Management and Budget's (OMB) Federal Enterprise Architecture (FEA) Business Reference Model (BRM) described in the *FEA Consolidated Reference Model Document Version 2.3*, dated October 2007.

Some of the *management and support* functions executed to support delivery of services or manage government resources are also executed by some agencies in delivering services to citizens. (See especially the "C.2.8 General Government" line of business.) Most of these information types could be included in Appendix D as *mission-based* information types. Because the BRM categorizes them as services delivery support functions, they are included in Volume I Section 4.1.2 and here in Appendix C. In order to reduce repetition, they are not repeated in Appendix D.

Appendix C.1, "Recommended Provisional Impact Levels for Management and Support Information Types," documents impact levels for information types identified in Section 4.1.2. These are provisional levels, subject to review and modification by agency stakeholders. Provisional impact level assignments are only the first step in impact assignment and are reviewed in the subsequent risk assessment processes. They are not designed to be used by auditors as a definitive checklist for information types and impact assignments.

Most information systems employed in both direct services and administrative/management support activities perform one or more of the service delivery support functions described in Appendix C.2, "Rationale and Factors for Services Delivery Support Information." These service support functions are the day-to-day activities necessary to the organizations that provide services to the general population and administrative/management services to government departments and agencies responsible for the provision of those services. As in the case of administrative/business information and information systems, the security objectives and impacts are determined by the direct service missions and constituencies ultimately being supported. It is likely that all Federal government information systems store, process, and operate under the control of information technology (IT) infrastructure maintenance information (e.g., password files and file and network access settings). At least a basic set of security controls will apply to this set of information and processes in order to combat potential corruption, misuse, or abuse of system information and processes.

Information necessary to conduct administrative or business services that support mission accomplishment includes the government resource management information types described in Appendix C.3, "Rationale and Factors for Government Resource Management Information." All of the departments and agencies performing direct service functions are supported by information systems that perform the activities described in Appendix C.3. Many departments and agencies operate their own support systems. Others obtain at least some support services from other organizations. Some agencies' missions are primarily to support other government departments and agencies in the conduct of direct service missions. As indicated above, security objectives and security impact levels for administrative and management information and information systems are determined by the natures of the supported direct services and constituencies being supported.

Much of the discussion of factors affecting assignment of impact level is common to many information types. Because this guideline is intended as a reference document, and it is anticipated that most users will refer only to one or a few information types of interest, several common or similar observations appear with each information type to which they are appropriate. Some impact factors common to all information types are discussed in Volume I, Section 4.2.3 and 4.4.2.

## C.1 Recommended Provisional Impact Levels for Management and Support Information Types

The eight information types associated with *support delivery of services* as well as the five *government resources management information* FEA lines of business are provided in Table C-1. Each of the information types associated sub-functions are detailed in Appendix C.2 and C.3. These management and support functions are the day-to-day activities necessary to provide the critical policy, programmatic, and managerial foundation that support Federal government operations.

**Table C-1: Management and Support Lines of Business and Information Types[2]**

| Services Delivery Support Information | | |
|---|---|---|
| **C.2.1 Controls and Oversight** | **C.2.4 Internal Risk Management & Mitigation** | **C.2.8 General Government** |
| Corrective Action (Policy/Regulation) | | Central Fiscal Operations |
| Program Evaluation | Contingency Planning | Legislative Functions |
| Program Monitoring | Continuity of Operations | Executive Functions |
| **C.2.2 Regulatory Development** | Service Recovery | Central Property Management |
| Policy & Guidance Development | **C.2.5 Revenue Collection** | Central Personnel Management |
| Public Comment Tracking | Debt Collection | Taxation Management |
| Regulatory Creation | User Fee Collection | Central Records & Statistics Management |
| Rule Publication | Federal Asset Sales | |
| **C.2.3 Planning & Budgeting** | **C.2.6 Public Affairs** | *Income Information* |
| Budget Formulation | Customer Services | *Personal Identity and Authentication* |
| Capital Planning | Official Information Dissemination | *Entitlement Event Information* |
| Enterprise Architecture | Product Outreach | *Representative Payee Information* |
| Strategic Planning | Public Relations | *General Information* |
| Budget Execution | **C.2.7 Legislative Relations** | |
| Workforce Planning | Legislation Tracking | |
| Management Improvement | Legislation Testimony | |
| Budgeting & Performance Integration | Proposal Development | |
| Tax & Fiscal Policy | Congressional Liaison Operations | |

[2] The recommended information types provided in NIST SP 800-60 are established from the “business areas” and “lines of business” from OMB’s Business Reference Model (BRM) section of Federal Enterprise Architecture (FEA) Consolidated Reference Model Document Version 2.3, dated October 2007.

**Table C-1: Management and Support Lines of Business and Information Types[2]**

**Government Resource Management Information**

**C.3.1 Administrative Management**

Facilities, Fleet, and Equipment Management
Help Desk Services
Security Management
Travel
Workplace Policy Development & Management

**C.3.2 Financial Management**

Accounting
Funds Control
Payments
Collections and Receivables
Asset and Liability Management
Reporting and Information
Cost Accounting/ Performance Measurement

**C.3.3 Human Resource Management**

HR Strategy
Staff Acquisition
Organization & Position Mgmt
Compensation Management
Benefits Management
Employee Performance Mgmt
Employee Relations
Labor Relations
Separation Management
Human Resources Development

**C.3.4 Supply Chain Management**

Goods Acquisition
Inventory Control
Logistics Management
Services Acquisition

**C.3.5 Information & Technology Management**

System Development
Lifecycle/Change Management
System Maintenance
IT Infrastructure Maintenance
Information Security
Record Retention
Information Management
System and Network Monitoring
Information Sharing

Table C-2 summarizes provisional impact level recommendations for administrative, management, and service information. Provisional impact levels are recommended for each security objective (confidentiality, integrity, availability) and for each *management and support* Federal government information type. The confidentiality, integrity, and availability impact levels define the security category of each information type.

*Implementation Tip*

Most government information systems access, process, and/or disseminate more than one class of information. Security objectives and impacts associated with all of the types of information and processes served by the information system need to be considered in determining the system's information security requirements.

Each information type may include one or more elements. For example, benefits management information includes employee identification information, benefit plan information for insurance and other products, cost information, claims and reimbursement policy information, claims procedures, etc.

In some cases, different impact levels are appropriate for different information elements. For example, elements of program monitoring information relating to remediation of information security vulnerabilities may have a different impact level than elements of program monitoring information relating to an office furniture upgrade.

Each agency that processes an information type may process a distinct combination of elements. The authority and responsibilities assigned to each agency that processes an information type can affect the actual impact level associated with the information within the context of that agency's operations.

In Table C-2, the existence of exceptions to provisional impact assignments are identified by displaying impact assignments in a gray font [**gray font**] and are described as applicable by security objective in the information type descriptions to follow. The specific descriptions are provided under the sub-heading “Special Factors Affecting [Security Objective] Impact Determination.”

Appendices C.2 and C.3 identify information elements and contexts that may result in variances from the basic impact level assignment. For example, some systems process information the compromise of which affect national security, critical infrastructures, or key national assets. Impacts associated with such systems are either outside the scope of this document (i.e., national security information) or may need to be adjusted upward based on the more severe consequences of compromises.

Many of the information types are also lifecycle-dependent. That is, information that requires protection at one stage in system development or operational use of the information is publicly accessible at a later stage or following some event. For example, information that has confidentiality attributes during the period that an agency is using it to make a decision may be public knowledge once the decision has been made (e.g., financial/budgetary information used during development of requests for proposals in procurement actions).

**Table C-2: Type-based Impacts for Federal Information and Information Systems**

**Security Categorization of Management and Support Information**

| | Confidentiality | Integrity | Availability |
|---|---|---|---|
| *Controls and Oversight* | | | |
| Corrective Action (Policy/Regulation) | Low | **Low** | **Low** |
| Program Evaluation | Low | **Low** | **Low** |
| Program Monitoring | Low[3] | Low | Low |
| *Regulatory Development* | | | |
| Policy and Guidance Development | Low | Low | **Low** |
| Public Comment Tracking | **Low** | **Low** | **Low** |
| Regulatory Creation | Low | Low | **Low** |
| Rule Publication | **Low** | **Low** | **Low** |
| *Planning and Budgeting* | | | |
| Budget Formulation | Low | Low | **Low** |
| Capital Planning | Low | Low | **Low** |
| Enterprise Architecture | Low | Low | **Low** |
| Strategic Planning | Low | Low | **Low** |
| Budget Execution | Low | Low | **Low** |
| Workforce Planning | Low | **Low** | **Low** |
| Management Improvement | Low | Low | **Low** |
| Budgeting & Performance Integration | Low | Low | **Low** |
| Tax and Fiscal Policy | Low | Low | **Low** |
| *Internal Risk Management and Mitigation* | | | |
| Contingency Planning | Moderate | **Moderate** | Moderate |
| Continuity of Operations | Moderate | **Moderate** | Moderate |

[3] The confidentiality impact assigned to the Program Monitoring Information Type may necessitate the highest confidentiality impact of the information types processed by the system.

**Security Categorization of Management and Support Information**

| | Confidentiality | Integrity | Availability |
|---|---|---|---|
| Service Recovery | Low | Low | Low |
| *Revenue Collection* | | | |
| Debt Collection | Moderate | Low | Low |
| User Fee Collection | Low | Low | Moderate |
| Federal Asset Sales | Low | Moderate | Low |
| *Public Affairs* | | | |
| Customer Services | Low | Low | Low |
| Official Information Dissemination | Low | Low | Low |
| Product Outreach | Low | Low | Low |
| Public Relations | Low | Low | Low |
| *Legislative Relations* | | | |
| Legislation Tracking | Low | Low | Low |
| Legislation Testimony | Low | Low | Low |
| Proposal Development | Moderate | Low | Low |
| Congressional Liason Operations | Moderate | Low | Low |
| *General Government* | | | |
| Central Fiscal Operations[4] | Moderate | Low | Low |
| Legislative Functions | Low | Low | Low |
| Executive Functions[5] | Low | Low | Low |
| Central Property Management | Low[6] | Low | Low[7] |
| Central Personnel Management | Low | Low | Low |
| Taxation Management | Moderate | Low | Low |
| Central Records and Statistics Management | Moderate | Low | Low |
| Income Information[8] | Moderate | Moderate | Moderate |
| Personal Identity and Authentication[8] | Moderate | Moderate | Moderate |
| Entitlement Event Information[8] | Moderate | Moderate | Moderate |
| Representative Payee Information[8] | Moderate | Moderate | Moderate |
| General Information[9] | Low | Low | Low |

[4] Tax-related functions are associated with the Taxation Management information type.

[5] The OMB Business Reference Model "Executive Function has been expanded to include general agency executive functions as well as Executive Office of the President (EOP) functions. Strictly EOP executive functions are treated in Appendix D, Examples of Impact Determination for Mission-Based Information and Information Systems.

[6] High where safety of major critical infrastructure components or key national assets is at stake.

[7] Moderate or High in emergency situations where time-critical processes affecting human safety or major assets are involved.

[8] The identified information types are not a derivative of OMB's Business Reference Model and were added to address privacy information.

[9] The OMB Business Reference Model does not include a General Information information type. This information type was added as a catch-all information type. As such, agencies may use this to identify additional information types not defined in the BRM and assign impact levels.

### Security Categorization of Management and Support Information

| | Confidentiality | Integrity | Availability |
|---|---|---|---|
| *Administrative Management* | | | |
| Facilities, Fleet, and Equipment Mgmt | Low[6] | Low[7] | Low[7] |
| Help Desk Services | Low | Low | Low |
| Security Management | Moderate | **Moderate** | Low |
| Travel | Low | **Low** | **Low** |
| Workplace Policy Development and Management | **Low** | **Low** | **Low** |
| *Financial Management* | | | |
| Asset and Liability Management | Low | Low | **Low** |
| Reporting and Information | Low | **Moderate** | **Low** |
| Funds Control | Moderate | **Moderate** | **Low** |
| Accounting | Low | Moderate | **Low** |
| Payments | Low | Moderate | Low |
| Collections and Receivables | **Low** | **Moderate** | **Low** |
| Cost Accounting/ Performance Measurement | **Low** | **Moderate** | **Low** |
| *Human Resource Management* | | | |
| HR Strategy | Low | **Low** | **Low** |
| Staff Acquisition | Low | **Low** | **Low** |
| Organization and Position Management | Low | **Low** | **Low** |
| Compensation Management | Low | Low | **Low** |
| Benefits Management | Low | **Low** | **Low** |
| Employee Performance Management | Low | **Low** | **Low** |
| Employee Relations | Low | Low | **Low** |
| Labor Relations | Low | Low | Low |
| Separation Management | Low | **Low** | **Low** |
| Human Resources Development | Low | **Low** | **Low** |
| *Supply Chain Management* | | | |
| Goods Acquisition | Low | Low | Low |
| Inventory Control | Low | **Low** | Low |
| Logistics Management | Low | **Low** | Low |
| Services Acquisition | Low | Low | **Low** |
| *Information & Technology Management* | | | |
| System Development | **Low** | Moderate | **Low** |
| Lifecycle/Change Management | Low | Moderate | **Low** |
| System Maintenance | **Low** | Moderate | **Low** |
| IT Infrastructure Maintenance[10] | Low | Low | Low |
| Information System Security | **Low** | **Moderate** | **Low** |

[10] The confidentiality impact assigned to the IT Infrastructure Maintenance Information Type may necessitate the highest confidentiality impact of the information types processed by the system.

**Security Categorization of Management and Support Information**

| | Confidentiality | Integrity | Availability |
|---|---|---|---|
| Record Retention | **Low** | **Low** | **Low** |
| Information Management[11] | **Low** | **Moderate** | **Low** |
| System and Network Monitoring | **Moderate** | **Moderate** | **Low** |
| Information Sharing | **N/A** | **N/A** | **N/A** |

## C.2 Rationale and Factors for Services Delivery Support Information

Services delivery support functions provide the critical policy, programmatic, and managerial foundation to support Federal government operations. Security objectives and impact levels for service delivery support information and systems are generally determined by the natures of the supported direct services and constituencies being supported. If a system stores, processes, or communicates *national security* information, it is defined as a *national security system*, and is outside the scope of this guideline.[12] Service delivery support activities are defined in this section.

### C.2.1 Controls and Oversight

Controls and Oversight information is used to ensure that the operations and programs of the Federal government and its external business partners comply with applicable laws and regulations and prevent waste, fraud, and abuse.

#### C.2.1.1 Corrective Action Information Type

Corrective Action involves the enforcement functions necessary to remedy programs that have been found non-compliant with a given law, regulation, or policy. The recommended security categorization for the corrective action information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of corrective action information on the ability of responsible agencies to remedy internal or external programs that have been found non-compliant with a given law, regulation, or policy. Unauthorized disclosure of most corrective action information should have only a limited adverse effect on agency operations, assets, or individuals.

[11] The confidentiality impact assigned to the Information Management Information Type may necessitate the highest confidentiality impact of the information types processed by the system.

[12] A *national security system* is any information system (including any telecommunications system) used or operated by an agency or by a contractor on behalf of an agency, or any other organization on behalf of an agency – (i) the function, operation, or use of which: involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapon system; or is critical to the direct fulfillment of military or intelligence missions (excluding a routine administrative or business applications system used for applications such as payroll, finance, logistics, and personnel management); or (ii) that processes classified information.

Special Factors Affecting Confidentiality Impact Determination: Where more sensitive information is involved, it will probably be personal information subject to the Privacy Act of 1974 or information that is proprietary to a corporation or other organization. Such information will often be assigned a ***moderate*** confidentiality impact level. The Privacy Act Information provisional impact levels are documented in the Personal Identity and Authentication information type. Additionally, there are legislative mandates prohibiting unauthorized disclosure of trade secrets. Trade secrets will generally be assigned a ***moderate*** confidentiality impact level.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for corrective action information is ***low***.

Integrity

The consequences of undetected unauthorized modification or destruction of corrective action information can conceivably compromise the effectiveness of compliance enforcement actions (e.g., by providing violators with a basis for claiming investigative or enforcement irregularities, thus supporting legal challenges to proposed corrective actions). The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. Unauthorized modification or destruction of most corrective action information should have only a limited adverse effect on agency operations, assets, or individuals.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for corrective action information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to the corrective action information. The availability impact is also dependent on whether the data is time-critical. In most cases, disruption of access to corrective action information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The provisional availability impact level recommended for corrective action information is ***low***.

### C.2.1.2 Program Evaluation Information Type

Program Evaluation involves the analysis of internal and external program effectiveness and the determination of corrective actions as appropriate. The impact levels should be commensurate with the impact levels of the program that is being evaluated. For example, if the program contains very sensitive financial data with moderate impact levels for confidentiality and integrity, the program evaluation impact levels for confidentiality and integrity should also be moderate. The recommended security categorization for the program evaluation information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

### Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of program evaluation information on the abilities of responsible agencies to analyze internal and external program effectiveness and to determine appropriate corrective actions. The confidentiality impact of program evaluation information is largely event-driven. Once the evaluation has been reported, most program evaluation information is in the public domain. However, premature unauthorized disclosure of program evaluation information can alert personnel associated with programs under evaluation to the focus and preliminary findings of investigative and evaluation activities.

Special Factors Affecting Confidentiality Impact Determination: Where a major programs or human safety is at stake, actions taken based on unauthorized disclosure of program evaluation information can pose a threat to human life or a loss of major assets. In such cases, the confidentiality impact is ***high***. Unauthorized disclosure of most program evaluation information often has the potential to seriously affect agency operations. Also, some program evaluation information, particularly in the case of current investigations, includes personal information subject to the Privacy Act of 1974 and/or information that is proprietary to a corporation or other organization. The Privacy Act Information provisional impact levels are documented in the Personal Identity and Authentication information type. Additionally, there are legislative mandates prohibiting unauthorized disclosure of trade secrets. Trade secrets will generally be assigned a ***moderate*** confidentiality impact level. If the program evaluation information is moved to the public domain, the confidentiality impact level becomes Not Applicable (NA).

Recommended Confidentiality Impact Level: Because there are many cases in which unauthorized disclosure of program evaluation information will have only a limited adverse effect on agency operations, assets, or individuals, the provisional confidentiality impact level recommended for program evaluation information is ***low***.

### Integrity

The consequences of undetected unauthorized modification or destruction of program evaluation information can compromise the effectiveness of an evaluation program (e.g., by providing false information intended to mislead investigators or evaluators or to give program personnel a basis for claiming investigative or evaluative irregularities). The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. Although there are time-sensitive exceptions, unauthorized modification or destruction of most program evaluation information should have only a limited adverse effect on agency operations, assets, or individuals.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for program evaluation information is ***low***.

### Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to the program evaluation information. Although there are time-sensitive exceptions, most program evaluation processes are tolerant of reasonable delays. In most cases, disruption of access to program evaluation information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The provisional availability impact level recommended for program evaluation information is ***low***.

### C.2.1.3 Program Monitoring Information Type

Program Monitoring involves the data-gathering activities required to determine the effectiveness of internal and external programs and the extent to which they comply with related laws, regulations, and policies. The impact levels should be commensurate with the impact levels of the programs that are being monitored. For example, if a program contains very sensitive financial data with moderate impact levels for confidentiality and integrity, the program monitoring impact levels for confidentiality and integrity should also be moderate. Subject to exception conditions described below, the recommended security categorization for the program monitoring information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of program monitoring information on the ability of responsible agencies to perform data-gathering activities required to determine the effectiveness of internal and external programs and the extent to which they comply with related laws, regulations, and policies.

Special Factors Affecting Confidentiality Impact Determination: There are legislative mandates prohibiting unauthorized disclosure of trade secrets. Trade secrets will generally be assigned a ***moderate*** confidentiality impact level. Note that *national security information* and *national security systems* are outside the scope of this guideline. Otherwise, where the data being collected belongs to one of the information types described in this guideline, the confidentiality impact assigned the data and system is that of the highest impact information type collected. Unauthorized disclosure of program monitoring information can alert personnel associated with programs being monitored to the focus and implications of monitoring activities. Where a major programs or human safety is at stake, actions taken based on unauthorized disclosure of program monitoring information can pose a threat to human life or a loss of major assets. In such cases, the confidentiality impact is ***high***. If the program monitoring information is moved to the public domain, the confidentiality impact level becomes Not Applicable (NA).

Recommended Confidentiality Impact Level: Although there are many circumstances in which serious adverse effects on agency operations, agency assets, or individuals can result to justify a ***moderate*** base confidentiality impact level for program monitoring information, in most Federal environments, unauthorized disclosure will have only a limited adverse effect on agency operations, assets, or individuals. Consequently, for most systems, a **low** provisional confidentiality impact level is recommended for program monitoring information.

Integrity

The consequences of unauthorized modification or destruction of program monitoring information can compromise the effectiveness of the monitoring program. Although there may be time-sensitive program monitoring situations, the integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The damage likely to be caused by unauthorized modification or destruction of program monitoring information may have consequent serious adverse effects on agency operations or public confidence in the agency.

Special Factors Affecting Integrity Impact Determination: The consequences can be particularly serious if the destruction or modification of monitoring information invalidates evaluation results concerning major programs or concerning threats to human safety. The integrity impact resulting from unauthorized modification or deletion of program monitoring information depends in part on the nature of the laws or policies with which compliance is being determined and in part on the criticality of the processes being monitored. For example, in the case of safety regulations affecting manned space flight, the integrity impact level may be ***high***.

Recommended Integrity Impact Level: There are some regulatory environments in which a ***high*** or ***moderate*** impact level is appropriate. For most compliance monitoring information, the recommended provisional integrity impact level is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to the program monitoring information. Although there may be time-sensitive program monitoring situations, more typically, disruption of access to program monitoring information will have only a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Availability Impact Determination: There are a limited number of compliance monitoring operations for which temporary loss of availability is likely to significantly degrade mission capability, place the agency at a significant disadvantage, result in loss of major assets, or pose a threat to human life. This can result in assignment of a ***moderate*** impact level to such information.

Recommended Availability Impact Level: The provisional availability impact level recommended for program monitoring information is ***low***.

### C.2.2 Regulatory Development

Regulatory Development involves activities associated with providing input to the lawmaking process in developing regulations, policies, and guidance to implement laws.

#### C.2.2.1 Policy and Guidance Development Information Type

Policy and Guidance Development involves the creation and dissemination of guidelines to assist in the interpretation and implementation of regulations. In most cases, the effect on public welfare of a loss of policy and guidance development mission capability can be expected to be delayed rather than immediate. As a result, the potential for consequent loss of human life or of major national assets is relatively low, since these most catastrophic consequences of impairment to mission capability can, in most cases, be corrected before they are fully realized. The recommended security categorization for the policy and guidance development information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

### Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of policy and guidance information on the ability of responsible agencies to create and disseminate guidelines to assist in the interpretation and implementation of regulations. The confidentiality impact of policy and guidance information is largely event-driven. Once a policy or guidance statement has been promulgated, most policy and guidance information is in the public domain. However, premature unauthorized disclosure of candidate policy and guidance material can result in disruption of (and inappropriate influence of special interests on) the policy development process.

Special Factors Affecting Confidentiality Impact Determination: The effects of loss of confidentiality of guidelines during the formative stage can result in attempts by affected entities and other interested parties to influence and/or impede the policy and guideline development process. Premature public release of formative policies and guidelines before internal coordination and review can result in unnecessary damage to public confidence in the agency. This is particularly likely where the release includes unedited internal commentary and discussion. Delays can impair an agency's mission, but loss of public confidence can do serious and persistent harm to an agency's ability to effectively perform its mission. In such cases, the provisional confidentiality impact level recommended for policy and guidance development information is ***moderate***. When the policy and guidance information is in the public domain, the confidentiality impact level becomes Not Applicable (NA).

Recommended Confidentiality Impact Level: Although there are cases in which unauthorized and premature disclosure of policy and guidance information can result in serious consequences for an agency, most of this information is intended to be available to the general public. Consequently, the provisional confidentiality impact level recommended for policy and guidance development information is ***low***.

### Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information.

Special Factors Affecting Integrity Impact Determination: Some policy and guidance information is time-critical. Unauthorized modification or destruction of information affecting external communications that contain policy and guidance development information (e.g., web pages, electronic mail) may adversely affect operations or public confidence in the agency, but the damage to the mission would usually be limited. Public confidence consequences can be expected to be much more serious in cases of agencies that have national defense, intelligence, or information security missions. In such cases, the impact may be at least ***moderate***.

Recommended Integrity Impact Level: The provisional integrity level recommended for policy and guidance development information is ***low***.

### Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to the policy and guidance development information. Though some policy and guidance information is time-critical, the policy and guidance development process is usually tolerant of delays.

Recommended Availability Impact Level: the provisional availability impact level recommended for policy and guidance development information is ***low***.

### C.2.2.2 Public Comment Tracking Information Type

Public Comment Tracking involves the activities of soliciting, maintaining, and responding to public comments regarding proposed regulations. Subject to exception conditions described below, the recommended security categorization for the public comment tracking information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of public comment tracking information on the ability of responsible agencies to solicit, maintain, and respond to public comments regarding proposed regulations.  The effects of loss of confidentiality of information associated with the public comment process are unlikely to pose the threat of serious harm to agency assets, personnel or operations.

In a few cases, the rationale for public comments can include information that is sensitive in terms of proprietary information sensitive Federal government information, or even national security information.  However, such cases are exceptional and the information in question would be expected to be representative of information types covered elsewhere in this guideline.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for public comment tracking information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information.

Unauthorized modification or destruction of information affecting external communications that contain public comment tracking information (e.g., web pages, electronic mail) may adversely affect operations or public confidence in the agency, but the damage to the mission would usually be limited.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for public comment tracking information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to the public comment tracking information.  The effects of disruption of access to public comment tracking information or information systems can delay development of standards, guidelines, or regulations.

The public comment tracking process is usually tolerant of delays. Permanent loss of comment information may disrupt some government operations by showing a lack of due diligence in response to comments.

Recommended Availability Impact Level: The provisional availability impact level recommended for public comment tracking information is ***low***.

### C.2.2.3 Regulatory Creation Information Type

Regulatory Creation involves the activities of researching and drafting proposed and final regulations. Subject to exception conditions described below, the recommended security categorization for the regulatory creation information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The level of confidentiality impact level is the effect of unauthorized disclosure of regulatory creation information on the ability of responsible agencies to research and draft proposed and final regulations. The effects of loss of confidentiality of early drafts of regulations can result in attempts by affected entities and other affected parties to influence and/or impede the regulation development process.

Special Factors Affecting Confidentiality Impact Determination: Premature public release of draft regulations before internal coordination and review has been conducted can result in unnecessary criticism of the proposed regulation and even damage public confidence in the agency. In such cases, the provisional confidentiality impact level recommended for regulatory creation information is ***moderate***. These consequences are particularly likely where the release includes unedited internal commentary and discussion. Delays can impair an agency's mission, but loss of public confidence can do serious and persistent harm to an agency's ability to effectively perform its mission. If the regulatory information is moved to the public domain, the confidentiality impact level becomes Not Applicable (NA).

Recommended Confidentiality Impact Level: Because most regulatory information is intended for release to the public, the provisional confidentiality impact level recommended for regulatory creation information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external communications that contain regulatory information (e.g., web pages, electronic mail) may adversely affect operations or public confidence in the agency. The consequences of a reduction in public confidence will be more serious for agencies that have national defense, intelligence, or information security missions. In such cases, the impact level may be at least ***moderate***.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for regulatory creation information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to the regulatory creation information. The regulatory creation process is usually tolerant of delays.

Recommended Availability Impact Level: The provisional availability impact level recommended for regulatory creation information is ***low***.

#### C.2.2.4 Rule Publication Information Type

Rule Publication includes all activities associated with the publication of a proposed or final rule in the Federal Register and Code of Federal Regulations. Subject to exception conditions described below, the recommended security categorization for the rule publication information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of rule publication information on the ability of responsible agencies to publish proposed or final rules in the Federal Register and Code of Federal Regulations. The published rules are, by definition, public information.

The effects of loss of confidentiality of information associated with the rule publication process are unlikely to pose the threat of serious harm to agency assets, personnel or operations.

Recommended Confidentiality Impact Level: In general, the provisional confidentiality impact level recommended for rule publication information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information.

In the worst cases, *errata* can be published. Unauthorized modification or destruction of information may result in unnecessary expenditures, some confusion, and limited damage to public confidence in the agency.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for rule publication information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to the rule publication information.

Rule publication processes are usually tolerant of delays.

Recommended Availability Impact Level: The provisional availability impact level recommended for rule publication information is ***low***.

### C.2.3 Planning and Budgeting

Planning and Budgeting involves the activities of determining strategic direction, identifying and establishing programs and processes to enable change, and allocating resources (capital and labor) among those programs and processes.

#### C.2.3.1 Budget Formulation Information Type

Budget Formulation involves all activities undertaken to determine priorities for future spending and to develop an itemized forecast of future funding and expenditures during a targeted period of time. This includes the collection and use of performance information to assess the effectiveness of programs and develop budget priorities.  Subject to exception conditions described below, the recommended security categorization for the budget formulation information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of budget formulation information on the ability of responsible agencies to determine priorities for future spending and to develop an itemized forecast of future funding and expenditures during a targeted period of time.  Most budget information is supposed to be available to the public.

Special Factors Affecting Confidentiality Impact Determination: Some budget information of is classified *national security information* and is outside the scope of this guideline.  The effects of loss of confidentiality of budget information or of early drafts of budgets can result in attempts by competing interests to influence and/or impede the regulation development process.  The consequences to agency programs and even of the ability of an agency to perform its mission can be very serious.  Premature public release of draft budgets before internal coordination and review has been conducted can result in unnecessary criticism of the proposed regulation and even damage public confidence in the agency.  These consequences are particularly likely where the release includes unedited internal commentary and discussion.  Delays that result from confidentiality compromise can imperil specific agency programs, but loss of public confidence can do persistent harm to an agency's ability to effectively perform its mission.  In such cases, the confidentiality impact level for budget formulation information is ***moderate***.  If the budget formulation information is moved to the public domain, the confidentiality impact level becomes Not Applicable (NA).

Recommended Confidentiality Impact Level: In spite of the serious harm that can be suffered by an agency due to unauthorized and premature disclosure of draft budget information (and associated commentary), the provisional confidentiality impact level recommended for budget formulation information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information.

Special Factors Affecting Integrity Impact Determination:  Some budget formulation information is time-critical.  Also, unauthorized modification or destruction of information affecting external communications that contain budget information (e.g., web pages, electronic mail) may adversely affect operations or public confidence in the agency, but the damage to the mission would usually be limited. Public confidence consequences will be more serious for agencies that have national defense, intelligence, or information security missions.  In such cases, the impact may be at least ***moderate***.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for budget formulation information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to the budget formulation information.

Although some budget formulation information is time-critical, the budget formulation processes are usually tolerant of delays.  Excessive recovery delays may result in loss of funding.

Recommended Availability Impact Level:  The provisional availability impact level recommended for budget formulation information is ***low***.

### C.2.3.2 Capital Planning Information Type

Capital Planning involves the processes for ensuring that appropriate investments are selected for capital expenditures.  The recommended provisional security categorization for capital planning information is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of capital planning information on the ability of responsible agencies to ensure that appropriate investments are selected for capital expenditures.  The effects of loss of confidentiality of capital investment plans during the formative stage can result in attempts by affected entities and other interested parties to influence and/or impede the policy and guideline development process.  Premature public release of draft plans before internal coordination and review can result in unnecessary damage to public confidence in the agency.  This is particularly likely where the release includes unedited internal commentary and discussion.  The diversion of investment funds that can result from compromise of draft plans can pervert investment priorities in a manner that is prejudicial to public interest.  However, the consequence of loss of confidentiality of most capital planning information is likely to do only limited harm to government assets, personnel, or missions.

Special Factors Affecting Confidentiality Impact Determination: Unauthorized disclosure of some of the background information that supports development of capital investment plans can reveal sensitive vulnerabilities, capabilities, or methods of anti-terrorism, law enforcement, or national security activities.  Depending on the information in question, the confidentiality impact can be ***moderate, high***, or involve *national security information* (outside the scope of this guideline). Also, some capital investment plans of some Federal agencies contain *national security information*.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for capital planning information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external communications that contain capital planning information (e.g., web pages, electronic mail) may adversely affect operations or public confidence in the agency, but the damage to the mission would usually be limited. Public confidence consequences will be more serious for agencies that have national defense, intelligence, or information security missions. In such cases, the impact may be at least ***moderate***.

Recommended Integrity Impact Level: The provisional integrity level recommended for capital planning information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to the capital planning information.

The capital planning processes are usually tolerant of delays.

Recommended Availability Impact Level: The provisional availability impact level recommended for capital planning information is ***low***.

#### C.2.3.3 Enterprise Architecture Information Type

Enterprise Architecture is an established process for describing the current state and defining the target state and transition strategy for an organization's people, processes, and technology. The recommended provisional security categorization for the enterprise architecture information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of enterprise architecture information on the ability of responsible agencies to describe the current state and define the target state and transition strategy for an organizations people, processes, and technology. The effects of loss of confidentiality of preliminary draft enterprise architecture plans can result in attempts by affected entities and other interested parties to influence and/or impede the policy and guideline development process. Premature public release of draft plans before internal coordination and review can result in unnecessary damage to public confidence in the agency. This is particularly likely where the release includes unedited internal commentary and discussion. However, the consequence of loss of confidentiality of most enterprise architecture information is likely to do only limited harm to government assets, personnel, or missions.

Special Factors Affecting Confidentiality Impact Determination: Unauthorized disclosure of some of the background information that supports development of Federal enterprise architecture can reveal sensitive vulnerabilities, capabilities, or methods of anti-terrorism, law enforcement, or national security activities.[13] Depending on the information in question, the confidentiality impact can be ***moderate, high***, or involve *national security information* (outside the scope of this guideline). Also, some enterprise architecture plans of some Federal agencies are themselves *national security information*. Finally, important financial decisions and planning information may be included in this category of information.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for enterprise architecture information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external communications that contain enterprise architecture information (e.g., web pages, electronic mail) may adversely affect operations or public confidence in the agency, but the damage to the mission would usually be limited. Public confidence consequences will be more serious for agencies that have national defense, intelligence, or information security missions. In such cases, the impact may be at least ***moderate***.

Recommended Availability Impact Level: In general, the provisional integrity level recommended for enterprise architecture information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to the enterprise architecture information. The enterprise architecture processes are usually tolerant of delays.

Recommended Availability Impact Level: The provisional availability impact level recommended for enterprise architecture information is ***low***.

### C.2.3.4 Strategic Planning Information Type

Strategic Planning entails the determination of long-term goals and the identification of the best approach for achieving those goals. The recommended provisional security categorization for strategic planning information is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

[13] The Office of Management and Budget (OMB) has placed some emphasis on protecting repositories of this information. Among other things it may contain details of the technology and security of an agency's network and include information about critical repositories of highly sensitive and/or even National Security information.

#### Confidentiality

The confidentiality impact level is the effect of the unauthorized disclosure of strategic planning information on the ability of responsible agencies to determine long-term goals and to identify the best approach for achieving those goals. Premature public release of draft plans before internal coordination and review can result in unnecessary damage to public confidence in the agency. This is particularly likely where the release includes unedited internal commentary and discussion. However, the consequence of loss of confidentiality of most strategic planning information is likely to do only limited harm to government assets, personnel, or missions.

Special Factors Affecting Confidentiality Impact Determination: Unauthorized disclosure of some of the background information that supports development of some Federal strategic plans can reveal sensitive vulnerabilities, capabilities, or methods of anti-terrorism, law enforcement, or national security activities. Depending on the information in question, the confidentiality impact can be ***moderate, high***, or involve *national security information* (outside the scope of this guideline). Also, some strategic plans are themselves *national security information*.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for strategic planning information is ***low***.

#### Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external communications that contain strategic planning information (e.g., web pages, electronic mail) may adversely affect operations or public confidence in the agency, but the damage to the mission would usually be limited. Public confidence consequences will be more serious for agencies that have national defense, intelligence, or information security missions. In such cases, the impact may be at least ***moderate***.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for strategic planning information is ***low***.

#### Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to the strategic planning information. Strategic planning processes are usually tolerant of delays.

Recommended Availability Impact Level: The provisional availability impact level recommended for strategic planning information is ***low***.

### C.2.3.5 Budget Execution Information Type

Budget Execution involves day-to-day requisitions and obligations for agency expenditures, invoices, billing dispute resolution, reconciliation, service level agreements, and distributions of shared expenses. The recommended provisional security categorization for budget execution information is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

### Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of budget execution information on the ability of responsible agencies to manage day-to-day requisitions and obligations for agency expenditures, invoices, billing dispute resolution, reconciliation, service level agreements, and distributions of shared expenses. The effects of loss of confidentiality of most budget execution information are unlikely to pose the threat of serious harm to agency assets, personnel or operations.

Special Factors Affecting Confidentiality Impact Determination: The effects of loss of confidentiality of budget execution information can violate privacy regulations, reveal information proprietary to private institutions, and reveal procurement-sensitive information. In aggregate, budget execution information can reveal capabilities and methods that some agencies (e.g., law enforcement, homeland security, national defense, intelligence) consider extremely sensitive. In these cases, the potential harm that can result from unauthorized disclosure ranges from ***moderate*** to ***high*** to *national security-related*. In the last case, the information is outside the scope of this document. Public release of sensitive budget execution information can result in unnecessary damage to public confidence in the agency. This is particularly likely where the release includes unedited internal commentary and discussion.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for most budget execution information is ***low***.

### Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. Where small dollar amounts are modified, the potential damage to an agency's mission is limited.

Special Factors Affecting Integrity Impact Determination: In the case of agreements or transactions involving large monetary values, asset losses, and damage to agency operations, the potential for serious loss of public confidence is high. The consequent integrity impact level is ***moderate*** to ***high***. If the budget execution information is time-critical or very sensitive, the integrity impact level may be ***moderate*** or ***high***.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for most budget execution information is ***low***.

### Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to the budget execution information. The budget execution processes are usually tolerant of delays.

Recommended Availability Impact Level: The provisional availability impact level recommended for budget execution information is ***low***.

### C.2.3.6 Workforce Planning Information Type

Workforce Planning involves the processes for identifying the workforce competencies required to meet the agency's strategic goals and for developing the strategies to meet these requirements. The recommended security categorization for workforce planning information is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of workforce planning information on the ability of responsible agencies to identify workforce competencies required to meet the agency's strategic goals and for developing the strategies to meet these requirements. Unauthorized disclosure of most workforce planning information will have only a limited adverse effect on agency operations, assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Unauthorized disclosure of some background information that supports development of Federal workforce plans can reveal sensitive vulnerabilities, tables of organization, capabilities, or methods of anti-terrorism, law enforcement, or national security activities. Depending on the information in question, the confidentiality impact can be ***moderate, high***, or involve *national security information* (outside the scope of this guideline).

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for workforce planning information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. Therefore, consequences of undetected unauthorized modification or destruction of workforce planning information may compromise the effectiveness of compliance enforcement actions (e.g., by providing violators with a basis for claiming investigative or enforcement irregularities).

Recommended Integrity Impact Level: The provisional integrity impact level recommended for workforce planning information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to the workforce planning information. The workforce planning processes are generally tolerant of reasonable delays. In most cases, disruption of access to workforce planning information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The provisional availability impact level recommended for workforce planning information is ***low***.

### C.2.3.7 Management Improvement Information Type

Management Improvement includes all efforts to gauge the ongoing efficiency of business processes and identify opportunities for reengineering or restructuring. The recommended provisional security categorization for the management improvement information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

### Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of management improvement information on the ability of responsible agencies to gauge the ongoing efficiency of business processes and identify opportunities for reengineering or restructuring. Premature public release of draft plans before internal coordination and review can result in unnecessary damage to public confidence in the agency. This is particularly likely where the release includes unedited internal commentary and discussion. However, the consequence of loss of confidentiality of most management improvement information is likely to involve only limited harm to government assets, personnel, or missions.

Special Factors Affecting Confidentiality Impact Determination: Unauthorized disclosure of some background information that supports development of Federal management improvement plans can reveal personnel-sensitive information, including information subject to the Privacy Act of 1974. The Privacy Act Information provisional impact levels are documented in the Personal Identity and Authentication information type. Other background information can reveal sensitive vulnerabilities, capabilities, or methods of anti-terrorism, law enforcement, or national security activities. Depending on the information in question, the confidentiality impact can be ***moderate, high***, or involve *national security information* (outside the scope of this guideline). Also, some strategic plans are themselves *national security information*.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for management improvement information is ***low***.

### Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external communications that contain management improvement information (e.g., web pages, electronic mail) may adversely affect operations or public confidence in the agency, but the damage to the mission would usually be limited. Public confidence consequences can be expected to be more serious for agencies that have national defense, intelligence, or information security missions. In such cases, the impact may be at least ***moderate***. Failure to detect malicious modification of personnel information (mostly background information) can result in disruption of some agency operations and disruptive administrative or legal actions.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for management improvement information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to the management improvement information. The management improvement planning processes are usually tolerant of delays.

Recommended Availability Impact Level: The provisional availability impact level recommended for management improvement information is ***low***.

### C.2.3.8 Budget and Performance Integration Information Type

Budget and Performance Integration involves activities that align Federal resources allocated through budget formulation, execution, and management actions with examinations of program objectives, performance, and demonstrated results such as Program Performance Assessments, Government Performance Results Act (GPRA) plans and reports, performance-based agency budget submissions, and Financial Management Cost Accounting and Performance Measurement data. Subject to exception conditions described below, the recommended security categorization for the budget and performance integration information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure budget and performance integration information on the abilities of responsible agencies to align Federal resources allocated through budget formulation, execution, and management actions. The consequences of unauthorized disclosure of the majority of budget and performance integration information will result in a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: The effects of loss of confidentiality of budget and performance integration information can violate privacy regulations, reveal information proprietary to private institutions, and reveal procurement-sensitive information. In aggregate, budget and performance integration information can reveal capabilities and methods that some agencies (e.g., law enforcement, homeland security, national defense, intelligence) consider extremely sensitive. In these cases, the potential harm that can result from unauthorized disclosure ranges from ***moderate*** to ***high*** to *national security-related*. In the last case, the information is outside the scope of this document. Public release of sensitive budget and performance integration information can result in unnecessary damage to public confidence in the agency. This is particularly likely where the release includes unedited internal commentary and discussion.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for resource budget and performance integration information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external communications that contain budget and performance integration information (e.g., web pages, electronic mail) may adversely affect operations or public confidence in the agency, but the damage to the mission would usually be limited. Public confidence consequences will be more serious for agencies that have national defense, intelligence, or information security missions. In such cases, the impact may be at least ***moderate***.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for budget and performance integration information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to budget and performance integration information. The budget and performance integration processes are usually tolerant of delays.

Recommended Availability Impact Level: The provisional availability impact level recommended for budget and performance integration information is ***low***.

### C.2.3.9 Tax and Fiscal Policy Information Type

Tax and Fiscal Policy encompasses analysis of the implications for economic growth and stability in the United States and the world of Federal tax and spending policies. This includes assessing the sustainability of current programs and policies, the best means for raising revenues, the distribution of tax liabilities, and the appropriate limits on debt. The recommended provisional security categorization for tax and fiscal policy information is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of tax and fiscal policy information on the abilities of responsible agencies to analyze the implications for economic growth and stability in the United States and the world of Federal tax and spending policies. The consequences of unauthorized disclosure of the majority of tax and fiscal policy information will result in a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: The effects of loss of confidentiality of tax and fiscal policy information can be more critical during the policy development process and may severe impacts to the agency mission and privacy information. Premature or accidental public release of sensitive tax and fiscal policy information can result in unnecessary damage to public confidence in the agency. Additionally, premature release of this information may create unfair economic advantages based on economic projections and fiscal policies. In these cases, the potential harm that can result from unauthorized disclosure ranges from ***moderate*** to ***high*** depending on the mission impacted.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended tax and fiscal policy information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external communications that tax and fiscal policy information (e.g., web pages, electronic mail) may adversely affect operations or public confidence in the agency, but the damage to the mission would usually be limited. Public confidence consequences will be more serious for agencies that have national defense, intelligence, or information security missions. In such cases, the impact may be at least ***moderate***.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for tax and fiscal policy information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to tax and fiscal policy information. Tax and fiscal policy processes are usually tolerant of delays.

Recommended Availability Impact Level: The provisional availability impact level recommended tax and fiscal policy information is ***low***.

## C.2.4 Internal Risk Management and Mitigation

Internal risk management and mitigation involves all activities relating to the processes of analyzing exposure to risk and determining appropriate counter-measures. Note that risks to information and information systems associated with internal risk management and mitigation activities may inherently affect the resistance to compromise/damage and recovery from damage with respect to a broad range of critical infrastructures and key national assets.

### C.2.4.1 Contingency Planning Information Type

Contingency planning involves the actions required to plan for, respond to, and mitigate damaging events. The recommended provisional security categorization for the contingency planning information type is as follows:

Security Category = {(confidentiality, Moderate), (integrity, Moderate), (availability, Moderate)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of contingency planning information on the ability of responsible agencies to plan for, respond to, and mitigate damaging events. Unauthorized disclosure of contingency planning information may equip an adversary with the information necessary to attack a system so that recovery is impaired.

Special Factors Affecting Confidentiality Impact Determination: Unauthorized disclosure of background information that supports development of Federal contingency plans can reveal sensitive vulnerabilities, capabilities, intelligence assessments, intelligence sources, or methods employed in anti-terrorism, law enforcement, or national security activities. Depending on the information in question, the confidentiality impact can be ***moderate, high***, or involve *national security information* (outside the scope of this guideline). Also, some contingency plans are themselves *national security information*. However, the purpose of most contingency planning information is to protect against inadvertent or accidental damaging events rather than against malicious attacks.  Even so, in the case of Federal government systems, the case of hostile attacks on systems must be considered.  The consequences of unauthorized disclosure of extracts from contingency plans are likely to have negligible to limited adverse effects on agency operations.  In such cases, the confidentiality impact would be, at most, ***low***.  Unauthorized disclosure of the entire plan to malicious entities may have serious effects.  As a result, the consequence of loss of confidentiality of comprehensive contingency plans is likely to involve serious harm to government assets, personnel, or missions. In such cases, the confidentiality impact would be, at least, ***moderate***.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for contingency planning information is ***moderate***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information.  Errors in contingency plans that result from integrity compromise can result in serious consequences to system recovery capabilities.  These can range from incorrect telephone numbers and e-mail addresses on notification lists to erroneous schedules and file designations for database back-ups and archives or software baselines, updates, and patches.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for contingency planning information is ***moderate***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to the contingency planning information. The effects of disruption of access to contingency planning information or information systems depend on the timing of the disruption.  If access to contingency planning information is denied because of a power outage, recovery may be delayed and the work of government agencies disrupted.

Special Factors Affecting Availability Impact Determination: The contingency *planning* processes are usually tolerant of delays. In contrast, the contingency plan *implementation* process is not tolerant of delays.  The consequences of disruption of access to contingency planning information depend on both the period of the outage and the criticality of the disrupted processes. The consequent impact level may range from ***low*** to ***high***.

Recommended Availability Impact Level:  The provisional availability impact level recommended for contingency planning information is ***moderate***.

### C.2.4.2 Continuity of Operations Information Type

Continuity of operations involves the activities associated with the identification of critical systems and processes, and the planning and preparation required to ensure that these systems and processes will be available in the event of a catastrophic event. The recommended provisional security categorization for the continuity of operations information type is as follows:

Security Category = {(confidentiality, Moderate), (integrity, Moderate), (availability, Moderate)}

#### Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of continuity of operations information on the ability of responsible agencies to identify critical systems and processes, and to conduct the planning and preparation required to ensure that these systems and processes will be available in the event of a catastrophic event. Unauthorized disclosure of the entire plan to malicious entities may have serious effects. As a result, the consequence of loss of confidentiality of most continuity of operations plans (and comprehensive continuity of operations plans) is likely to do serious harm to government assets, personnel, or missions.

Special Factors Affecting Confidentiality Impact Determination: Unauthorized disclosure of background information that supports development of Federal continuity of operations plans can reveal sensitive vulnerabilities, capabilities, intelligence assessments, intelligence sources, or methods employed in anti-terrorism, law enforcement, or national security activities. Depending on the information in question, the confidentiality impact can be ***moderate, high***, or involve *national security information* (outside the scope of this guideline). Unauthorized disclosure of continuity of operations information for critical infrastructures and key national assets may require a ***high*** impact level. However, the purpose of most continuity of operations information is to protect against inadvertent or accidental damaging events rather than against malicious attacks. Even so, in the case of Federal government systems, hostile attacks on systems must be considered.

The consequences of unauthorized disclosure of extracts from continuity of operations plans are likely to have negligible to limited adverse effects on agency operations. In such cases, the confidentiality impact would be, at most, ***low***. Unauthorized disclosure of continuity of operations information may inform an adversary regarding what facilities and processes are considered to be critical. Such unauthorized disclosure may also equip an adversary with the information necessary to attack a system so that operations are disrupted, and that recovery is impaired. In such cases, the confidentiality impact would be, at least, ***moderate***.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for continuity of operations information is ***moderate***.

#### Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. Errors in continuity of operations plans that result from integrity compromise can result in serious consequences to system recovery capabilities. These can range from incorrect telephone numbers and e-mail addresses on notification lists to erroneous version numbers for database back-ups and archives or software baselines, updates, and patches.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for continuity of operations information is ***moderate***.

#### Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to the continuity of operations information.

Special Factors Affecting Availability Impact Determination: The effects of disruption of access to continuity of operations information or information systems depend on the timing of the disruption. If access to continuity of operations information is denied because of a power outage, recovery may be delayed and the work of government agencies disrupted. The continuity of operations planning process is usually tolerant of delays. In contrast, the continuity of operations *implementation* process is not tolerant of delays. The consequences of disruption of access to continuity of operations information depend on both the period of the outage and the criticality of the disrupted processes. The consequent impact level will range from ***low*** to ***high***.

Recommended Availability Impact Level: The provisional availability impact level recommended for continuity of operations information is ***moderate***.

### C.2.4.3 Service Recovery Information Type

Service recovery involves the internal actions necessary to develop a plan for resuming operations after a catastrophe occurs, such as a fire or earthquake. The recommended provisional security categorization for the service recovery information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of the unauthorized disclosure of service recovery information on the ability of responsible agencies to develop plans for resuming operations after a catastrophe occurs, such as a fire or earthquake. In the case of service recovery plans for natural catastrophes, the information associated with service recovery planning is not intrinsically sensitive. In the case of catastrophes caused by malicious activity, unauthorized disclosure of service recovery information may inform an adversary regarding what facilities and processes are considered to be critical. Such unauthorized disclosure may also equip an adversary with the information necessary to attack a system in such a way that operations are disrupted, and that recovery is impaired or even blocked. The purpose of most service recovery information is to protect against natural catastrophes rather than against malicious attacks. In most cases, the consequence of loss of confidentiality of service recovery information is not likely to do serious harm to government assets, personnel, or missions.

Special Factors Affecting Confidentiality Impact Determination: Unauthorized disclosure of background information that supports development of Federal service recovery plans can reveal sensitive vulnerabilities, capabilities, intelligence assessments, intelligence sources, or methods employed in anti-terrorism, law enforcement, or national security activities. Depending on the information in question, the confidentiality impact can be ***moderate, high***, or involve *national security information* (outside the scope of this guideline). Also, some service recovery plans are themselves *national security information*.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for service recovery information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for service recovery information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to the service recovery information. The effects of disruption of access to service recovery information or information systems depend on the timing of the disruption. If access to service recovery information is denied because of a power outage, recovery may be delayed and the work of government agencies disrupted.

Special Factors Affecting Availability Impact Determination: Service recovery *planning* processes are usually tolerant of delay. In contrast, the *implementation* of recovery plans is not tolerant of delays. For service recovery implementation, the consequences of access disruption depend on the time period of the disruption and the criticality of the disrupted processes. The consequent impact level may range from ***low*** to ***high***.

Recommended Availability Impact Level: The provisional availability impact level recommended for service recovery information is ***low***.

## C.2.5 Revenue Collection

Revenue Collection includes the collection of Government income from all sources. Note: Tax collection is accounted for under the Taxation Management information type in the General Government mission area.

### C.2.5.1 Debt Collection Information Type

Debt Collection supports activities associated with the collection of money owed to the United States government from both foreign and domestic sources. The recommended security categorization for debt collection information is as follows:

Security Category = {(confidentiality, Moderate), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of debt collection information on the ability of responsible agencies to properly and efficiently collect money owed to the United States government from both foreign and domestic sources. The consequences of unauthorized disclosure of debt collection information are generally dependent on the identity of the debtor and of the nature and value of the debt being collected. Typically, unauthorized disclosure of debt collection information will have only a limited adverse effect on agency operations, assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Where more sensitive information is involved, it will commonly be personal information subject to the Privacy Act of 1974, information that is proprietary to a corporation or other organization, or information that is politically sensitive by a foreign government. The Privacy Act Information provisional impact levels are documented in the Personal Identity and Authentication information type. Such information will often be associated with debt collection processes. Where the amount of the debt is significant, and unauthorized knowledge might imperil successful collection, then the associated confidentiality impact assigned to debt collection information might be ***moderate*** (or even ***high*** in the case of extremely high dollar value cases).

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for debt collection information is ***moderate***.

#### Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. Therefore, the consequences of unauthorized modification or destruction of debt collection information depend on the type of property being managed and on the immediacy with which the information is expected to be used.

Special Factors Affecting Integrity Impact Determination: If the modified or destroyed information is substantive financial data, there is a greater potential for harm to result from actions being taken based on incomplete or false information. This can have serious adverse effects on individual financial actions with consequent loss of revenue from, or other unanticipated consequences regarding the personal property under disposition. The severity of the consequences depends on the type of the debt and of the debtor but would be most likely be ***moderate***.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for debt collection information is ***low***.

#### Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to the debt collection information.

Most Federal debt collection processes are tolerant of delays. Also, the consequences of temporary inability to access information concerning foreign or domestic debt will be minimal.

Recommended Availability Impact Level: The provisional availability impact level recommended for debt collection information is ***low***.

### C.2.5.2 User Fee Collection Information Type

User fee Collection involves the collection of fees assessed on individuals or organizations for the provision of Government services and for the use of Government goods or resources (i.e. National Parks). The recommended security categorization for the user fee collection information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Moderate)}

#### Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of user fee collection information on the ability of responsible agencies to correctly and efficiently enforce, regulate, and effect the collection of fees assessed on individuals or organizations for the provision of Government services and for the use of Government goods or resources. In general, particularly in aggregate, this information is public record.

Recommended Confidentiality Impact Level: The recommended provisional confidentiality impact level for user fee collection information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. For example, there may be some circumstances when the unauthorized modification or destruction of user fee collection information is undertaken as part of a scheme to divert payments, conceal underpayment of failure to make payment of fees, or otherwise defraud the government. In addition, the consequences of unauthorized modification or destruction of user fee collection information may depend on the urgency with which the information is needed or the immediacy with which the information is used. In most cases, it is unlikely that the information will be needed urgently or acted upon immediately.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external communications might have an adverse effect on agency operations, image and reputation. The integrity impact level assigned may be ***moderate***.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for user fee collection information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to the user fee collection information. The missions supported by user fee collection information are generally tolerant of delay. However, any extended period of unavailability would likely be seriously disruptive to the operations for which fees are collected.

Recommended Availability Impact Level: The provisional availability impact level recommended for user fee collection information is ***moderate***.

### C.2.5.3 Federal Asset Sales Information Type

Federal Asset Sales encompasses the activities associated with the acquisition, oversight, tracking, and sale of non-internal assets managed by the Federal Government with a commercial value and sold to the private sector. The recommended security categorization for the Federal asset sales information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Moderate), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of the unauthorized disclosure of Federal asset sales information on the ability of responsible agencies to properly and efficiently acquire, oversee, track, and sell non-internal assets managed by the Federal Government with a commercial value and sold to the private sector. The consequences of unauthorized disclosure of Federal asset sales information are generally dependent on the nature and value of the property being disposed.

Generally, Federal asset sales information is public. Most managed property would not be of sufficient individual value to occasion such an occurrence (bid rigging, etc.).

Special Factors Affecting Confidentiality Impact Determination: Where unauthorized knowledge regarding the property being disposed of might lead to unfair advantage (i.e., ability to accurately bid on an auction lot to the detriment of other bidders), then the associated confidentiality impact assigned to Federal asset sales information might be ***moderate***. Such an instance might arise if a disruption of the proper procedures could reasonably cause an adverse effect on future operations of the responsible agency, or if the agency's image, or individual reputations might be damaged.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for Federal asset sales information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of Federal asset sale information is partially dependent on the type of property being managed and whether the data is time-critical. If the modified or destroyed information is substantive financial data, actions that are taken based on incomplete or false information could have serious adverse effects on individual financial actions.

Unauthorized modification or destruction of information affecting external communications (e.g., web pages, solicitations for bid, official notices of disposition, etc.) may adversely affect the operations, image or reputation of an agency. However, the damage to the management mission would usually be of more immediate concern. The severity of the consequent integrity impact depends on the nature of the property but would be most likely be ***moderate***.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for Federal asset sales information is ***moderate***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to the Federal asset sale information. The missions supported by Federal asset sale information are generally tolerant of delay. Generally, the consequences of temporary inability to access solicitations for bid, official notices of disposition, etc., will be minimal.

Recommended Availability Impact Level: The provisional availability impact level recommended for Federal asset sale information is ***low***.

### C.2.6 Public Affairs

Public Affairs activities involve the exchange of information and communication between the Federal Government, citizens and stakeholders in direct support of citizen services, public policy, and/or national interest.

### C.2.6.1 Customer Services Information Type

Customer Service supports activities associated with providing and managing the delivery of information and support to the government's customers. The recommended security categorization for the customer service information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of customer service information on the ability of responsible agencies to provide and manage the delivery of information and support to the government's customers. Most customer service information is likely to be in the public domain and poses no confidentiality impact. In most cases, unauthorized disclosure of customer service information will have at most a limited adverse effect on agency operations, assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Some customer service information may include customer-provided information covered by the provisions of the Privacy Act of 1974. The Privacy Act Information provisional impact levels are documented in the Personal Identity and Authentication information type. Unauthorized disclosure of large volumes of information protected under the Privacy Act can be expected to have a serious to severe effect on public confidence in the agency. Actions taken that are intended to establish blame, compensate victims, or repair damage done with the exposed information can cause serious disruption of an agency's mission capability. In such cases, the confidentiality impact can be ***moderate***.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for customer service information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. Typically, the adverse effects of unauthorized modification or destruction of customer service information on overall agency mission functions or public confidence in the agency are limited. The more serious integrity impacts become increasingly likely as E-government initiatives progress. Typically, the unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) will result in limited adverse affect on operations or public confidence in the agency and the damage to most missions would usually be limited.

Special Factors Affecting Integrity Impact Determination: An increasing proportion of customer service activities are interactive. Consequently, there is a potential for customer actions being taken based on modified or incomplete information. Similarly, unauthorized modification or deletion of customer-supplied information can result in government mishandling of interactions with customers. If this occurs on a large-scale serious damage to public confidence in the agency may result. In such cases, a ***moderate*** integrity may be associated with customer service information.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for customer service information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to the customer service information. The effects of disruption of access to or use of customer service information can usually be In addition, customer service *operations* are not typically tolerant of delay. Even temporary loss of availability of customer service information is likely to disrupt customer *operations*. In most cases, disruption of access to customer service information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Availability Impact Determination: While most outages will result in only limited adverse effects on government operations, repeated outages can have a serious adverse effect on public confidence in the agency. In such cases, the availability impact might be ***moderate***.

Recommended Availability Impact Level: The provisional availability impact level recommended for customer service information is ***low***.

### C.2.6.2 Official Information Dissemination Information Type

Official Information Dissemination includes all efforts to provide official government information to external stakeholders through the use of various types of media, such as video, paper, web, etc. The recommended security categorization for the official information dissemination information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of official information dissemination information on the ability of responsible agencies to provide official Federal government information to external stakeholders through the use of various communications media. Official information dissemination information is usually in the public domain and poses no confidentiality impact.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for official information dissemination information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. In general, the adverse effects of unauthorized modification or destruction of official information dissemination information on overall agency mission functions will be limited.

Special Factors Affecting Integrity Impact Determination: There is a potential for customer actions taken based on modified or incomplete information. In addition, unauthorized modification or destruction of official information dissemination information may result in distribution of false and misleading information (e.g., modified web pages, electronic mail, video). Such events can adversely affect operations or public confidence in the agency. This can significantly degrade the official information dissemination mission capability. In such cases, a ***moderate*** integrity impact may exist. Also, the more serious integrity impacts become increasingly likely as E-government initiatives progress.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for official information dissemination information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to the official information dissemination information. Official information dissemination *processes* are generally tolerant of limited delays. However, even temporary loss of availability of official information dissemination information is likely to have an adverse effect on *public confidence* in the agency. In most cases, disruption of access to official information dissemination information can be expected to have only a limited adverse effect on overall agency operations, agency assets, or individuals.

Special Factors Affecting Availability Impact Determination: While most cases will result in only limited consequences, repeated outages can have a serious adverse effect on public confidence in the agency. This can significantly degrade the official information dissemination mission capability. In such cases, the availability impact might be ***moderate***.

Recommended Availability Impact Level: The provisional availability impact level recommended for official information dissemination information is ***low***.

### C.2.6.3 Product Outreach Information Type

Product Outreach relates to the marketing of government services products, and programs to the general public in an attempt to promote awareness and increase the number of customers/beneficiaries of those services and programs. The recommended security categorization for the product outreach information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of product outreach information on the ability of responsible agencies to market government services products, and programs to the general public in an attempt to promote awareness and increase the number of customers/beneficiaries of those services and programs. Product outreach information is usually in the public domain and poses no confidentiality impact.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for product outreach information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. In most cases, the adverse effect of unauthorized modification or destruction of product outreach information on overall agency mission functions will be limited.

Special Factors Affecting Integrity Impact Determination: The unauthorized modification or destruction of product outreach information may result in distribution of false and misleading information. Such events may adversely affect operations or public confidence in the agency and may significantly degrade the product marketing mission capability. In such cases, a ***moderate*** integrity impact may exist.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for product outreach information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to the product outreach information. Product outreach *processes* are generally tolerant of limited delays. In most cases, disruption of access to product outreach information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The provisional availability impact level recommended for product outreach information is ***low***.

### C.2.6.4 Public Relations Information Type

Public Relations activities involve the efforts to promote an organizations image through the effective handling of citizen concerns. The recommended security categorization for the public relations information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of public relations information on the ability of responsible agencies to promote an organizations image through the effective handling of citizen concerns. Public relations information itself is usually in the public domain and poses no confidentiality impact.

Special Factors Affecting Confidentiality Impact Determination: Internal correspondence associated with development of public relations information can contain information, the unauthorized disclosure of which can have a serious adverse effect on agency operations. This can result in assignment of a ***moderate*** impact level to such information.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for public relations information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. In most cases, the adverse effects of unauthorized modification or destruction of public relations information on overall agency mission functions will be limited.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of public relations information may result in distribution of false and misleading information. Such events can be expected to adversely affect operations and/or public confidence in the agency. This can significantly degrade the public relations mission capability. In such cases, a ***moderate*** integrity impact may exist.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for public relations information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to the public relations information. Public relations processes are generally tolerant of limited delays. In most cases, disruption of access to public relations information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The provisional availability impact level recommended for public relations information is ***low***.

## C.2.7 Legislative Relations

Legislative Relations involves activities aimed at the development, tracking, and amendment of public laws through the legislative branch of the Federal Government.

### C.2.7.1 Legislation Tracking Information Type

Legislation Tracking involves following legislation from conception to adoption. The recommended security categorization for the legislation tracking information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of legislation tracking information on the ability of responsible agencies to follow legislation from conception to adoption. Legislation tracking information itself is usually in the public domain and poses no confidentiality impact.

Special Factors Affecting Confidentiality Impact Determination: In some cases, internal correspondence associated with legislation tracking information can contain information, that if improperly disclosed, will have a serious adverse effect on agency relationships with other agencies and with the legislative branch. This can result in assignment of a ***moderate*** impact level to such information.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for legislation tracking information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. In most cases, the adverse effects of unauthorized modification or destruction of legislation tracking information on overall agency mission functions will be limited.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for legislation tracking information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to the legislation tracking information. Legislation tracking *processes* are generally tolerant of limited delays. In most cases, disruption of access to legislation tracking information will have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The provisional availability impact level recommended for legislation tracking information is ***low***.

### C.2.7.2 Legislation Testimony Information Type

Legislation Testimony involves activities associated with providing testimony/evidence in support or, or opposition to, legislation from conception to adoption. Subject to exception conditions described below, the recommended security categorization for the legislation testimony information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of legislation testimony information on the ability of responsible agencies to provide testimony/evidence in support or, or opposition to, legislation from conception to adoption. Most testimony regarding legislation is in the public domain, and even premature release should result in no more than limited harm to agency assets, personnel, or operations.

Special Factors Affecting Confidentiality Impact Determination: The effects of loss of confidentiality of some information applicable to pending testimony may result in attempts by competing interests to influence and/or impede a specific legislative process. The consequences to agency programs and of the ability of an agency to perform its mission can be very serious. Premature public release of draft testimony before internal coordination and review has been conducted can result in unnecessary criticism of the proposed testimony and damage public confidence in the agency. These consequences are particularly likely where the release includes unedited internal commentary and discussion. The results of unauthorized disclosure of information to the public can imperil specific agency programs, but a consequent loss of public confidence can do persistent harm to an agency's ability to effectively perform its mission. This can result in assignment of a ***moderate*** impact level to such information. Some information associated with legislative testimony is classified *national security information* and is outside the scope of this guideline.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for legislation testimony information is ***low***.

#### Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information.

Unauthorized modification or destruction of information affecting external publication of testimony associated with legislation (e.g., web pages, electronic mail) may adversely affect inter-agency relationships, relations with Congress, or public confidence in the agency. However, damage to the mission would usually be limited.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for legislation testimony information is ***low***.

#### Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to the legislation testimony information. The legislation testimony processes are usually tolerant of delays.

Special Factors Affecting Availability Impact Determination: Excessive recovery delays can result in damage to agency reputation and to interests associated with specific legislation. This can result in assignment of a ***moderate*** impact level to such information.

Recommended Availability Impact Level: The provisional availability impact level recommended for legislation testimony information is ***low***.

### C.2.7.3 Proposal Development Information Type

Proposal Development involves drafting proposed legislation that creates or amends laws subject to Congressional legislative action. Subject to exception conditions described below, the recommended security categorization for the proposal development information type is as follows:

Security Category = {(confidentiality, Moderate), (integrity, Low), (availability, Low)}

#### Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of proposal development information on the ability of responsible agencies to draft proposed legislation that creates or amends laws subject to Congressional legislative action. Legislation is normally in the public domain. However, the effects of loss of confidentiality of background information used in the development of proposed legislation or of early drafts of proposed legislation could result in attempts by competing interests to influence and/or impede a specific legislative process. The consequences to agency programs and of the ability of an agency to perform its mission can be very serious. Premature public release of proposed legislation before internal coordination and review has been conducted can result in unnecessary criticism of the proposed legislation and even damage public confidence in the agency. These consequences are particularly likely where the release includes unedited internal commentary and discussion. In general, unauthorized disclosure of much legislative proposal information, particularly in early phases of the process, is likely to result in serious harm to agency assets or operations.

Special Factors Affecting Confidentiality Impact Determination: Some proposal development information used by specific Federal agencies (e.g., homeland security, law enforcement, defense, intelligence community) is very sensitive or classified *national security information*. *National security information* is outside the scope of this guideline. The sensitivity level recommended for the very sensitive information is ***high***. If the proposal development information is moved to the public domain, the confidentiality impact level becomes Not Applicable (NA).

Recommended Confidentiality Impact Level: In order to accommodate event-driven consequences of unauthorized disclosure of pre-release drafts, the provisional confidentiality impact level recommended for proposal development information is ***moderate***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information.

Unauthorized modification or destruction of information affecting external publication of proposed legislation (e.g., web pages, electronic mail) might adversely affect inter-agency relationships, relations with Congress, or public confidence in the agency. However, damage to the mission would usually be limited.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for proposal development information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to the proposal development information. Proposal development *processes* are usually tolerant of delays.

Special Factors Affecting Availability Impact Determination: Excessive recovery delays can result in damage to agency reputation and to interests associated with specific legislation. This can result in assignment of a ***moderate*** impact level to such information.

Recommended Availability Impact Level: The provisional availability impact level recommended for proposal development information is ***low***.

### C.2.7.4 Congressional Liaison Operations Information Type

Congressional Liaison Operations involves all activities associated with supporting the formal relationship between a Federal Agency and the U.S. Congress. Subject to exception conditions described below, the recommended security categorization for the Congressional liaison information type is as follows:

Security Category = {(confidentiality, Moderate), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of Congressional liaison information on the ability of responsible agencies to support their formal relationships with U.S.

Congress. The effects of loss of confidentiality of information associated with Congressional liaison can facilitate attempts by competing interests to influence and/or impede a specific legislative process or poison inter-branch relations. The consequences to agency programs and even of the ability of an agency to perform its mission can be very serious. Premature public release of information associated with Congressional liaison before internal coordination and review has been conducted can result in unnecessary criticism of the preliminary data or positions, and even damage public confidence in the agency. These consequences are particularly likely where the release includes unedited internal commentary and discussion. In general, unauthorized disclosure of much Congressional liaison information is likely to result in serious harm to agency assets and/or operations. If the Congressional liaison information is moved to the public domain, the confidentiality impact level becomes Not Applicable (NA).

Special Factors Affecting Confidentiality Impact Determination: Some Congressional liaison information used by Federal agencies (e.g., homeland security, law enforcement, defense, intelligence community) is very sensitive or even classified *national security information*. *National security information* is outside the scope of this guideline. The sensitivity level associated with the very sensitive information is ***high***.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for Congressional liaison information is ***moderate***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for Congressional liaison information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to the Congressional liaison information. Congressional liaison *processes* are usually tolerant of delays.

Special Factors Affecting Availability Impact Determination: Excessive recovery delays can result in damage to agency reputation and to interests associated with specific legislation. This can result in assignment of a ***moderate*** impact level to such information.

Recommended Availability Impact Level: The provisional availability impact level recommended for Congressional liaison information is ***low***.

### C.2.8 General Government

General Government involves the overhead costs of the Federal Government, including legislative and executive activities; provision of central fiscal, personnel, and property activities; and the provision of services that cannot reasonably be classified in any other service support area. As a normal rule, all activities reasonably or closely associated with other service support areas or information types shall be included in those service support areas or information types rather than listed as a part of general government. This service support area is reserved for central government management operations; most service delivery (mission-based) management activities would not be included here. Unlike the other service support functions, some general government information types are associated with specific organizations (e.g., Department of the Treasury, Executive Office of the President, Internal Revenue Service).

### C.2.8.1 Central Fiscal Operations Information Type

Central Fiscal Operations includes the fiscal operations that the Department of Treasury performs on behalf of the Government.[14] [Note: Tax-related functions are associated with the Taxation Management information type.] Impacts to some information and information systems associated with central fiscal operations may affect the security of the critical banking and finance infrastructure. In most cases, the effect on public welfare of a loss of central fiscal operations functionality can be expected to be delayed rather than immediate. The potential for consequent loss of human life or of major national assets is low. . The provisional security categorization recommended for the central fiscal operations information type is as follows:

Security Category = {(confidentiality, Moderate), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of central fiscal operations information on the fiscal operations that the Department of Treasury performs on behalf of the Government. The effects of loss of confidentiality can reasonably be expected to jeopardize relationships and administrative actions necessary to mission fulfillment and/or to seriously damage public confidence in the agency. For example, the unauthorized disclosure of investigative and enforcement information can have serious economic impact on both individual companies and the broader market place (e.g., short-term stock market perturbations). The consequences of such unauthorized disclosures may have a serious adverse effect on public confidence in the agency.

Special Factors Affecting Confidentiality Impact Determination: Where the operations in question involve liaison with law enforcement or homeland security organizations, the consequences of unauthorized disclosure can imperil operations critical to the security of human life, critical infrastructure protection, ore the protection of key national assets. For those operations, the consequences to key financial infrastructure elements can be serious to severe. In such cases, the associated confidentiality impact level will be ***high***.

Recommended Confidentiality Impact Level: The confidentiality impact level recommended for most central fiscal operations information is ***moderate***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information.

Unauthorized modification or destruction of information affecting external communications that include central fiscal operations information (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited.

[14] Central fiscal operations focus on central Federal government functions rather than on central agency functions.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for central fiscal operations information is normally ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to the central fiscal operations information. Central fiscal operations *processes* are usually tolerant of delays.

Recommended Availability Impact Level: The provisional availability impact level recommended for central fiscal operations information is ***low***.

### C.2.8.2 Legislative Functions Information Type

Legislative functions include the service support activities associated with costs of the Legislative Branch other than the Tax Court, the Library of Congress, and the Government Printing Office revolving fund. The recommended security categorization for the legislative service support information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of legislative functions information on the ability of responsible agencies to provide service support activities associated with costs of the Legislative Branch other than the Tax Court, the Library of Congress, and the Government Printing Office revolving fund. The effects of loss of confidentiality of information associated with legislative functions can be expected to have only a limited impact on Federal government assets, operations, or personnel welfare.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for legislative functions information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. Misunderstandings resulting from modified information that is actually exchanged can usually be resolved and any resulting damage to the support function from modified information that is exchanged would usually be limited.

Unauthorized modification or destruction of information affecting external publication of legislative service support information (e.g., web pages, electronic mail) may adversely affect inter-agency relationships, relations with Congress, or public confidence in the agency. However, damage to the mission would usually be limited.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for legislative functions information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to the legislative service support information. Legislative functions processes are usually tolerant of delays.

Special Factors Affecting Availability Impact Determination: Excessive recovery delays can result in damage to agency reputation and to interests associated with specific legislation. This can result in assignment of a ***moderate*** impact level to such information.

Recommended Availability Impact Level: The provisional availability impact level recommended for legislative functions information is ***low***.

### C.2.8.3 Executive Functions Information Type

Subject to exception conditions described below, the recommended provisional security categorization for the executive information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level associated with the executive information type is associated with executive functions. The effects of loss of confidentiality of policies and guidance during the formative stage can result in attempts by affected entities and other interested parties to influence and/or impede the policy and guidance development process. Premature public release of formative policies and guidance before internal coordination and review can result in unnecessary damage to public confidence in the executive office. These consequences may occur when the release includes unedited internal commentary and discussion.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for executive functions information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information.

Unauthorized modification or destruction of information affecting external communications that contain executive information (e.g., web pages, electronic mail) may adversely affect public confidence in the government.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for executive information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to the executive information.

Recommended Availability Impact Level: The provisional availability impact level recommended for executive functions information is ***low***.

### C.2.8.4 Central Property Management Information Type

Central Property Management involves most of the operations of the General Services Administration. The following recommended provisional security categorization of central property management information is particularly subject to change where critical infrastructure elements or key national assets are involved:

Security Category = {(confidentiality, Low[15]), (integrity, Low), (availability, Low[16])}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of central property management information on the ability of the General Services Administration to acquire, provide, and centrally administer offices buildings, fleets, machinery, and other capital assets and consumable supplies used by the Federal government. The consequences of unauthorized disclosure of most central property management information are likely to have only a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Unauthorized disclosure of information associated with very large procurements can result in fraud, waste, abuse, and/or legal proceedings that can have a serious to severe effect on Federal government assets and operations. Also, information associated with acquisition, maintenance, administration, and operation of many Federal government office buildings, transportation fleets, and operational facilities can be of material use to criminals seeking to gain access to Federal facilities to facilitate or perpetrate fraud, theft, or some other criminal enterprise. In this case, unauthorized disclosure of information can have a serious adverse effect on agency operations, agency assets, or individuals. The consequent confidentiality impact would be at least ***moderate.***

Information associated with maintenance, administration, and operation of other Federal government facilities can be of material use to terrorists seeking to penetrate and/or commandeer such facilities as part of operations intended to harm critical infrastructures, key national assets, or people. Examples of more potentially damaging information include architectural, maintenance and administrative information that might permit either covert pedestrian or unimpeded vehicular access to government buildings (e.g., Congressional office buildings, FBI Headquarters, the National Archives, Smithsonian Institution buildings, dams, nuclear power plants, etc.). In such cases, the confidentiality impact level may be ***high***.

[Some information is classified as *national security* and is outside the scope of this guideline.] Anticipated or realized unauthorized disclosure of one agency's central property management information by GSA could result in negative impacts on cross-jurisdictional coordination within the central property management infrastructure and the general effectiveness of organizations tasked with acquiring and managing government facilities and supplies.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for central property management information is ***low***.

[15] Impact level is usually ***high*** where safety of major critical infrastructure components or key national assets is at stake.

[16] Impact level is usually ***moderate*** to ***high*** in emergency situations where time-critical processes affecting human safety or major assets are involved.

#### Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. In addition, the consequences of unauthorized modification or destruction of central property management information usually depends on the urgency with which the information is needed or the immediacy with which the information is used. In most cases, it is unlikely that the information will be time-critical or acted upon immediately.

Unauthorized modification or destruction of information affecting external publication of central property management information (e.g., web pages, electronic mail) may adversely affect public confidence in the agency. However, damage to the mission would usually be limited.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for central property management information is ***low***.

#### Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to the central property management information. The functions supported by most central property management information are tolerant of delays. Typically, the disruption of access to central property management information will have a limited adverse effect on agency operations (including mission functions and public confidence in the agency), agency assets, or individuals.

Special Factors Affecting Availability Impact Determination: Exceptions may include emergency response aspects of disaster management. In such cases, delays measured in hours can cost lives and major property damage. Consequently, the availability impact level associated with unauthorized modification or destruction of central property management information needed to respond to emergencies may be ***high***.

Recommended Availability Impact Level: The provisional availability impact level recommended for central property management information is ***low***.

### C.2.8.5 Central Personnel Management Information Type

Central Personnel Management involves most of the operating activities of the Office of Personnel Management and related agencies. The recommended security categorization for the central personnel management information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

#### Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of central personnel management information on the ability of the Office of Personnel Management (OPM) to build a high quality and diverse Federal workforce, based on merit system principles. Central personnel management information includes human resources management and consulting services, education and leadership development services, and investigation services. The unauthorized disclosure of most central personnel management information will have only a limited adverse effect on agency operations, assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Very sensitive information is typically personal information subject to the Privacy Act of 1974. (The Privacy Act Information provisional impact levels are documented in the Personal Identity and Authentication information type.) Such information will often be assigned a ***moderate*** confidentiality impact level. Some information associated with investigative services may be particularly sensitive and require a ***high*** confidentiality impact level.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for central personnel management information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of undetected unauthorized modification or destruction of central personnel management information can conceivably disrupt central personnel management operations (e.g., (e.g., by modifying sensitive private personal information or compromising confidentiality mechanisms).

Unauthorized modification or destruction of information affecting external publication of central personnel management information (e.g., web pages, electronic mail) may adversely affect public confidence in the government. However, damage to the mission would usually be limited.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for central personnel management information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to the central personnel management information. Central personnel management *processes* are generally tolerant of reasonable delays. In most cases, disruption of access to central personnel management information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The provisional availability impact level recommended for central personnel management information is ***low***.

### C.2.8.6 Taxation Management Information Type

Taxation Management includes activities associated with the implementation of the Internal Revenue Code and the collection of taxes in the United States and abroad. The recommended security categorization for the taxation management information type is as follows:

Security Category = {(confidentiality, Moderate), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of taxation management information on the ability of the Internal Revenue Service (IRS) to enforce the Internal Revenue

Code and to collect taxes in the United States and abroad. The IRS *Guidebook for Information Sensitivity Analysis* provides guidelines for identifying IRS Official Use Only (OUO) Information. Sensitive information is identified in the IRM as any information which if lost, stolen, (accessed), or altered without proper authorization may adversely affect Service operations. The IRM states that unauthorized disclosure of sensitive information may cause lawsuits against Service officials as well as the Service, unwanted notoriety for the Service, and public distrust of the Service's ability to protect such information – all of which may result in an increase in noncompliance with tax laws. It notes that unauthorized release of information such as the name and address of an informant (in cases of tax evasion or fraud) may threaten a person's life.[17] Additionally, sensitive information is defined in Section 25.10 of the IRM as information that requires protection due to the risk or magnitude of loss that could result from inadvertent or deliberate disclosure of the information. Sensitive information includes information whose improper use could adversely affect the ability of the agency to accomplish its mission, proprietary information, records about individuals that require protection under the Privacy Act, and information not releasable under the Freedom of Information Act. The IRS OUO guideline notes that prevention of unauthorized disclosure of information revealing internal matters, the disclosure of which would risk circumvention of a legal requirement or agency rules and regulations has assumed an increasingly important role in homeland security. Unauthorized disclosure of sensitive or private IRS information can be expected to have a serious effect on both the welfare of individuals and public confidence in the government.

Special Factors Affecting Confidentiality Impact Determination: In cases where unauthorized disclosure of taxation information can impede anti-terrorism or other homeland security activities or endanger the lives of agents or informants, the confidentiality impact level is ***high***.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for taxation management information is ***moderate***.

### Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. In addition, the consequences of unauthorized modification or destruction of taxation management information may depend on the urgency with which the information is needed or the immediacy with which the information is used. In most cases, it is unlikely that the information will be needed urgently or acted upon immediately. Also, the adverse effects of unauthorized modification or destruction of taxation management information on overall agency mission functions is expected to be limited.

Special Factors Affecting Integrity Impact Determination: There is a potential for tax code enforcement, other law enforcement, or anti-terrorism actions being taken based on modified or incomplete information. Also, unauthorized modification or destruction of taxation management information may result in distribution of false and misleading information. Such events can be expected to adversely affect individuals, operations, and/or public confidence in the agency. This can significantly degrade the taxation management mission capability. In extreme cases (e.g., misidentification of an informant), the consequences can be life threatening. In such cases, a ***high*** integrity impact may exist.

[17] Such information would have a ***high*** confidentiality default confidentiality impact rating.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for taxation management information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to the taxation management information. Taxation management processes are generally tolerant of limited delays. In most cases, disruption of access to taxation management information can be expected to have only a limited adverse effect on overall agency operations, agency assets, or individuals. However, even temporary loss of availability of taxation management information is likely to have an adverse effect on *public confidence* in the agency and on Federal government cash flow.

Special Factors Affecting Availability Impact Determination: While most cases will result in only limited consequences, repeated disruptions can have a serious adverse effect on public confidence in the agency. This can significantly degrade the taxation management mission capability. In such cases, the availability impact might be ***moderate***. Loss of availability of significant amounts of taxation management information over long periods of time can do serious harm to Federal government operations. The economic ramifications would potentially be severe.

Recommended Availability Impact Level: The provisional availability impact level recommended for taxation management information is ***low***.

### C.2.8.7 Central Records and Statistics Management Information Type

Central Records and Statistics Management involves the operations surrounding the management of official documents, statistics, and records for the entire Federal Government. This information type is intended to include information and information systems associated with the management of records and statistics for the Federal government as a whole, such as the records management performed by NARA or the statistics and data collection performed by the Bureau of the Census. Note: Many agencies perform records and statistics management for a particular business function and as such should be mapped to the service support, management, or mission area associated with that business function. The central records and statistics management information type is intended for functions performed on behalf of the entire Federal government. The recommended security categorization for the central records and statistics management information type is as follows:

Security Category = {(confidentiality, Moderate), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of central records and statistics management information on the ability of responsible agencies to manage official documents, statistics, and records for the entire Federal Government. Unauthorized disclosure of raw data and other source information for central records and statistics management operations is likely to violate the Privacy Act of 1974 and other regulations applicable to the dissemination of personal and government information. (The provisional impact levels for personnel information are documented in the Personal Identity and Authentication, Income, Representative Payee, and Entitlement Event information types.)

Special Factors Affecting Confidentiality Impact Determination: Unauthorized disclosure of some centrally managed records can pose a threat to human life or a loss of major assets. In such cases, the confidentiality impact is ***high***.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for central records and statistics management information is ***moderate***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. In addition, the consequences of unauthorized modification or destruction of central records and statistics management information may depend on the urgency with which the information is needed or the immediacy with which the information is used. In most cases, it is unlikely that the information will be time-critical or acted upon immediately.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for central records and statistics management information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to the central records and statistics management information. Central records and statistics management *processes* are generally tolerant of reasonable delays. Generally, disruption of access to central records and statistics management information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The provisional availability impact level recommended for central records and statistics management information is ***low***.

### C.2.8.8 Income Information Information Type

Income information includes all the wages, self-employment earnings, savings data and other financial resources information that is needed to help determine the amount of Retirement, Survivor, or Disability benefits that individuals may be entitled to receive or not receive from the Supplementary Security Income or RSDI Title II Programs. In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability of income information on the ability of the Federal government to identify citizen entitlements and obligations and to protect individuals against identity theft and the Federal government against fraud. The recommended security categorization for the income information type is as follows:

Security Category = {(confidentiality, Moderate), (integrity, Moderate), (availability, Moderate)}

Confidentiality

The confidentiality impact level is based on the effects of unauthorized disclosure of income information on the ability of the Federal government to identify citizen entitlements and obligations and to protect individuals against identity theft and the Federal government against fraud. Unauthorized disclosure of raw data and other source information for benefits determination and revenue collection operations is likely to violate the Privacy Act of 1974 and other regulations applicable to the dissemination of personal and government information. Unauthorized disclosure of centrally managed income information can have a serious adverse effect on agency missions. Therefore, for agencies that manage large income information involving records of the general public, the provisional confidentiality impact level can be expected to be at least ***moderate***.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for income information is ***moderate***.

### Integrity

The integrity impact level is based on the specific purpose to which income information is put; and not on the time required to detect the modification or destruction of information. In the case of very large data bases containing income information relating to the general public, there is a significant probability that erroneous actions will be taken affecting the benefits entitlements or liabilities (e.g., tax liabilities) of large numbers of individuals. This can result in at least short-term financial hardship for citizens. It can also be expected to result in very serious disruption of the agency operations due to large time and resource requirements for taking corrective actions. In such cases, the integrity impact level would be at least ***moderate***.

Special Factors Affecting Integrity Impact Determination: In the case of smaller organizations, and where the information affected is limited to employees, the consequences may justify only a ***low*** provisional impact rating.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for income information is ***moderate***.

### Availability

The availability impact level is based on the specific purpose to which income information is put; and not on the time required to re-establish access to the income information. Benefits determination and liability calculation (e.g., taxation) *processes* are generally tolerant of reasonable delays. In many cases, disruption of access to income information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Availability Impact Determination: In the case of very large data bases containing income information relating to the general public, there is a significant probability that processing delays will affect the benefits entitlements or liabilities (e.g., tax liabilities) of large numbers of individuals. The larger the number of records affected, the longer the delays that can be expected to result. This can result in financial hardship for citizens and in serious disruption of the agency operations due to large time and resource requirements for backlog processing. In such cases, the availability impact level would be at least ***moderate***. In the case of permanent loss of records, the impact might even be ***high***.

Recommended Availability Impact Level: The provisional availability impact level recommended for income information is ***moderate***.

### C.2.8.9 Personal Identity and Authentication Information Information Type

Personal identity and authentication information includes that information necessary to ensure that all persons who are potentially entitled to receive any federal benefit are enumerated and identified so that Federal agencies can have reasonable assurance that they are paying or communicating with the right individuals. This information include individual citizen's Social Security Numbers, names, dates of birth, places of birth, parents' names, etc.[18] The recommended security categorization for the personal identity and authentication information type is as follows:

Security Category = {(confidentiality, Moderate), (integrity, Moderate), (availability, Moderate)}

Confidentiality

The confidentiality impact level is based on the effects of unauthorized disclosure of personal identity and authentication information on the ability of Federal agencies to determine that communications with and payments to individuals are being made with or to the correct individuals - and to protect individuals against identity theft and the Federal government against fraud. Unauthorized disclosure of raw data and other source information for identity authentication operations is likely to violate the Privacy Act of 1974 and other regulations applicable to the dissemination of personal and government information. There are many cases in which unauthorized disclosure of personal identity and authentication information will have only a limited adverse effect on government operations, assets, or individuals. However, the potential for use of such information by criminals to perpetrate identity theft and related fraud can do serious harm to individuals. Unauthorized disclosure of centrally managed personal identity and authentication information, such as passport and visa control databases can have a serious adverse effect on agency missions.

Special Factors Affecting Confidentiality Impact Determination: For agencies that manage large income information involving records of the general public, the provisional confidentiality impact level can be expected to be at least ***moderate***. Where personal identity and authentication information is used in controlling access to facilities (e.g., Federal facilities, critical infrastructure facilities, key national assets) or for border control purposes, the consequences of unauthorized disclosure that permits credentials forgery can justify a ***high*** impact assignment.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for personal identity and authentication information is ***moderate***.

Integrity

The integrity impact level is based on the specific purpose to which personal identity and authentication information is put; and not on the time required to detect the modification or destruction of information. In the case of very large databases containing personal identity and authentication information relating to the general public, there is a significant probability that erroneous actions will be taken affecting benefits entitlements of or access to facilities by large numbers of individuals. In the case of benefits, this can result in at least short-term financial

[18] Persons conducting sensitive or payment related business with the government must identify themselves to the level prescribed by appropriate governing directives using such data.

hardship for citizens. It can also be expected to result in very serious disruption of the agency operations due to large time and resource requirements for taking corrective actions.

Special Factors Affecting Integrity Impact Determination: In the case of smaller organizations, and where the information affected is limited to employees, there will still be an impact, but the consequences may justify only a ***low*** provisional impact rating. Where a data modification permits access to facilities (or ingress into the United States) by individuals to whom access should be prohibited, the integrity impact could be ***high***.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for personal identity and authentication information is ***moderate***.

Availability

The availability impact level is based on the specific purpose to which personal identity and authentication information is put; and not on the time required to re-establish access to the personal identity and authentication information. Benefits determination *processes* are generally tolerant of reasonable delays. In many cases, disruption of access to personal identity and authentication information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Availability Impact Determination: In the case of very large data bases containing personal identity and authentication information relating to the general public, there is a significant probability that processing delays will affect the benefits entitlements of or access to facilities by large numbers of individuals. The larger the number of records affected, the longer the delays that can be expected to result. This can result in financial hardship for citizens and in serious disruption of the agency operations due to large time and resource requirements for backlog processing. In such cases, the availability impact level would be at least ***moderate***. In the case of permanent loss of records or access to facilities by emergency personnel, the impact might even be ***high***.

Recommended Availability Impact Level: The provisional availability impact level recommended for personal identity and authentication information is ***moderate***.

### C.2.8.10 Entitlement Event Information Information Type

Entitlement event information includes information about events such as death and date of occurrence, date of a disabling event and the relating data that can reasonably prove the severity of such disability, proof of age for retirement benefits, birth and relationship of spouse and/or children who may be entitled to benefits only as auxiliaries of the primary beneficiary, and other related information needed to process a claim for benefits. This also includes means-related information required to administer all the means related benefits associated with the Title XVI (Supplementary Security Income Program) and the new drug provisions of the recently revised Medicare Program. The recommended security categorization for the entitlement event information type is as follows:

Security Category = {(confidentiality, Moderate), (integrity, Moderate), (availability, Moderate)}

### Confidentiality

The confidentiality impact level is based on the effects of unauthorized disclosure of entitlement event information on the ability of the Federal government to establish qualifications of individuals to receive government benefits - and to protect individuals and the Federal government against fraud.   Unauthorized disclosure of raw data and other source information for entitlement operations is likely to violate the Privacy Act of 1974 and other regulations applicable to the dissemination of personal information.

Unauthorized disclosure of centrally managed entitlement event information can have a serious adverse effect on agency missions.  Therefore for agencies that manage large income information involving records of the general public, the provisional confidentiality impact level can be expected to be at least ***moderate***.

Recommended Confidentiality Impact Level:  The provisional confidentiality impact level recommended for entitlement event information is ***moderate***.

### Integrity

The integrity impact level is based on the specific use of the entitlement event information and not on the time required to detect the modification or destruction of information.  In the case of very large databases containing entitlement event information relating to the general public, there is a significant probability that erroneous actions will be taken affecting the benefits entitlements of large numbers of individuals.  This can result in at least short-term financial hardship for citizens.  It can also be expected to result in serious disruption of the agency operations due to the time and resource requirements for taking corrective actions.  In such cases, the integrity impact level would be at least ***moderate***.

Special Factors Affecting Integrity Impact Determination:  In the case of smaller organizations, and where the information affected is limited to employees, the consequences may justify only a ***low*** provisional impact rating.

Recommended Integrity Impact Level:  The provisional integrity impact level recommended for entitlement event information is ***moderate***.

### Availability

The availability impact level is based on the specific use of the entitlement event information and not on the time required to re-establish access to the income information.  Benefits determination *processes* are generally tolerant of reasonable delays.  In many cases, disruption of access to entitlement event information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Availability Impact Determination:  In the case of very large data bases containing entitlement event information relating to the general public, there is a significant probability that processing delays will affect the benefits entitlements of large numbers of individuals.  The larger the number of records affected, the longer the delays that can be expected to result.  This can result in financial hardship for citizens.  It can also result in very serious disruption of the agency operations due to large time and resource requirements for backlog processing.  In such cases, the availability impact level would be at least ***moderate***.  In the case of permanent loss of records, the impact might even be ***high***.

Recommended Availability Impact Level: The provisional availability impact level recommended for income information is ***moderate***.

### C.2.8.11 Representative Payee Information Information Type

Representative payee information includes the information required to determine the need for representative payees and the data that is gathered to make the determination of who should serve as the representative payee for all beneficiaries of federal benefits who are unable to manage their own funds. This also includes accountability information required to provide reasonable assurance that the funds are being used appropriately for the well being of entitled individuals. The recommended security categorization for the representative payee information type is as follows:

Security Category = {(confidentiality, Moderate), (integrity, Moderate), (availability, Moderate)}

Confidentiality

The confidentiality impact level is based on the effects of unauthorized disclosure of representative payee information on the ability of the Federal government to determine that entitlement funds are being used appropriately for the well being of entitled individuals - and to protect individuals against identity theft and the Federal government against fraud. Unauthorized disclosure of data for representative payee operations is likely to violate the Privacy Act of 1974 and other regulations applicable to the dissemination of personal information.

Unauthorized disclosure of centrally managed representative payee information can have a serious adverse effect on agency missions and on large numbers of individuals. Therefore, in the case of large representative payee information databases, the provisional confidentiality impact level can be expected to be at least ***moderate***.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for representative payee information is ***moderate***.

Integrity

The integrity impact level is based on the specific use of the payee information and not on the time required to detect the modification or destruction of information. In the case of very large databases containing representative payee information relating to the general public, there is a significant probability that erroneous actions will be taken affecting the benefits payments to large numbers of individuals. This can result in at least short-term financial hardship for our most vulnerable citizens. Loss of integrity can result in serious disruption of the agency operations. In such cases, the integrity impact level would be at least ***moderate***.

Special Factors Affecting Integrity Impact Determination: In the case of fraudulent diversion of payments intended for particularly dependent individuals, there can be life-threatening consequences. In such cases, a ***high*** integrity impact rating may be justified.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for representative payee information is ***moderate***.

Availability

The availability impact level is based on the specific use of the representative payee information and not on the time required to re-establish access to the representative payee information. Benefits payment *processes* are not necessarily tolerant of delays. In many cases, disruption of access to representative payee information can be expected to have a very serious adverse effect on individuals.

Special Factors Affecting Availability Impact Determination: In the case of very large data bases containing representative payee information relating to the general public, there is a significant probability that processing delays will affect the benefits payments to large numbers of individuals. The larger the number of records affected, the longer the delays that can be expected to result. This can result in financial hardship for some individuals and in serious disruption of agency operations. In such cases, the availability impact level would be at least ***moderate***. In the case of permanent loss of records, the impact might even be ***high***.

Recommended Availability Impact Level: The provisional availability impact level recommended for representative payee information is ***moderate***.

### C.2.8.12 General Information Information Type

An additional *management and support* sub-function information type has been defined to address General Information as a catch-all information type that may not be defined by the FEA BRM. As such, agencies may find it necessary to identify additional information types not defined in the BRM and assign impact levels to those types. Agency personnel may uniquely identify information types using a FIPS 199 process to identify information not contained neatly in the FEA BRM.

Not all of these information types are likely to have the same impact levels. The impacts to some information types will jeopardize system functionality and the agency mission more than other information types. General Information impact levels must be assessed in the context of the agencies mission.

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is based on the effects of unauthorized disclosure of representative general information on the ability of the agency to accomplish its mission.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for general information is ***low***.

Integrity

The integrity impact level is based on the specific use of the general information and not on the time required to detect the modification or destruction of information.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for general information is ***low***.

Availability

The availability impact level is based on the specific use of the general information and not on the time required to re-establish access to the general information.

Recommended Availability Impact Level: The provisional availability impact level recommended for general information is ***low***.

## C.3 Rationale and Factors for Government Resource Management Information

Resource management functions are the back office support activities that enable the government to operate effectively. Security objectives and impacts for resource management functions are determined by the direct service missions and constituencies ultimately being supported. It is likely that all Federal government information systems store, process, and operate under the control of IT infrastructure maintenance information (e.g., password files and file and network access settings). A basic set of security controls will apply to this information and processes to combat potential corruption, misuse, or abuse of system information and processes.

### C.3.1 Administrative Management

Administrative Management involves the day-to-day management and maintenance of the internal infrastructure. Administrative information is usually routine and is relatively low impact. However, some administrative management information is either very sensitive (e.g., logistics management for nuclear or other hazardous materials, security management information, and security clearance management information) or critical (e.g., inventory control and logistics management information needed to support time-critical operations). *National security information* is outside the scope of this guideline. [See Appendix A, Glossary of Terms, for a definition of *national security information/systems*.] Routine administrative management information systems that do not process classified information are not usually designated *national security systems*, even if they are critical to the direct fulfillment of military or intelligence missions.

#### C.3.1.1 Facilities, Fleet, and Equipment Management Information Type

Facilities, Fleet, and Equipment management involves the maintenance, administration, certification, and operation of office buildings, fleets, machinery, and other capital assets considered as possessions of the Federal government. Impacts to some information and information systems associated with facilities, fleet, and equipment management may affect the security of some key national assets (e.g., nuclear power plants, dams, and other government facilities). The following recommended provisional categorization of the facilities, fleet, and equipment management information type is particularly subject to change where critical infrastructure elements or key national assets are involved:

Security Category = {(confidentiality, Low[19]), (integrity, Low[20]), (availability, Low[20])}

[19] Impact level is usually ***high*** where safety of major critical infrastructure components or key national assets is at stake.

### Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of facilities, fleet, and equipment management information on the ability of responsible agencies to maintain, administer, and operate offices buildings, fleets, machinery, and other capital assets of the Federal government. The consequences of unauthorized disclosure of most facilities, fleet, and equipment management information are likely to have only a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Information associated with maintenance, administration, and operation of many Federal government office buildings, transportation fleets, and operational facilities can be of material use to criminals seeking to gain access to Federal facilities in order to facilitate or perpetrate fraud, theft, or some other criminal enterprise (e.g., extract inmates from Federal detention facilities). In this case, unauthorized disclosure of information can have a serious adverse effect on agency operations, agency assets, or individuals. The consequent confidentiality impact would be at least ***moderate.***

Information associated with maintenance, administration, and operation of other Federal government office buildings, transportation fleets, and operational facilities can be of material use to terrorists seeking to penetrate and/or commandeer such facilities as part of operations intended to harm critical infrastructures, key national assets, or people. Examples of this information include information that reveals specific measures respecting limiting access to and operation of government aircraft, maintenance and administrative information that might permit either covert pedestrian or unimpeded vehicular access to government buildings (e.g., Congressional office buildings, FBI Headquarters, the National Archives, Smithsonian Institution buildings, dams, nuclear power plants, etc.), and schedules/itineraries of government surface transportation fleets (e.g., for transport of executive personnel or hazardous materials). In these cases, the confidentiality impact must be considered to be ***high***.

[Some information regarding transportation and storage of nuclear materials is classified as *national security related* and is outside the scope of this guideline. Other information, such as Nuclear Regulatory Commission "SAFEGUARDS" information is not *national security information,* but must have a ***high*** confidentiality impact level.]

Anticipated or realized unauthorized disclosure of one agency's facilities, fleet, and equipment management information by another agency could result in negative impacts on cross-jurisdictional coordination within the facilities, fleet, and equipment management infrastructure and the general effectiveness of organizations tasked with facilities, fleet, and/or equipment management.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for facilities, fleet, and equipment management information is ***low***.

### Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. In addition, the

[20] Impact level is usually ***moderate*** to ***high*** in emergency situations where time-critical processes affecting human safety or major assets are involved.

consequences of unauthorized modification to or destruction of facilities, fleet, and equipment management information may depend on the urgency with which the information is needed or the immediacy with which the information is used.  In most cases, it is unlikely that the information will be time-critical or acted upon immediately.

Special Factors Affecting Integrity Impact Determination:  Exceptions may include emergency response aspects of disaster management or leadership protection.  In such cases, the integrity impact level associated with unauthorized modification or destruction of facilities, fleet, and equipment management information can be ***high***.

Recommended Integrity Impact Level:  The provisional integrity impact level recommended for facilities, fleet, and equipment management information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to the facilities, fleet, and equipment management information.  Functions supported by most facilities, fleet, and equipment management information are tolerant of delays. Typically, disruption of access to facilities, fleet, and equipment management information has a limited adverse effect on agency operations (including mission functions and public confidence in the agency), agency assets, or individuals.

Special Factors Affecting Availability Impact Determination:  Exceptions may include emergency response aspects of disaster management or leadership protection.  In such cases, delays measured in seconds can cost lives and major property damage.   Consequently, the availability impact level associated with unauthorized modification or destruction of facilities, fleet, and equipment management information needed to respond to emergencies will be ***high***.

Recommended Availability Impact Level:  The provisional availability impact level recommended for facilities, fleet, and equipment management information is ***low***.

### C.3.1.2 Help Desk Services Information Type

Help Desk Services involves the management of a service center to respond to government employees' technical and administrative questions. Subject to exception conditions described below, the recommended provisional security categorization for the help desk service information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of help desk service information on the ability of responsible agencies to manage of service center responses to government employees' technical and administrative questions.  The consequences of unauthorized disclosure of most help desk service information are likely to have only a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination:  Information associated with service center responses can provide useful information to adversaries seeking to penetrate Federal systems. If the contents or functions of a system have sufficient sensitivity and/or criticality, a ***moderate*** or ***high*** impact level may be considered for help desk information.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for help desk service information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. In addition, the consequences of unauthorized modification to or destruction of help desk service information usually depends on the urgency with which the information is needed or the immediacy with which the information is used. In most cases, it is unlikely that the information will be time-critical or acted upon immediately.

Special Factors Affecting Integrity Impact Determination: In relatively few cases would the consequences of unauthorized modification of help desk information that is acted upon immediately result in more than limited damage to agency operations or assets. Exceptions may include bogus information regarding operation of communications processors, data base systems, or other systems necessary to emergency response aspects of disaster management, criminal apprehension, air traffic control or other time-critical missions. In such cases, a ***moderate*** or ***high*** integrity impact level might be considered for unauthorized modification or destruction of help desk service information.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for help desk service information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to help desk service information. Typically, disruption of access to help desk service information will have a limited adverse effect on agency operations (including mission functions and public confidence in the agency), agency assets, or individuals.

Special Factors Affecting Availability Impact Determination: Exceptions may include emergency response components of disaster management or other time-critical functions (e.g., some systems that support air traffic control functions). Consequently, the availability impact level associated with unauthorized modification or destruction of help desk service information needed to respond to emergencies can be ***high***.

Recommended Availability Impact Level: The provisional availability impact level recommended for help desk service information is ***low***.

### C.3.1.3 Security Management Information Type

Security Management involves the physical protection of an organization's personnel, assets, and facilities (including security clearance management). Impacts to some information and information systems associated with security management may affect the security of some critical infrastructure elements and key national assets (e.g., nuclear power plants, dams, and other government facilities). Impact levels associated with security information directly relate to the potential threat to human life associated with the asset(s) being protected (e.g., consequences to the public of terrorist access to dams or nuclear power plants). The following recommended categorization of the security management information type is subject to change where critical infrastructure elements or key national assets are involved:

Security Category = {(confidentiality, Moderate), (integrity, Moderate), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of security management information on the ability of responsible organizations to physically protect their personnel, assets, and facilities. The consequences of unauthorized disclosure of most security management information depend on the likelihood that the information might jeopardize the physical security of an organization's assets and the value, and potential for damage of the assets being protected.

Information associated with the physical security of many Federal government office buildings, transportation fleets, and operational facilities can be of material use to criminals seeking to gain access to Federal facilities in order to perpetrate a major crime (e.g., extraction of inmates from Federal detention facilities, theft of commodities market projections, access to information associated with a felony criminal investigation or prosecution, theft of blank license issuing facilities and/or materials, access to competition-sensitive information associated with major procurements, undetected access to national archives or museum properties, access to currency printing facilities or materials, theft of major currency or bullion storage facilities). In such cases, unauthorized disclosure of information can have a serious adverse effect on agency operations, agency assets, or individuals. Unauthorized disclosure of one agency's security management information by another agency could result in negative impacts on cross-jurisdictional coordination within the security management infrastructure and the general effectiveness of organizations tasked with physical protection of Federal facilities. The consequences of physical protection failures at most Federal facilities are more likely to result in serious[21] adverse effects.

Special Factors Affecting Confidentiality Impact Determination: Information associated with security management at other Federal government office buildings, transportation fleets, and operational facilities can be of material use to terrorists seeking to penetrate and/or commandeer such facilities as part of operations intended to harm critical infrastructures, key national assets, or people. Examples of more potentially damaging information includes information that reveals specific measures for protecting government aircraft, information that might permit access that creates an opportunity to bomb a government building (e.g., Congressional office buildings, FBI Headquarters, the National Archives, Smithsonian Institution buildings, dams, nuclear power plants, etc.), and leadership protection details that could result in assassination opportunities. In these cases, the confidentiality impact must be ***high***.

Unauthorized disclosure of security management information that can be reasonably expected to pose a serious threat to human life (including those of security guards) must also be assigned a ***high*** confidentiality impact. [Security management information associated with some Federal government assets is classified. The classified information is *national security related* and is

[21] A loss of confidentiality that causes a significant degradation in mission capability, places the agency at a significant disadvantage, or results in major damage to assets, requiring extensive corrective actions or repairs.

outside the scope of this guideline.] Other security management information, such as that affecting Nuclear Regulatory Commission "SAFEGUARDS" or Internal Revenue Service "Limited For Official Use Only" information is not *national security information*, but must be treated as having ***high*** confidentiality impact.

Recommended Confidentiality Impact Level: The confidentiality impact level recommended for most security management information is ***moderate***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of security management information may depend on the urgency with which the information is needed or the immediacy with which the information is used. In cases of intrusion indications, security management information can be time-critical.

The consequences of unauthorized modification or destruction of time-critical security management information can reasonably be expected to result in physical security vulnerabilities. The range of potential consequences is covered above in *Confidentiality*.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for most security management information is ***moderate***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to the security management information. Functions supported by most security management information are tolerant of delays. Typically, disruption of access to security management information will have a limited adverse effect on agency operations (including mission functions and public confidence in the agency), agency assets, or individuals.

Special Factors Affecting Availability Impact Determination: Exceptions may include alarm and alert communications and interconnections for security management systems and automated control systems that support security management processes (e.g., door and gate operations in buildings to which access is limited such as detention facilities and many Federal office buildings For these exceptions, the data is time-critical. The availability impact level associated with unauthorized modification or destruction of such alarm, alert, and automated process security management information may be ***high***.

Recommended Availability Impact Level: The provisional availability impact level recommended for security management information is ***low***.

### C.3.1.4 Travel Information Type

Travel involves the activities associated with planning, preparing, and monitoring of business related travel for an organization's employees. The following security categorization is recommended for the travel information type:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

### Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of travel information on the abilities of responsible agencies to plan, prepare, and monitor business related travel for the organization's employees. Generally, the consequences of unauthorized disclosure of the majority of travel information will result in a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Unauthorized disclosure of employee identification information coupled with credit information (e.g., name, social security number, credit card number) can result in moderate to serious consequences for individuals and local organizations. The Privacy Act Information provisional impact levels are documented in the Personal Identity and Authentication information type.

Unauthorized disclosure of information concerning carrier/provider contract negotiations can have significant financial or legal consequences and put an agency at a serious disadvantage. Also, severe consequences may result from unauthorized disclosure of information regarding leadership travel plans that might jeopardize personnel security or the confidentiality of sensitive operations plans. In the most sensitive cases, the confidentiality impact level may be ***high***.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for travel information is ***low***.

### Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of travel information partially depends on the urgency with which the information is normally needed and the consequences of aborted or modified travel.

In the case of travel planning information, the effects of such modifications are generally limited with respect to agency mission capabilities or assets. There may be scenarios in which integrity compromise of travel information may expose Federal leadership to harm or endanger a sensitive or critical operation. However, most such scenarios are dealt with in the context of impacts to mission operations information (Appendix D).

Recommended Integrity Impact Level: The provisional integrity impact level recommended for travel information is ***low***.

### Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to the travel information. The nature of travel processes is usually tolerant of reasonable delays, at least on the agency mission scale.

Recommended Availability Impact Level: The provisional availability impact level recommended for travel information is ***low***.

#### C.3.1.5 Workplace Policy Development and Management Information Type (*Intra-Agency Only*)

Workplace policy development and management includes all activities required to develop and disseminate workplace policies such as dress codes, time reporting requirements, telecommuting, etc. The following security categorization is recommended for the workplace policy development and management information type:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of workplace policy development and management information on the abilities of responsible agencies to develop and disseminate workplace policies such as dress codes, time reporting requirements, and telecommuting. The consequences of unauthorized disclosure of the majority of workplace policy development and management information will result in a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for workplace policy development and management information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification to or destruction of workplace policy development and management information depends primarily on the criticality of the information with respect to agency mission capability, protection of agency assets, and safety of individuals. Typically, the effects of modification or deletion of this information are generally limited.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for workplace policy development and management information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to the workplace policy development and management information. Generally, workplace policy development and management processes are tolerant of reasonable delays.

Recommended Availability Impact Level: The provisional availability impact level recommended for workplace policy development and management information is ***low***.

### C.3.2 Financial Management

Financial management involves the aggregate set of accounting practices and procedures that allow for the accurate and effective handling of all government revenues, funding, and expenditures. Confidentiality impacts associated with financial management information are generally associated with the sensitivity of the existence of specific projects, programs, and/or technologies that might be revealed by unauthorized disclosure of information. For integrity, temporary successful frauds can affect agency image, and corrective actions are often disruptive to agency operations. Permanent loss/unavailability of financial management information can cripple agency operations.

### C.3.2.1 Assets and Liability Management Information Type

Assets and Liability Management provide accounting support for the management of assets and liabilities of the Federal government. Assets and liability management activities measure the total cost and revenue of Federal programs, and their various elements, activities and outputs. Assets and liability management is essential for providing accurate program measurement information, performance measures, and financial statements with verifiable reporting of the cost of activities. The recommended security categorization for the assets and liability management information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of assets and liability management information on the ability of responsible agencies to provide accounting support for the management of assets and liabilities of the Federal government. Generally, the unauthorized disclosure of assets and liability management information will have only a limited adverse effect on agency operations, assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Unauthorized disclosure of some asset and liability management information for programs that process high-impact information can assist some criminals to evade enforcement activities. Examples range from tax evasion resulting from unauthorized disclosure of information regarding audit budgets to unauthorized disclosure of budget details for specific border control, antiterrorism, or witness protection expenditures. Where actions taken based on unauthorized disclosure of assets and liability management details pose a threat to human life or a loss of major assets, the confidentiality impact is ***high***.

Recommended Confidentiality Impact Level: The recommended provisional confidentiality impact level for assets and liability management information is ***low***.

Integrity

The accuracy of assets and liability management information is essential to providing accurate program measurement information, performance measures, and financial statements with verifiable reporting of the cost of activities. The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. Also, the consequences of unauthorized modification or destruction of assets and liability management information may depend on the urgency with which the information is needed. Assets and liability management activities are not generally time-critical and a compromise would have only limited adverse effects on agency operations, agency assets, or individuals.

Special Factors Affecting Integrity Impact Determination: If reports based on modified or incomplete information are circulated, the adverse effect on mission functions and public confidence in the agency can be serious. In such cases, the integrity impact would be ***moderate***.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for assets and liability management information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to the assets and liability management information. Assets and liability management processes are generally tolerant of delay. Typically, disruption of access to assets and liability management information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The provisional availability impact level recommended for assets and liability management information is ***low***.

### C.3.2.2 Reporting and Information Information Type

Reporting and Information includes providing financial information, reporting and analysis of financial transactions. Financial reporting includes the activities necessary to support: management's fiduciary role; budget formulation and execution functions; fiscal management of program delivery and program decision making; and internal and external reporting requirements. The recommended security categorization for the "financial reporting and information" information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Moderate), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of financial reporting information on an agency's ability to provide financial information and reporting and analysis of financial transactions. Typically, the unauthorized disclosure of financial reporting information will have only a limited adverse effect on agency operations, assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Unauthorized disclosure of financial reporting information for programs that process high-impact information can give adversaries damaging insights into details of agency plans, priorities, and operations. In relatively rare cases, actions taken based on unauthorized disclosure of financial reporting details pose a threat to human life or a loss of major assets, so the confidentiality impact is ***high***.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for reporting and information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. Financial reporting activities are not generally time-critical. Many integrity compromises would result in limited adverse effects on agency operations, agency assets, or individuals.

If planning documents, proposals, or reports based on modified or incomplete information are circulated; the adverse effect on mission functions or public confidence in the agency can be serious. In most cases, serious adverse effects on agency operations, agency assets, or individuals can be expected. The extensive audit and investigative actions that often follow discovery of an agency's use of falsified financial reports or omission of financial reporting data can place the agency at a significant disadvantage.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for reporting and information is ***moderate***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to the assets and liability management information. Financial reporting processes are generally tolerant of delay. Typically, disruption of access to financial reporting information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The provisional availability impact recommended for reporting and information is ***low***.

### C.3.2.3 Funds Control Information Type

Funds Control includes the management of the Federal budget process including the development of plans and programs, budgets, and performance outputs as well as financing Federal programs and operations through appropriation and apportionment of direct and reimbursable spending authority, fund transfers, investments and other financing mechanisms. Funds control management includes the establishment of a system for ensuring an organization does not obligate or disburse funds in excess of those appropriated or authorized. The recommended security categorization for the funds control information type is as follows:

Security Category = {(confidentiality, Moderate), (integrity, Moderate), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of funds control information on the ability of responsible agencies to develop plans and programs, budgets, and performance outputs and outcomes; and to finance Federal programs and operations through appropriation and apportionment of direct and reimbursable spending authority, fund transfers, investments and other financing mechanisms.

In general, unauthorized disclosure of funds control information, particularly of budget allocations for specific programs or program elements, can be seriously detrimental to government interests in procurement processes. In many instances, such unauthorized disclosure is prohibited by executive order or by law (e.g., *Federal Acquisition Regulation*). Premature release of draft funds control information can yield advantages to competing interests and seriously endanger agency operations – or even agency mission.

Special Factors Affecting Confidentiality Impact Determination: Unauthorized disclosure of funds control information for programs that process classified or high-impact information can give adversaries damaging insights into details of agency plans, priorities, and operations. (Classified programs and systems are outside the scope of this guideline.) In rare cases, actions taken based on unauthorized disclosure of funds control details can pose a threat to human life or a loss of major assets, so the confidentiality impact would be ***high***.

Recommended Confidentiality Impact Level: While, in many cases, unauthorized disclosure of funds control information will have only a limited adverse effect on agency operations, assets, or individuals, the potential for serious harm is such that the provisional confidentiality impact level recommended for funds control information is ***moderate***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. Funds control activities are not generally time-critical. An accumulation of small changes to data or deletion of small entries can result in budget shortfalls or cases of excessive obligations or disbursements.

Recommended Integrity Impact Level: In most cases, the adverse effects of consequent negative publicity on mission functions, image or public confidence in the agency can be serious. Therefore, the provisional integrity impact level recommended for funds control information is ***moderate***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to the funds control information. Funds control processes are generally tolerant of delay. Typically, disruption of access to funds control information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The provisional availability impact level recommended for funds control information is ***low***.

### C.3.2.4 Accounting Information Type

Accounting entails accounting for assets, liabilities, fund balances, revenues and expenses associated with the maintenance of Federal funds and expenditure of Federal appropriations (Salaries and Expenses, Operation and Maintenance, Procurement, Working Capital, Trust Funds, etc.), in accordance with applicable Federal standards (FASAB, Treasury, OMB, GAO, etc.). The recommended security categorization for the accounting information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Moderate), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of accounting information on the abilities of government agencies to maintain Federal funds and expenditure of Federal appropriations in accordance with applicable Federal standards. Unauthorized disclosure of accounting information for programs that process classified or high-impact information can give adversaries damaging insights into details of agency plans, priorities, and operations. In most cases, unauthorized disclosure of accounting information will have only a limited adverse effect on agency operations, assets, or individuals. (Classified programs and systems are outside the scope of this guideline.)

Special Factors Affecting Confidentiality Impact Determination: In relatively rare cases, actions taken based on unauthorized disclosure of accounting details can pose a threat to human life or a loss of major assets, so the confidentiality impact would be ***high***.

In some cases, unauthorized disclosure of accounting information can violate proprietary information or other non-disclosure agreements. In such cases, the government may suffer not only a loss of public confidence, but may become vulnerable to legal actions. Where sensitive or proprietary information is involved, the impact of unauthorized disclosure is likely to be ***moderate***. Where the accounting information is involved in an audit associated with suspected fraud or other criminal activities, the investigation may be imperiled. Here too, the impact of unauthorized disclosure is likely to be ***moderate***.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for accounting information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. Accounting activities are not generally time-critical. An accumulation of small changes to data or deletion of small entries can result in cost overruns and other cases of excessive obligations or disbursements. In most cases, the adverse effects of consequent negative publicity and institution of corrective action programs on mission functions and public confidence in the agency can be serious.

Special Factors Affecting Integrity Impact Determination: In some cases, undetected integrity compromises can be extremely expensive to the government and its employees in terms of both monetary losses and loss of reputation.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for accounting information is ***moderate***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to the accounting information. Accounting processes are generally tolerant of delay. Typically, disruption of access to accounting information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The provisional availability impact level recommended for accounting information is ***low***.

### C.3.2.5 Payments Information Type

Payments include disbursements of Federal funds, via a variety of mechanisms, to Federal and private individuals, Federal agencies, state, local and international Governments, and the private sector, to effect payment for goods and services, or distribute entitlements, benefits, grants, subsidies, loans, or claims. Payment management provides appropriate control over all payments made by or on behalf of an organization, including but not limited to payments made to: vendors in accordance with contracts, purchase orders and other obligating documents; state governments under a variety of programs; employees for salaries and expense reimbursements; other Federal agencies for reimbursable work performed; individual citizens receiving Federal benefits; and recipients of Federal loans. The recommended security categorization for the payments information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Moderate), (availability, Low)}

### Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of payments information on the ability of responsible agencies to provide appropriate control over all payments made by or on behalf of an organization. In most cases, unauthorized disclosure of payments information will have only a limited adverse effect on agency operations, assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Payment information typically includes information needed for electronic payments such as bank account numbers. Unauthorized access to this type of information could result in significant financial loss for both the Federal government and its payees. Where payment activities are part of an agency's service delivery mission (e.g., payment of benefits), Privacy Act information and other information subject to statutory or regulatory dissemination controls must appear in the payment vehicles (e.g., name and social security number on check records). (The provisional impact levels for personnel information are documented in the Personal Identity and Authentication, Income, Representative Payee, and Entitlement Event information types.) In such cases, the confidentiality impact level can be at least ***moderate***. (See C.2.8.8.)

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for payments information is ***low***.

### Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. Payments activities are not generally time-critical. An accumulation of small changes to data or deletion of small entries can result in cost overruns and other cases of excessive disbursements. In most cases, the adverse effects of consequent negative publicity and institution of corrective action programs on mission functions or public confidence in the agency can be serious.

Special Factors Affecting Integrity Impact Determination: Where payment activities are part of an agency's service delivery mission (e.g., payment of benefits), the consequences of integrity compromises that result in failure of payments to go to the appropriate entity can range from minor to life-threatening. In such cases, the availability impact level can be ***high***. (See C.2.8.11.)

Recommended Integrity Impact Level: For most Federal government payment systems, the provisional integrity impact level recommended for payments information is ***moderate***.

### Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to the payments information. Payment processes are generally tolerant of delay. Typically, disruption of access to payments information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Availability Impact Determination: Where payment activities are part of an agency's service delivery mission (e.g., payment of benefits), the consequences of loss of information availability that result in failure of payments to go to the appropriate entity can range from minor to life-threatening. In such cases, the availability impact level can be ***moderate*** or ***high***. (See C.2.8.11.)

Recommended Availability Impact Level: For most Federal government payment systems, the provisional availability impact level recommended for payments information is ***low***.

#### C.3.2.6 Collections and Receivables Information Type

Collections and Receivables include deposits, fund transfers, and receipts for sales or service. Receivable management supports activities associated with recognizing and recording debts due to the Government, performing follow-up actions to collect on these debts, and recording cash receipts. The recommended security categorization for the collections and receivables information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Moderate), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of collections and receivables information on the ability of responsible agencies to recognize and record debts due to the Government, perform follow-up actions to collect on these debts, and record cash receipts. In most cases, unauthorized disclosure of receivable management information will have only a limited adverse effect on agency operations, assets, or individuals.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for collections and receivables information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. An accumulation of small changes to data or deletion of small entries can result in revenue shortfalls. In most cases, the adverse effects of consequent negative publicity and institution of corrective action programs on mission functions or public confidence in the agency can be serious.

Recommended Integrity Impact Level: The provisional integrity impact recommended for collections and receivables information is ***moderate***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to the collections and receivables information. Collections and receivables processes are generally tolerant of delay. Typically, disruption of access to collections and receivables information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The provisional availability impact level recommended for collections and receivables information is ***low***.

### C.3.2.7 Cost Accounting/ Performance Measurement Information Type

Cost Accounting / Performance Measurement is the process of accumulating, measuring, analyzing, interpreting, and reporting cost information useful to both internal and external groups concerned with the way in which an organization uses, accounts for, safeguards, and controls its resources to meet its objectives. Cost accounting information is necessary in establishing strategic goals, measuring service efforts and accomplishments, and relating efforts to accomplishments. Also, cost accounting, financial accounting, and budgetary accounting all draw information from common data sources. The recommended security categorization for the cost accounting / performance measurement information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Moderate), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of cost accounting / performance measurement information on the ability of responsible agencies to process accumulating, measuring, analyzing, interpreting, and reporting cost information useful to both internal and external groups concerned with the way in which an organization uses, accounts for, safeguards, and controls its resources to meet its objectives, and will have only a limited adverse effect on agency operations, assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: In some cases, unauthorized disclosure of cost accounting / performance measurement information can violate proprietary information or other non-disclosure agreements. In such cases, the government may suffer not only a loss of public confidence, but may become vulnerable to legal actions. Where sensitive or proprietary information is involved, the impact of unauthorized disclosure is likely to be ***moderate***. Where the cost accounting information is involved in an audit associated with suspected fraud or other criminal activities, the investigation may be imperiled. Here too, the impact of unauthorized disclosure is likely to be ***moderate***.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for cost accounting / performance measurement information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information.

In most cases, the adverse effects of consequent negative publicity and institution of corrective action programs on mission functions or public confidence in the agency can be serious.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for cost accounting / performance measurement information is ***moderate***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to cost accounting / performance measurement information. Cost accounting / performance measurement processes are generally tolerant of delay. Typically, disruption of access to cost accounting / performance measurement information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The provisional availability impact level recommended for cost accounting / performance measurement information is ***low***.

## C.3.3 Human Resource Management

Human resource management activities involve all activities associated with the recruitment and management of personnel.

### C.3.3.1 HR Strategy Information Type

HR Strategy develops effective human capital management strategies to ensure federal organizations are able to recruit, select, develop, train, and manage a high-quality, productive workforce in accordance with merit system principles. This sub-function includes: conducting both internal and external environmental scans; developing human resources and human capital strategies and plans; establishing human resources policy and practices; managing current and future workforce competencies; developing workforce plans; developing succession plans; managing the human resources budget; providing human resources and human capital consultative support; and measuring and improving human resources performance. The recommended provisional security categorization for HR strategy information is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of HR strategy information on the ability of responsible agencies to develop effective human capital management strategies to ensure federal organizations are able to recruit, select, develop, train, and manage a high-quality, productive workforce in accordance with merit system principles, and will have only a limited adverse effect on agency operations, assets, or individuals. The consequences of unauthorized disclosure of the majority of HR strategy information will result in a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Where more sensitive information is involved, it will probably be personal information subject to the Privacy Act of 1974, the Health Insurance Portability and Accountability Act of 1996, or other laws and executive orders affecting the dissemination of information regarding individuals. In such cases, the consequences of unauthorized disclosure of HR strategy information could be serious. In such cases, the confidentiality impact level might be ***moderate***. In a few cases (e.g., where some employees are potential targets for retaliation by criminal elements or targets of foreign intelligence organizations), unauthorized disclosure of some HR strategy information (e.g., succession plans, names, addresses, title, organization, dependents' information) can have life-threatening consequences and has a ***high*** confidentiality impact level.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for disclosure of HR strategy information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of HR strategy information depends mostly on the criticality of the information with respect to agency mission, protection of agency assets, and safety of individuals. Although there can be serious short-term effects for individuals, the effects of modifications or deletion of this information are generally limited with respect to agency mission capabilities or assets.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for HR strategy information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to HR strategy information. HR strategy processes are generally tolerant of delay. Typically, disruption of access HR strategy information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The provisional availability impact level recommended for HR strategy information is ***low***.

#### C.3.3.2 Staff Acquisition Information Type

Staff Acquisition establishes procedures for recruiting and selecting high-quality, productive employees with the right skills and competencies, in accordance with merit system principles. This sub-function includes: developing a staffing strategy and plan; establishing an applicant evaluation approach; announcing the vacancy, sourcing and evaluating candidates against the competency requirements for the position; initiating pre-employment activities; and hiring employees. The recommended provisional security categorization for staff acquisition information is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of staff acquisition information on the ability of responsible agencies to establish procedures for recruiting and selecting high-quality, productive employees with the right skills and competencies, in accordance with merit system principles will have only a limited adverse effect on agency operations, assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Where more sensitive information is involved, it will probably be personal information subject to the Privacy Act of 1974. The Privacy Act Information provisional impact levels are documented in the Personal Identity and

Authentication information type. This can result in assignment of a ***moderate*** impact level to such information.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for disclosure of staff acquisition information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of staff acquisition information depends mostly on the criticality of the information with respect to agency mission, protection of agency assets, and safety of individuals. Although there can be serious short-term effects for individuals, the effects of modifications or deletion of this information are generally limited with respect to agency mission capabilities or assets.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for staff acquisition information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to staff acquisition information. Staff acquisition processes are generally tolerant of delay. Typically, disruption of staff acquisition information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The provisional availability impact level recommended for staff acquisition information is ***low***.

### C.3.3.3 Organization & Position Management Information Type

Organization and Position Management designs, develops, and implements organizational and position structures that create a high-performance, competency-driven framework that both advances the agency mission and serves agency human capital needs. The recommended provisional security categorization for organization and position management information is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of organization and position management information on the ability of responsible agencies to design, develop, and implement organizational and position structures creating a high-performance, competency-driven framework that both advances the agency mission and serves agency human capital needs. In most cases, unauthorized disclosure of organization and position management information will have only a limited adverse effect on agency operations, assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Where more sensitive information is involved, it will probably be personal information subject to the Privacy Act of 1974. The

Privacy Act Information provisional impact levels are documented in the Personal Identity and Authentication information type.  This can result in assignment of a ***moderate*** impact level to such information.

Recommended Confidentiality Impact Level:  The provisional confidentiality impact level recommended for disclosure of organization and position management information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information.  The consequences of unauthorized modification or destruction of organization and position management information depends mostly on the criticality of the information with respect to agency mission capability, protection of agency assets, and safety of individuals.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for organization and position management information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to organization and position management information. Organization and position management processes are generally tolerant of delay. Typically, disruption of organization and position management information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level:  The provisional availability impact level recommended for organization and position management information is ***low***.

### C.3.3.4 Compensation Management Information Type

Compensation Management designs, develops, and implements compensation programs that attract, retain and fairly compensate agency employees. In addition, designs, develops, and implements pay for performance compensation programs to recognize and reward high performance, with both base pay increases and performance bonus payments. This sub-function includes: developing and implementing compensation programs; administering bonus and monetary awards programs; administering pay changes; managing time, attendance, leave and pay; and managing payroll.  The recommended provisional security categorization for compensation management information is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of compensation management information on the ability of responsible agencies to design, develop, and implements compensation programs that attract, retain and fairly compensate agency employees will have only a limited adverse effect on agency operations, assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination:  Where more sensitive information is involved, it will probably be personal information subject to the Privacy Act of 1974.  The

Privacy Act Information provisional impact levels are documented in the Personal Identity and Authentication information type. In a few cases (e.g., where some employees are potential targets for retaliation by criminal elements or targets of foreign intelligence organizations), unauthorized disclosure of some compensation management information (e.g., name, address, title, organization, dependents' information) can have life-threatening consequences and has a ***high*** confidentiality impact level.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for disclosure compensation management information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. Compensation management activities are not generally time-critical.

Special Factors Affecting Integrity Impact Determination: An accumulation of small changes to data or deletion of small entries can result in excessive disbursements of payroll, bonus and monetary awards or affects pay changes, time and attendance, etc. In some cases, the adverse effects of consequent negative publicity on mission functions or public confidence in the agency can be serious. In some other cases, integrity compromises that adversely affect a significant subset of the workforce can result in staff issues and work stoppages that adversely affect the agency's mission. Where interruptions to agency missions can have serious or life-threatening consequences for individuals, the impacts of integrity compromises can be ***moderate*** or even ***high***.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for compensation management information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to compensation management information. Compensation management processes are generally tolerant of delay. Typically, disruption compensation management information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The provisional availability impact level recommended compensation management information is ***low***.

### C.3.3.5 Benefits Management Information Type

Benefits Management designs, develops, and implements benefit programs that attract, retain and support current and former agency employees. This sub-function includes: establishing and communicating benefits programs; processing benefits actions; and interacting as necessary with third party benefits providers. The recommended provisional security categorization for benefits management information is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

#### Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure benefits management information on the ability of responsible agencies to design, develop, and implement benefit programs that attract, retain and support current and former agency employees will have only a limited adverse effect on agency operations, assets, or individuals. The consequences of unauthorized disclosure of the majority of benefits management information will result in a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Where more sensitive information is involved, it will probably be personal information subject to the Privacy Act of 1974, the Health Insurance Portability and Accountability Act of 1996, or information that is proprietary to a corporation or other organization. In such cases, the consequences of unauthorized disclosure of benefits management information could be serious (particularly in cases of exposure of large data bases that might reveal private medical information or facilitate identity theft or other financial fraud). (The provisional impact levels for personnel information are documented in the Personal Identity and Authentication, Income, and Entitlement Event information types.) In such cases, the confidentiality impact level would be ***moderate***.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for disclosure of benefits management information is ***low***.

#### Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of benefits management information depends mostly on the criticality of the information with respect to agency mission capability, protection of agency assets, and safety of individuals. In general, the effects of modifications or deletion of this information are generally limited with respect to agency mission capabilities or assets.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for benefits management information is ***low***.

#### Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to benefits management information. Benefits management processes are generally tolerant of delay. Typically, disruption benefits management information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The provisional availability impact level recommended benefits management information is ***low***.

### C.3.3.6 Employee Performance Management Information Type

Employee Performance Management designs, develops, and implements a comprehensive performance management approach to ensure agency employees are demonstrating competencies required of their work assignments. Design, develop and implement a comprehensive performance management strategy that enables managers to make distinctions in performance and links individual performance to agency goal and mission accomplishment. This sub-function also includes managing employee performance at the individual level and evaluating the overall effectiveness of the agency's employee development approach.  The recommended provisional security categorization for employee performance management information is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of employee performance management information regarding the agencies ability to design, develop, and implement a comprehensive performance management approach to ensure agency employees are demonstrating competencies required of their work assignments.  In most cases, unauthorized disclosure of employee performance management information will have only a limited adverse effect on agency operations, assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Where more sensitive information is involved, it will probably be personal information subject to the Privacy Act of 1974.  The Privacy Act Information provisional impact levels are documented in the Personal Identity and Authentication information type.  This can result in assignment of a ***moderate*** impact level to such information.

Recommended Confidentiality Impact Level:  The provisional confidentiality impact level recommended for disclosure of employee performance management information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information.  The consequences of unauthorized modification or destruction of employee performance management information depends mostly on the criticality of the information with respect to agency mission capability, protection of agency assets, and safety of individuals. Although there can be serious short-term effects for individuals, the effects of modifications or deletion of this information are generally limited with respect to agency mission capabilities or assets.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for employee performance management information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to employee performance management information. Employee performance management processes are generally tolerant of delay. Typically, disruption employee performance management information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level:  The provisional availability impact level recommended employee performance management information is ***low***.

### C.3.3.7 Employee Relations Information Type

Employee Relations designs, develops, and implements programs that strive to maintain an effective employer-employee relationship that balance the agency's needs against its employees' rights. This sub-function includes: addressing employee misconduct; addressing employee performance problems; managing administrative grievances; providing employee accommodation; administering employees assistance programs; participating in administrative third party proceedings; and determining candidate and applicant suitability. The recommended provisional security categorization for employee relations information is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of employee relations information on the ability of responsible agencies to design, develop, and implement programs that strive to maintain an effective employer-employee relationship that balance the agency's needs against its employees' rights. The consequences of unauthorized disclosure of the employee relations information will result in a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Where more sensitive information is involved, it will probably be personal information subject to the Privacy Act of 1974, the Health Insurance Portability and Accountability Act of 1996, or other laws and executive orders affecting the dissemination of information regarding individuals. (The provisional impact levels for personnel information are documented in the Personal Identity and Authentication.) In such cases, the consequences of unauthorized disclosure of Employee Relations information could be serious. In such cases, the confidentiality impact level might be ***moderate***.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for disclosure of employee relations information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of employee relations information depends mostly on the criticality of the information with respect to agency mission capability, protection of agency assets, and safety of individuals. Although there can be serious short-term effects for individuals, the effects of modifications or deletion of this information are generally limited with respect to agency mission capabilities or assets.

Special Factors Affecting Integrity Impact Determination: In some cases, integrity compromises that adversely affect a significant subset of the workforce can result in work stoppages that adversely affect the agency's mission. Where interruptions to agency missions can have serious or life-threatening consequences for individuals, the impacts of integrity compromises can be ***moderate*** or even ***high***.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for employee relations information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access employee relations information. Employee relations processes are generally tolerant of delay. Typically, disruption employee relations information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The provisional availability impact level recommended employee relations information is ***low***.

### C.3.3.8 Labor Relations Information Type

Labor Relations manages the relationship between the agency and its unions and bargaining units. This includes negotiating and administering labor contracts and collective bargaining agreements; managing negotiated grievances; and participating in negotiated third party proceedings. The recommended provisional security categorization for labor relations information is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of labor relations information on the ability of responsible agencies to manage the relationship between the agency and its unions and bargaining units. This includes negotiating and administering labor contracts and collective bargaining agreements; managing negotiated grievances; and participating in negotiated third party proceedings. The consequences of unauthorized disclosure of the majority of labor relations information will result in a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: In cases where the consequences of unauthorized disclosure of labor relations information could seriously affect the agencies mission capability, protection of agency assets, and safety of individuals, the confidentiality impact level might be ***moderate***

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for disclosure of labor relations information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of labor relations information depends mostly on the criticality of the information with respect to agency mission capability, protection of agency assets, and safety of individuals. Although there can be serious short-term effects for individuals, the effects of modifications or deletion of this information are generally limited with respect to agency mission capabilities or assets.

Special Factors Affecting Integrity Impact Determination: In some cases (e.g., where an agency's mission is strongly dependent on organized labor), integrity compromises that adversely affect a significant subset of the workforce can result in work stoppages that adversely affect the agency's mission. Where interruptions to agency missions can have serious or life-threatening consequences for individuals, the impacts of integrity compromises can be ***moderate*** or even ***high***.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for labor relations information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to labor relations information. Labor relations processes are generally tolerant of delay. Typically, disruption labor relations information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Availability Impact Determination: In some cases (e.g., where an agency's mission is strongly dependent on organized labor), loss of availability of information that adversely affects a significant subset of the workforce can result in work stoppages that adversely affect the agency's mission. Where interruptions to agency missions can have serious or life-threatening consequences for individuals, the impacts of availability compromises can be ***moderate*** or even ***high***.

Recommended Availability Impact Level: The provisional availability impact level recommended labor relations information is ***low***.

### C.3.3.9 Separation Management Information Type

Separation Management conducts efficient and effective employee separation programs that assist employees in transitioning to non-Federal employment; facilitates the removal of unproductive, non-performing employees; and assists employees in transitioning to retirement. The recommended provisional security categorization for separation management information is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of separation management information on the ability of responsible agencies conducts efficient and effective employee separation programs that assist employees in transitioning to non-Federal employment; facilitates the removal of unproductive, non-performing employees; and assists employees in transitioning to retirement. In most cases, unauthorized disclosure of separation management information will have only a limited adverse effect on agency operations, assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Where more sensitive information is involved, it will probably be personal information subject to the Privacy Act of 1974. The Privacy Act Information provisional impact levels are documented in the Personal Identity and Authentication information type. This can result in assignment of a ***moderate*** impact level to such information.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for disclosure of separation management information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of separation management information is generally limited with respect to agency mission capabilities or assets.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for separation management information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access separation management. Separation management processes are generally tolerant of delay. Typically, disruption separation management information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The provisional availability impact level recommended separation management information is ***low***.

### C.3.3.10 Human Resources Development Information Type

Human Resources Development designs, develops, and implements a comprehensive employee development approach to ensure that agency employees have the right competencies and skills for current and future work assignments. This sub-function includes conducting employee development needs assessments; designing employee development programs; administering and delivering employee development programs; and evaluating the overall effectiveness of the agency's employee development approach. The recommended provisional security categorization for human resources development information is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of human resources development information on the ability of responsible agencies to design, develop, and comprehensive employee development approach to ensure that agency employees have the right competencies and skills for current and future work assignments. In most cases, unauthorized disclosure of human resource development information will have only a limited adverse effect on agency operations, assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Where more sensitive information is involved, it will probably be personal information subject to the Privacy Act of 1974. The Privacy Act Information provisional impact levels are documented in the Personal Identity and Authentication information type. This can result in assignment of a ***moderate*** impact level to such information.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for disclosure of human resources development information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of human resource development information depends mostly on the criticality of the information with respect to agency mission capability, protection of agency assets, and safety of individuals. Although there can be serious short-term effects for individuals, the effects of modifications or deletion of this information are generally limited with respect to agency mission capabilities or assets.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for human resources development information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish human resources development information. Human resources development information is generally tolerant of delay. Typically, disruption of human resources development information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The provisional availability impact level recommended human resources development information is ***low***.

### C.3.4 Supply Chain Management

Supply chain management involves the purchasing, tracking, and overall management of goods and services.

#### C.3.4.1 Goods Acquisition Information Type

Goods acquisition involves the procurement of physical goods, products, and capital assets to be used by the Federal government. The recommended security categorization for the goods acquisition information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of goods acquisition information on the ability of agencies to procure physical goods, products, and capital assets to be used by the Federal government. The consequences of unauthorized disclosure of most goods acquisition information will have only a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Unauthorized disclosure of information associated with large procurements can result in fraud, waste, abuse, and/or legal proceedings that can have a serious to severe effect on Federal government assets and operations. Also, information associated with acquisition of many Federal government facilities can be useful to criminals seeking to gain access to those facilities. In these cases, unauthorized disclosure of information can have a serious adverse effect on agency operations, agency assets, or individuals. The consequent confidentiality impact would range from ***moderate*** to ***high***. Also, unauthorized disclosure of one agency's goods acquisition information by another agency could result in negative impacts on cross-jurisdictional coordination within the goods acquisition infrastructure and the general effectiveness of organizations tasked with acquisition of government facilities and supplies. Additionally, some procurement information associated with proposals is proprietary. In the case of competitive procurements, much information associated with unsuccessful bids remains proprietary following award of the contract (e.g., pricing information). Unauthorized disclosure of proprietary information can have serious consequences for agencies and have at least a ***moderate*** confidentiality impact level. Some procurement information is classified. The classified information is *national security related* and is outside the scope of this guideline.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for goods acquisition information is ***low***.

### Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of goods acquisition information usually depends on the urgency with which the information is needed or the immediacy with which the information is used

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external publication of goods acquisition information (e.g., web pages, electronic mail) may adversely affect public confidence in the agency. However, damage to the mission would usually be limited. Unauthorized modification or destruction of information relating to procurement actions (particularly proposal information) can result in serious disruption of procurement processes that can be important or even critical to agency operations. In such cases, the integrity impact level can be ***moderate*** or even ***high***.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for modification or destruction of most goods acquisition information is ***low***.

### Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to the goods acquisition information. Functions and processes supported by most goods acquisition information are tolerant of delays i.e., the data supporting the functions/processes are not time-critical. Typically, disruption of access will have a limited adverse effect on agency operations (including mission functions and public confidence in the agency), agency assets, or individuals.

Special Factors Affecting Availability Impact Determination: Exceptions may include emergency procurements necessary to support response aspects of disaster management. In such cases, delays may cost lives and major property damage. Consequently, the availability impact level associated with disruption of access to goods acquisition information needed to respond to emergencies may be ***high***.

Recommended Availability Impact Level: The provisional availability impact level recommended for goods acquisition information is ***low***.

### C.3.4.2 Inventory Control Information Type

Inventory control refers to the tracking of information related to procured assets and resources with regards to quantity, quality, and location. The recommended security categorization for the inventory control information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of inventory control information on the ability of agencies to track information related to procured assets and resources with regards to quantity, quality, and location. The consequences of unauthorized disclosure of most inventory control information are likely to have only a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Unauthorized disclosure of information associated with inventories of hazardous materials (e.g., radioactive materials, toxins, bio-hazardous items, explosives) can facilitate terrorist or other criminal activities that may result in serious effects on Federal government assets and operations and on the general public. In general, inventory control information can be of material use to criminals seeking to perpetrate fraud, theft, or some other criminal enterprise. In these cases too, unauthorized disclosure of information can have a serious adverse effect on agency operations, agency assets, or individuals. The consequent confidentiality impact of these types of criminal exploitation of unauthorized disclosure of inventory control information would range from ***moderate*** to ***high***. Also, unauthorized disclosure of one agency's inventory control information by another agency could result in negative impacts on cross-jurisdictional coordination within the inventory control infrastructure and the general effectiveness of organizations tasked with the distribution and accounting of government facilities and supplies. Some inventory control information is classified. The classified information is *national security related* and is outside the scope of this guideline.

Recommended Confidentiality Impact Level: Regardless of the ***moderate*** or ***high*** impact associated with unauthorized disclosure of some inventory control information, the provisional confidentiality impact level recommended for inventory control information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of inventory control information usually depends on the urgency with which the information is needed or the immediacy with which the information is used. In most cases, it is unlikely that the information will be needed urgently or acted upon immediately.

Unauthorized modification or destruction of information affecting external publication of inventory control information (e.g., web pages, electronic mail) may adversely affect public confidence in the agency. However, damage to the mission would usually be limited.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for inventory control information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to inventory control information. Functions and processes supported by most inventory control information are tolerant of delays i.e., the data supporting the functions/processes are not time-critical. Typically, disruption of access to inventory control information will have a limited adverse effect on agency operations (including mission functions and public confidence in the agency), agency assets, or individuals.

Special Factors Affecting Availability Impact Determination: Exceptions may include emergency requirements to access and distribute materials necessary for disaster management. In such cases, delays may cost lives and major property damage. Consequently, the impact level for inventory control information needed to respond to emergencies will be ***high***.

Recommended Availability Impact Level: The provisional availability impact level recommended for inventory control information is ***low***.

### C.3.4.3 Logistics Management Information Type

Logistics management involves the planning and tracking of personnel and their resources in relation to their availability and location. The recommended security categorization for the logistics management information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of logistics management information on the ability of agencies to plan and track the availability and location of personnel and their resources. The consequences of unauthorized disclosure of most logistics management information are likely to have only limited adverse effects on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Unauthorized disclosure of logistics information associated with homeland security, law enforcement and some transportation activities (e.g., air transport) can facilitate terrorist or other criminal activities that may result in serious on Federal government assets and operations and on the general public. Logistics management information associated with a broad range of mission areas can be of material use to criminals seeking to perpetrate fraud, theft, or other criminal enterprises. Also, this information is a key intelligence target for those seeking information on defense or law enforcement capabilities, dispositions and intent. In all these cases, the unauthorized disclosure of logistics management information may result in serious adverse effects on agency operations, agency assets, and individuals. Therefore, the confidentiality impact level for these types of criminal exploitation of unauthorized disclosure of logistics management information will range from ***moderate*** to ***high***. Some logistics management information is classified (e.g., some military logistics information). The classified information is *national security related* and is outside the scope of this guideline.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for most logistics management information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of logistics management information usually depends on the urgency with which the information is needed or the immediacy with which the information is used. In most cases, the information will not be needed urgently or acted upon immediately.

Unauthorized modification or destruction of information affecting external publication of logistics management information (e.g., web pages, electronic mail) may adversely affect public confidence in the agency. However, damage to the mission would usually be limited.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for logistics management information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to logistics management information. Functions and processes supported by most logistics management information are tolerant of delays i.e., the data supporting the functions/processes are not time-critical. Typically, disruption of access to logistics management information will have a limited adverse effect on agency operations (including mission functions and public confidence in the agency), agency assets, or individuals.

Special Factors Affecting Availability Impact Determination: Exceptions may include emergency requirements to deploy personnel and their resources to support disaster management. In such cases, delays may cost lives and major property damage. Consequently, the impact level for logistics management information needed to respond to emergencies will be ***high***.

Recommended Availability Impact Level: The availability impact level recommended for logistics management information is ***low***.

### C.3.4.4 Services Acquisition Information Type

Services acquisition involves the oversight and/or management of contractors and service providers from the private sector. The recommended security categorization for the services acquisition information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

### Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of services acquisition information on the ability of agencies to oversee and/or manage contractors and service providers from the private sector. The consequences of unauthorized disclosure of most services acquisition information are likely to have only a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Unauthorized disclosure of information associated with very large procurements can result in fraud, waste, abuse, and/or legal proceedings that can have a serious effect on Federal government assets and operations. Also, information associated with acquisition of some services (e.g., security or protection services) can be of material use to criminals seeking to gain access to Federal facilities or information in order to facilitate or perpetrate sabotage, murder, fraud, theft, or other criminal enterprises. In these cases, unauthorized disclosure of information can have a serious adverse effect on agency operations, agency assets, and/or individuals. The consequent confidentiality impact will range from ***moderate*** to ***high***. Additionally, some procurement information associated with proposals is proprietary. In the case of competitive procurements, much information associated with unsuccessful bids remains proprietary following award of the contract (e.g., pricing information). Unauthorized disclosure of proprietary information can have serious consequences for agencies and have at least a ***moderate*** confidentiality impact level. Some services procurement information is classified. The classified information is *national security related* and is outside the scope of this guideline.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for most services acquisition information is ***low***.

### Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of services acquisition information usually depends on the urgency with which the information is needed or the immediacy with which the information is used. In most cases, the information will not be needed urgently or acted upon immediately. Also, unauthorized modification or destruction of information affecting external publication of services acquisition information (e.g., web pages, electronic mail) may adversely affect public confidence in the agency. However, damage to the mission would usually be limited.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information relating to procurement actions (particularly proposal information) can result in serious disruption of procurement processes and loss of availability of services that can be important or even critical to agency operations. In such cases, the integrity impact level can be ***moderate*** or even ***high***.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for most services acquisition information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to services acquisition information. Functions and processes supported by most services acquisition information are tolerant of delays i.e., the data supporting the functions/processes are not time-critical. In most cases, disruption of access to services procurement information can be expected to have a limited adverse effect on agency operations (including mission functions and public confidence in the agency), agency assets, or individuals.

Recommended Availability Impact Level: The provisional availability impact level recommended for services acquisition information is ***low***.

### C.3.5 Information and Technology Management

IT management involves the coordination of IT resources and systems required to support or enable a citizen service. Impacts to information associated with the operation of IT systems generally need to be considered even when all mission-related information processed by the system is intended to be available to the general public. The relevant issues may be different for integrity and availability than for confidentiality. Information that has been made public, by definition, requires no confidentiality protection. In contrast, integrity and availability protection cannot be maintained for copies of information that have been distributed to the public. Integrity and availability assurance can only be maintained by maintaining copies of information in organization-controlled information systems.

#### C.3.5.1 System Development Information Type

System Development supports all activities associated with the in-house design and development of software applications. The recommended security categorization for the system development information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Moderate), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of system development information on the ability of responsible agencies to design and develop software applications in-house. In the system development phase, a system's security configuration baseline is established. In most cases, the system development information is not particularly sensitive and is distributed to the users. In general, disclosure of the system development information is likely to result in only limited adverse effects on the confidentiality of system information and processes.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for system development information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of system development information depend on the maximum aggregate sensitivity and criticality of the information and processes associated with the system.

Special Factors Affecting Integrity Impact Determination: The Recommended Integrity Impact Level may range from ***low*** to ***high*** to *national security information* (outside the scope of this guideline).

Recommended Integrity Impact Level: The provisional integrity impact level recommended for most system development information is ***moderate***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to system development information. Functions and processes supported by most system development information are not time-critical. That is, temporary disruption of access to system development information will usually have only a limited adverse effect on agency operations (including mission functions and public confidence in the agency), agency assets, or individuals.

Recommended Availability Impact Level: The provisional availability impact level recommended for system development information is ***low***.

#### C.3.5.2 Lifecycle/Change Management Information Type

Lifecycle/Change Management involves the processes that facilitate a smooth evolution, composition, and workforce transition of the design and implementation of changes to agency resources such as assets, methodologies, systems, or procedures. The recommended security categorization for the lifecycle/change management information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Moderate), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of lifecycle/change management information on the ability of responsible agencies to execute processes that facilitate a smooth evolution, composition, and workforce transition of the design and implementation of changes to agency resources such as assets, methodologies, systems, or procedures.

Special Factors Affecting Confidentiality Impact Determination: Unauthorized disclosure of some lifecycle/change management information can provide adversaries with intelligence information that may be useful in efforts to compromise the system. This can result in assignment of a ***moderate*** impact level to such information. Additionally, there are legislative mandates prohibiting unauthorized disclosure of trade secrets. Trade secrets will generally be assigned a ***moderate*** confidentiality impact level.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for lifecycle/change management information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of undetected or unauthorized modification or destruction of lifecycle/change management information depends on the maximum aggregate sensitivity and criticality of the information and processes associated with the system.

Special Factors Affecting Integrity Impact Determination: The Recommended Integrity Impact Level can range from ***low*** to ***high*** to *national security information* (outside the scope of this guideline).

Recommended Integrity Impact Level: The provisional integrity impact level recommended for lifecycle/change management information is ***moderate***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to lifecycle/change management information. Functions and processes supported by most lifecycle/change management information are not time-critical. That is, temporary disruption of access to lifecycle/change management information will usually have only a limited adverse effect on agency operations (including mission functions and public confidence in the agency), agency assets, or individuals.

Recommended Availability Impact Level: The provisional availability impact level recommended for lifecycle/change management information is ***low***.

### C.3.5.3 System Maintenance Information Type

System Maintenance supports all activities associated with the maintenance of in-house designed software applications. The recommended security categorization for the system maintenance information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Moderate), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of system maintenance information on the ability of responsible agencies to maintain in-house designed software applications. In most cases, system maintenance information is not particularly sensitive and is distributed to the users. In general, disclosure of system maintenance information is likely to result in only limited adverse effects on the confidentiality of system information and processes.

Recommended Confidentiality Impact Level: The provisional impact level recommended for system maintenance information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of system maintenance information can be particularly serious because specific modifications to system changes can be difficult to identify.

Special Factors Affecting Integrity Impact Determination: The consequences of undetected or unauthorized modification or destruction of system maintenance information may depend on the maximum aggregate sensitivity and criticality of the information and processes associated with the system. The Recommended Integrity Impact Level can range from ***low*** to ***high*** to *national security information* (outside the scope of this guideline).

Recommended Integrity Impact Level: The provisional integrity impact level recommended for system maintenance information is ***moderate***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to maintenance information. Functions and processes supported by most maintenance information are not time-critical. That is, temporary disruption of access to maintenance information will usually have only a limited adverse effect on agency operations (including mission functions and public confidence in the agency), agency assets, or individuals.

Recommended Availability Impact Level: The provisional availability impact level recommended for system maintenance information is ***low***.

### C.3.5.4 IT Infrastructure Maintenance Information Type

IT infrastructure maintenance involves the planning, design, implementation, and maintenance of an IT Infrastructure to effectively support automated needs (i.e. operating systems, applications software, platforms, networks, servers, printers, etc.). IT infrastructure maintenance also includes information systems configuration and security policy enforcement information. This information includes password files, network access rules and implementing files and/or switch setting, hardware and software configuration settings, and documentation that may affect access to the information system's data, programs, and/or processes. The impact levels associated with IT infrastructure maintenance information are primarily a function of the information processed in and through that infrastructure.

The IT Maintenance Information type represents a complex set of data elements that are used to secure the design, implementation, and maintenance of systems and networks. The security of each of these data elements is dependent on the security of the other data elements. Security compromise of one data element type will propagate to others.

The recommended security categorization for the IT infrastructure maintenance information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of IT infrastructure maintenance information on the ability of responsible agencies to plan, design, implement, and maintain an IT Infrastructure to effectively support automated needs (i.e. operating systems, applications software, platforms, networks, servers, printers, etc.). [See also Appendices C.3.5.5, IT Security Information and C.3.5.7, Information Management Information.] IT infrastructure maintenance also includes information systems configuration and security policy enforcement information. Unauthorized disclosure of some IT infrastructure maintenance information can lead to confidentiality compromise of information processed by the system (e.g., password files, file access tables, cryptographic keying information, network access rules, and hardware and software configuration settings, and documentation that may affect access to the information system's data, programs, and/or processes). As a result, the confidentiality impact associated with this information is that of the highest impact information processed by the system. Also, a higher confidentiality impact may be associated with information in aggregate than is associated with any single element of information.

Recommended Confidentiality Impact Level: Particularly in the case of passwords and cryptographic keys, the provisional impact level recommended for IT infrastructure maintenance information depends on the sensitivity and criticality of system information and processes. Although an individual organization's IT infrastructure maintenance information type base may include data elements that will require a higher rating, the recommended provisional impact is ***low***.

### Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of IT infrastructure maintenance information usually depends on the urgency with which the data processed in the IT infrastructure is needed or the time-critical nature of the data. In most cases, it is unlikely that the information will be needed urgently or acted upon immediately. In most cases, the consequences of unauthorized modification of IT infrastructure maintenance information will result in limited damage to agency operations or assets.

Special Factors Affecting Integrity Impact Determination: Exceptions may include incorrect information used for emergency response aspects of disaster management, criminal apprehension, air traffic control or other time-critical missions. In such cases, a ***moderate*** or ***high*** integrity impact level might be considered.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for IT infrastructure maintenance information is ***low***.

### Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to IT infrastructure maintenance information. Functions and processes supported by most IT infrastructure maintenance information are not time-critical. Also, disruption of access will have a limited adverse effect on agency operations (including mission functions and public confidence in the agency), agency assets, or individuals.

Special Factors Affecting Availability Impact Determination: Exceptions may include emergency response aspects of disaster management or other high load and time critical functions (e.g., some systems that support air traffic control functions). The effects of disruption of access to

IT infrastructure maintenance information or information systems may be to deny mission-critical IT resources to all affected organizations. The availability impact level associated with denial-of-service to IT infrastructure maintenance information needed to respond to emergencies or critical to public safety can be ***high***.

Recommended Availability Impact Level: The provisional availability impact level recommended for IT infrastructure maintenance information is ***low***.

### C.3.5.5 Information Security Information Type

IT Security involves all functions pertaining to the securing of Federal data and systems through the creation and definition of security policies, procedures and controls covering such services as identification, authentication, and non-repudiation. The recommended security categorization for the IT security information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Moderate), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of IT security information on the ability of responsible agencies to secure Federal data and systems through the creation and definition of security policies, procedures and controls covering such services as identification, authentication, and non-repudiation. In most cases, the security policy, procedures, and available controls are not particularly sensitive. Typically, the security information is used in initializing and implementing the controls (e.g., passwords, cryptographic keys) that need to be protected. In general, disclosure of the security policies, procedures, and controls will result in only limited adverse effects on the confidentiality of system information and processes.

Recommended Confidentiality Impact Level: The recommended provisional confidentiality impact level recommended for IT security information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for IT security information is ***moderate***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to IT security information. Temporary disruption of access to IT security information can usually be expected to have a limited adverse effect on agency operations (including mission functions and public confidence in the agency), agency assets, or individuals.

Recommended Availability Impact Level: The provisional availability impact level recommended for IT security information is ***low***.

### C.3.5.6 Record Retention Information Type

Records Retention involves the operations surrounding the management of the official documents and records for an agency. Subject to exception conditions described below, the recommended security categorization for the record retention information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of record retention information on the ability of responsible organizations to store, track, account for, maintain, retrieve, and disseminate official documents and records. When the data being retained belongs to one of the information types described in this guideline, the confidentiality impact assigned the data and system is at least that of the highest impact information type collected. Typically, the unauthorized disclosure of most business management information retained will have only a limited adverse effect on agency operations, assets, or individuals. *National security information* and *national security systems* are outside the scope of this guideline.

Special Factors Affecting Confidentiality Impact Determination: Where more sensitive information is involved, it will most commonly be personal information subject to the Privacy Act of 1974 or information that is proprietary to a corporation or other organization. The Privacy Act Information provisional impact levels are documented in the Personal Identity and Authentication information type. Such information will often be assigned a ***moderate*** confidentiality impact level. Where any of the information to be collected can reasonably be expected to have a ***high*** confidentiality impact level, then the record retention system must be assigned a ***high*** confidentiality impact level. In some cases, the impact assessment should consider that the aggregate of information retained might have a higher confidentiality impact than any individual information element.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for record retention information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information.

Special Factors Affecting Integrity Impact Determination: Where integrity compromise adversely affects the ability of an organization to access its records or results in erroneous back-up information or archives, the impact on agency operations can be serious. In such cases, the integrity impact level would be ***moderate***. In the case of large-scale archives or archives involving key national assets (e.g., national archives), the integrity impact can be particularly severe and the impact level would be ***high***.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for record retention information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to record retention information. Functions and processes supported by most record retention information are not time-critical. Record retention processes are generally tolerant of reasonable delays. In most cases, disruption of access to record retention information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Not many business management systems perform functions for which temporary loss of availability can cause significant degradation in mission capability, place the agency at a significant disadvantage, result in major damage to assets, or pose a threat to human life.

Recommended Availability Impact Level: The provisional availability impact level recommended for record retention information is ***low***.

### C.3.5.7 Information Management Information Type

Information Management involves the coordination of information collection, storage, and dissemination, and destruction as well as managing the policies, guidelines, and standards regarding information management. Subject to exception conditions described below, the recommended security categorization for the information management information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Moderate), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of information management information on the ability of responsible agencies to perform the day-to-day processes of information collection, storage, dissemination, and destruction and managing the policies, guidelines, and standards regarding information management. The consequences of unauthorized disclosure depend largely on the content and use of the information being managed. The unauthorized disclosure of information management information relevant to most information managed by the government will have only a limited adverse effect on agency operations, assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Information collection and storage involve the day-to-day processes of gathering and storing data from agency programs, partners, and stakeholders. More sensitive information being managed is usually personal information subject to the Privacy Act of 1974 or information that is proprietary to a corporation or other organization. The Privacy Act Information provisional impact levels are documented in the Personal Identity and Authentication information type. Such information will often be assigned a ***moderate*** confidentiality impact level

Where any of the information to be managed can be expected to have a ***high*** confidentiality, impact level, then the information management information must be assigned a ***high*** confidentiality impact level. When the data being managed belongs to one of the information types described in this guideline, the confidentiality impact assigned to the system is that of the highest impact information type processed by the system. Depending on the agency and the mission being supported, the sensitivity of the information can range from none (public information) to ***high***.  (National *security information* and *national security systems* are outside the scope of this guideline.)

Recommended Confidentiality Impact Level:  Particularly in the case of passwords and cryptographic keys, the provisional impact level recommended for information management information depends on the sensitivity and criticality of system information and processes. Although an individual organization's IT infrastructure maintenance information type base may include data elements that will require a higher rating, the recommended provisional impact is ***low***.

### Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of information management information (e.g., configuration settings, passwords, authorization codes, cryptographic keying material) can compromise the effectiveness of the system and impair agency operations.  The level of impact depends on the criticality of system functionality to the agency mission

Special Factors Affecting Integrity Impact Determination:  The loss of integrity for some information management information (e.g., encryption keys) can be very serious for agency operations and can have serious consequences for public confidence in the agency.  The integrity impact level recommended for information management information associated with highly critical information is ***high***.

Recommended Integrity Impact Level:  Potentially serious adverse effects can be expected in most government organizations resulting from the unauthorized modification or deletion of information management information.  Therefore, the provisional integrity impact level recommended for information management information is ***moderate***.

### Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to information management information. The effects of disruption of access to information management information may temporarily impair agency operations.  The level of impact depends on the sensitivity of the information being managed and the criticality of the system to the agency mission. Except for information needed by real-time processes (e.g., information that feeds real-time monitoring or audit functions), information management processes are generally tolerant of reasonable delays. In most cases, disruption of access to information management information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.  Not many business management systems perform functions for which loss of availability can cause significant degradation in mission capability, place the agency at a significant disadvantage, result in major damage to assets, or pose a threat to human life.

Recommended Availability Impact Level:  The provisional availability impact level recommended for information management information is ***low***.

### C.3.5.8 System and Network Monitoring Information Type

System and Network Monitoring supports all activities related to the real-time monitoring of systems and networks for optimal performance. System and network monitoring describes the use of tools and observation to determine the performance and status of information systems and is closely tied to other Information and Technology Management sub-functions. System and network monitoring information type should be considered broadly to include an agency's network [performance, health, and status] and security operations [intrusion monitoring, auditing, etc.] support. Subject to exception conditions described below, the recommended security categorization for the information management information type is as follows:

Security Category = {(confidentiality, Moderate), (integrity, Moderate), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of system and network monitoring information on the ability of responsible agencies to perform the day-to-day processes of real-time monitoring of systems and networks for optimal performance. The consequences of unauthorized disclosure depend largely on the content and use of the monitoring information gathered, retained, and reported. The unauthorized disclosure of system and network monitoring containing architectural information, vulnerabilities, and availability information may have a serious adverse effect on agency operations, assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Where the system and network monitoring information collected can be expected to have a ***high*** confidentiality impact level, then the system and network monitoring information must be assigned a ***high*** confidentiality impact level. When the system and network monitoring data being collected supports information types described in this guideline, agency personnel should consider a confidentiality impact assignment of the highest impact information type processed by the system. Depending on the agency and the mission being supported, the sensitivity of the information can range from ***low*** to ***high***. (National *security information* and *national security systems* are outside the scope of this guideline.)

Recommended Confidentiality Impact Level: Particularly in the case of architectural information (IP addresses, etc.), vulnerabilities, and availability information, the provisional impact level recommended for system and network monitoring information depends on the sensitivity and criticality of system information and processes. The provisional confidentiality impact level recommended is ***Moderate***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of system and network monitoring information can compromise the effectiveness of the system and impair agency network and security operations leading to inaction or incorrect decisions and actions. The level of impact depends on the criticality of system functionality to the agency mission

Special Factors Affecting Integrity Impact Determination: The loss of integrity for some system and network monitoring information can be very serious for agency network and security operations, as well as, the functionality of the information system. Additionally, a loss of integrity can have severe consequences for the agency's mission and critical business functions. The integrity impact level recommended for system and network monitoring information associated with highly critical information is ***high***.

Recommended Integrity Impact Level: Potentially serious adverse effects can be expected in most government organizations resulting from the unauthorized modification or deletion of system and network monitoring information. Therefore, the provisional integrity impact level recommended for system and network monitoring information is ***moderate***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to system and network monitoring information. The effects of disruption of access to system and network monitoring information may temporarily impair or blind agency operations personnel from actual network and security performance. The level of impact depends on the sensitivity of the information and the criticality of the system to the agency mission. In most cases [the exception dual-fault situations], disruption of access to system and network monitoring information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals. Not many system and network monitoring systems perform functions for which loss of availability can cause significant degradation in mission capability, place the agency at a significant disadvantage, result in major damage to assets, or pose a threat to human life.

Recommended Availability Impact Level: The provisional availability impact level recommended for system and network monitoring information is ***low***.

### C.3.5.9 Information Sharing Information Type

The BRM provided in the *FEA Consolidated Reference Model Document, Version 2.3*, October 2007 specifies Information Sharing as relating to any method or function, for a given business area, facilitating: data being received in a usable medium by one or more departments or agencies as provided by a separate department or agency or other entity; and data being provided, disseminated or otherwise made available or accessible by one department or agency for use by one or more separate departments or agencies, or other entities, as appropriate.

Since Information Sharing, as a function, is receiving and disseminating data [other information types] from business areas already identified, this BRM information type will not require its own impact assessment. Therefore, agency personnel should identify the information sharing information type as a pure resource management support activity for the evaluated information system. With the information sharing information type identified, agency personnel can track the flow of information to interfacing systems. The recommended security categorization for the information sharing information type is as follows:

Security Category = {(confidentiality, N/A), (integrity, N/A), (availability, N/A)}

# APPENDIX D: IMPACT DETERMINATION FOR MISSION-BASED INFORMATION AND INFORMATION SYSTEMS

In general, individual agencies should identify the mission information types processed by their systems. This Appendix identifies some information types that might be processed by Federal government organizations. The material includes mission information and potential impacts of unauthorized disclosure, modification, or unavailability of mission information.

The primary purpose for Federal government information systems is to support provision of basic services to U.S. citizens and residents. This section addresses information types associated with both services provided by the Federal government to citizens and mechanisms used to achieve the purposes of government or deliver services for citizens. Delivery mechanisms include financial vehicles, direct government delivery, and indirect government delivery. Federal government missions or delivery mechanisms distributed among 26 mission areas and modes of delivery are identified in Table D-1. Each mission area and delivery mode corresponds to a *Services to Citizens* or *Mode of Delivery* business area as defined in the BRM described in the *FEA Consolidated Reference Model Document Version 2.3*. There is not a one-to-one mapping of services and delivery modes to government departments and agencies. Some departments and agencies focus on a single mission. Others support multiple missions within a mission area. Still others provide services associated with several different mission areas**.**

An information type is associated with each Federal government mission and delivery mode. The identity of each information type is defined by the mission with which it is associated. Some of the *management and support* functions executed to support delivery of services or manage government resources are also executed by some agencies in delivering services to citizens. (See especially the “General Government” functions in Section C.2.8. of Appendix C) Most of these information types could be included in Appendix D as *mission-based* information types. Because the BRM categorizes them as services delivery support functions, they are included in Volume I, Section 4.1.2 and Appendix C and are not repeated in Appendix D.

The common impact determination factors described in Volume I, Section 4.2.3 and 4.4, also apply to mission-based information.

## Table D-1: Mission-Based Information Types and Delivery Mechanisms[22]

### Mission Areas and Information Types

**D.1 Defense & National Security**

Strategic National & Theater Defense
Operational Defense
Tactical Defense

**D.2 Homeland Security**

Border and Transportation Security
Key Asset and Critical Infrastructure Protection
Catastrophic Defense
*Executive Functions of the Executive Office of the President (EOP)*

**D.3 Intelligence Operations**

Intelligence Planning
Intelligence Collection
Intelligence Analysis & Production
Intelligence Dissemination
Intelligence Processing

**D.4 Disaster Management**

Disaster Monitoring and Prediction
Disaster Preparedness and Planning
Disaster Repair and Restoration
Emergency Response

**D.5 International Affairs & Commerce**

Foreign Affairs
International Development and Humanitarian Aid
Global Trade

**D.6 Natural Resources**

Water Resource Management
Conservation, Marine and Land Management
Recreational Resource Management and Tourism
Agricultural Innovation and Services

**D.7 Energy**

Energy Supply
Energy Conservation and Preparedness
Energy Resource Management
Energy Production

**D.8 Environmental Management**

Environmental Monitoring and Forecasting
Environmental Remediation
Pollution Prevention and Control

**D.9 Economic Development**

Business and Industry Development
Intellectual Property Protection
Financial Sector Oversight
Industry Sector Income Stabilization

**D.10 Community & Social Services**

Homeownership Promotion
Community and Regional Development
Social Services
Postal Services

**D.11 Transportation**

Ground Transportation
Water Transportation
Air Transportation
Space Operations

**D.12 Education**

Elementary, Secondary, and Vocational Education
Higher Education
Cultural and Historic Preservation
Cultural and Historic Exhibition

**D.13 Workforce Management**

Training and Employment
Labor Rights Management
Worker Safety

**D.14 Health**

Access to Care
Population Health Mgmt and Consumer Safety
Health Care Administration
Health Care Delivery Services
Health Care Research and Practitioner Education

**D.15 Income Security**

General Retirement and Disability
Unemployment Compensation
Housing Assistance
Food and Nutrition Assistance
Survivor Compensation

**D.16 Law Enforcement**

Criminal Apprehension
Criminal Investigation and Surveillance
Citizen Protection
Leadership Protection
Property Protection
Substance Control
Crime Prevention
*Trade Law Enforcement*

**D.17 Litigation & Judicial Activities**

Judicial Hearings
Legal Defense
Legal Investigation
Legal Prosecution and Litigation
Resolution Facilitation

**D.18 Federal Correctional Activities**

Criminal Incarceration
Criminal Rehabilitation

**D.19 General Sciences & Innovation**

Scientific and Technological Research and Innovation
Space Exploration and Innovation

### Mode of Delivery

### Services Delivery Mechanisms and Information Types

**D.20 Knowledge Creation & Management**

Research and Development
General Purpose Data and Statistics
Advising and Consulting
Knowledge Dissemination

**D.21 Regulatory Compliance & Enforcement**

Inspections and Auditing
Standards Setting/Reporting Guideline Development
Permits and Licensing

**D.22 Public Goods Creation & Management**

Manufacturing
Construction
Public Resources, Facility and Infrastructure Management
Information Infrastructure Management

**D.23 Federal Financial Assistance**

Federal Grants (Non-State)
Direct Transfers to Individuals
Subsidies
Tax Credits

**D.24 Credit and Insurance**

Direct Loans
Loan Guarantees
General Insurance

**D.25 Transfers to State/ Local Governments**

Formula Grants
Project/Competitive Grants
Earmarked Grants
State Loans

**D.26 Direct Services for Citizens**

Military Operations
Civilian Operations

[22] The recommended information types provided in NIST SP 800-60 are established from the “business areas” and “lines of business” from OMB’s Business Reference Model (BRM) section of Federal Enterprise Architecture (FEA) Consolidated Reference Model Document Version 2.3, dated October 2007.

Table D-2 includes provisional impact assessments for each mission information type or delivery mode represented in Table D-1. In Table D-2, exceptions to provisional impact assignments are identified by displaying impact assignments in a gray font [**gray font**] and are described as applicable by security objective in the information type descriptions to follow. The specific descriptions are provided under the sub-heading "Special Factors Affecting [Security Objective] Impact Determination.

*Implementation Tip*

The impact levels assigned to several information types should be considered context-dependent. For example, a given information type in some agencies may include information elements, the compromise of which may endanger human life. In other agencies, the same information type may not include such elements.

Many of the information types are also lifecycle-dependent. That is, information that requires protection at one stage in the system development process may be publicly accessible at a later stage or following some event. For example, information that has confidentiality attributes during the period that an agency is using it to make a decision may be public knowledge once the decision has been made (e.g., financial/budgetary information used during development of requests for proposals in procurement actions).

The following sections describe information attributes that affect impact assessment for each information type.

**Table D-2: Security Categorization of Mission Information**

| | Confidentiality | Integrity | Availability |
|---|---|---|---|
| *Defense & National Security* | **Nat'l Security** | **Nat'l Security** | **Nat'l Security** |
| *Homeland Security* | | | |
| Border Control and Transportation Security | **Moderate** | **Moderate** | **Moderate** |
| Key Asset and Critical Infrastructure Protection | **High** | **High** | **High** |
| Catastrophic Defense | **High** | **High** | **High** |
| Executive Functions of the EOP[23] | **High** | **Moderate** | **High** |
| *Intelligence Operations*[24] | **High** | **High** | **High** |
| *Disaster Management* | | | |
| Disaster Monitoring and Prediction | **Low** | **High** | **High** |
| Disaster Preparedness and Planning | **Low** | **Low** | **Low** |
| Disaster Repair and Restoration | **Low** | **Low** | **Low** |
| Emergency Response | **Low** | **High** | **High** |

[23] The identified information types are not a derivative of OMB's Business Reference Model and were added to address functions of the Executive Office of the President (EOP).

[24] Where foreign intelligence information is involved, the information and information systems are categorized as *national security* information or systems and are outside the scope of this guideline.

**Table D-2: Security Categorization of Mission Information**

| | Confidentiality | Integrity | Availability |
|---|---|---|---|
| *International Affairs and Commerce* | | | |
| Foreign Affairs | **High** | **High** | **Moderate** |
| International Development and Humanitarian Aid | **Moderate** | **Low** | **Low** |
| Global Trade | **High** | **High** | **High** |
| *Natural Resources* | | | |
| Water Resource Management | **Low** | **Low** | **Low** |
| Conservation, Marine, and Land Management | **Low** | **Low** | **Low** |
| Recreational Resource Management and Tourism | **Low** | **Low** | **Low** |
| Agricultural Innovation and Services | **Low** | **Low** | **Low** |
| *Energy* | | | |
| Energy Supply | **Low**[25] | **Moderate**[26] | **Moderate**[26] |
| Energy Conservation and Preparedness | **Low** | **Low** | **Low** |
| Energy Resource Management | **Moderate** | **Low** | **Low** |
| Energy Production | **Low** | **Low** | **Low** |
| *Environmental Management* | | | |
| Environmental Monitoring/ Forecasting | **Low** | **Moderate** | **Low** |
| Environmental Remediation | **Moderate** | **Low** | **Low** |
| Pollution Prevention And Control | **Low** | **Low** | **Low** |
| *Economic Development* | | | |
| Business and Industry Development | **Low** | **Low** | **Low** |
| Intellectual Property Protection | **Low** | **Low** | **Low** |
| Financial Sector Oversight | **Moderate** | **Low** | **Low** |
| Industry Sector Income Stabilization | **Moderate** | **Low** | **Low** |
| *Community and Social Services* | | | |
| Homeownership Promotion | **Low** | **Low** | **Low** |
| Community and Regional Development | **Low** | **Low** | **Low** |
| Social Services | **Low** | **Low** | **Low** |
| Postal Services | **Low** | **Moderate** | **Moderate** |
| *Transportation* | | | |
| Ground Transportation | **Low** | **Low** | **Low** |
| Water Transportation | **Low** | **Low** | **Low** |
| Air Transportation | **Low** | **Low** | **Low** |
| Space Operations | **Low** | **High** | **High** |
| *Education* | | | |
| Elementary, Secondary, and Vocational Education | **Low** | **Low** | **Low** |
| Higher Education | **Low** | **Low** | **Low** |
| Cultural & Historic Preservation | **Low** | **Low** | **Low** |
| Cultural & Historic Exhibition | **Low** | **Low** | **Low** |
| *Workforce Management* | | | |

[25] High where safety of radioactive materials, highly flammable fuels, or transmission channels or control processes at risk.

[26] Usually Moderate or High where mission-critical procedures are involved.

**Table D-2: Security Categorization of Mission Information**

| | Confidentiality | Integrity | Availability |
|---|---|---|---|
| Training and Employment | Low | Low | **Low** |
| Labor Rights Management | **Low** | **Low** | **Low** |
| Worker Safety | **Low** | **Low** | **Low** |
| *Health* | | | |
| Access to Care | Low | **Moderate** | Low |
| Population Health Management and Consumer Safety | Low | Moderate | Low |
| Health Care Administration | Low | Moderate | **Low** |
| Health Care Delivery Services | Low | **High** | Low |
| Health Care Research and Practitioner Education | **Low** | **Moderate** | **Low** |
| *Income Security* | | | |
| General Retirement and Disability | **Moderate** | Moderate | Moderate |
| Unemployment Compensation | Low | **Low** | **Low** |
| Housing Assistance | Low | **Low** | **Low** |
| Food and Nutrition Assistance | Low | **Low** | **Low** |
| Survivor Compensation | Low | **Low** | **Low** |
| *Law Enforcement* | | | |
| Criminal Apprehension | Low | Low | **Moderate** |
| Criminal Investigation and Surveillance | Moderate | Moderate | Moderate |
| Citizen Protection | Moderate | Moderate | Moderate |
| Leadership Protection | Moderate | Low | Low |
| Property Protection | Low | Low | Low |
| Substance Control | Moderate | Moderate | Moderate |
| Crime Prevention | Low | **Low** | Low |
| Trade Law Enforcement[27] | **Moderate** | Moderate | **Moderate** |
| *Litigation and Judicial Activities* | | | |
| Judicial Hearings | Moderate | **Low** | Low |
| Legal Defense | Moderate | High | Low |
| Legal Investigation | Moderate | Moderate | Moderate |
| Legal Prosecution and Litigation | Low | Moderate | Low |
| Resolution Facilitation | Moderate | **Low** | **Low** |
| *Federal Correctional Activities* | | | |
| Criminal Incarceration | **Low** | Moderate | Low |
| Criminal Rehabilitation | Low | **Low** | **Low** |
| *General Science and Innovation* | | | |
| Scientific and Technological Research and Innovation | Low | **Moderate** | **Low** |
| Space Exploration and Innovation | Low | **Moderate** | **Low** |
| *Knowledge Creation and Management* | | | |
| Research and Development | Low | **Moderate** | **Low** |
| General Purpose Data and Statistics | Low | **Low** | **Low** |
| Advising and Consulting | Low | **Low** | **Low** |
| Knowledge Dissemination | Low | Low | Low |

[27] The identified information types are not a derivative of OMB's Business Reference Model and were added to address trade law enforcement.

**Table D-2: Security Categorization of Mission Information**

| | Confidentiality | Integrity | Availability |
|---|---|---|---|
| *Regulatory Compliance and Enforcement* | | | |
| Inspections and Auditing | Moderate | Moderate | Low |
| Standards Setting/ Reporting Guideline Development | Low | Low | Low |
| Permits and Licensing | Low | Low | Low |
| *Public Goods Creation and Management* | | | |
| Manufacturing | Low | Low | Low |
| Construction | Low | Low | Low |
| Public Resources, Facility, and Infrastructure Management | Low | Low | Low |
| Information Infrastructure Management | Low | Low | Low |
| *Federal Financial Assistance* | | | |
| Federal Grants (Non-State) | Low | Low | Low |
| Direct Transfers to Individuals | Low | Low | Low |
| Subsidies | Low | Low | Low |
| Tax Credits | Moderate | Low | Low |
| *Credits and Insurance* | | | |
| Direct Loans | Low | Low | Low |
| Loan Guarantees | Low | Low | Low |
| General Insurance | Low | Low | Low |
| *Transfers to State/Local Governments* | | | |
| Formula Grants | Low | Low | Low |
| Project/Competitive Grants | Low | Low | Low |
| Earmarked Grants | Low | Low | Low |
| State Loans | Low | Low | Low |
| *Direct Services for Citizens* | | | |
| Military Operations[28] | N/A | N/A | N/A |
| Civilian Operations[28] | N/A | N/A | N/A |

## D.1 Defense and National Security

Defense and national security operations protect and advance U.S. National Security interests and, if deterrence fails, decisively defeat threats to those interests. Defense and national security activities include military operations, border protection, and intelligence gathering. Defense operations are subdivided into the following sub-elements:

- **Strategic National and Theater Defense –** Establishing national and multinational military objectives, sequencing initiatives, defining limits and assessing risks for the use of military and other instruments of national power, developing global plans or theater war plans to achieve these objectives, and providing military forces and other capabilities in accordance with strategic plans;

[28] As mode of delivery of mission-based services, the security categorization of Direct Services to Citizens sub-functions Military Operations and Civilian Operation is dependent on the mission services delivered to the citizens [e.g., Health Care; Emergency Response, Environmental Remediation] should be categorized in accordance with the mission-based information type.

- **Operational Defense –** Linking tactics and strategy by establishing operational objectives needed to accomplish the strategic objectives, sequencing events to achieve the operational objectives, initiating actions, and applying resources to bring about and sustain these events; and
- **Tactical Defense –** The ordered arrangement and maneuver of combat elements in relation to each other and to the enemy to achieve combat objectives.

Impacts to information and many information systems associated with defense and national security missions may affect the security of a broad range of critical infrastructures and key national assets. Systems that, involve command and control of military forces, weapons control[29], involve equipment that is an integral part of a weapon or weapons system, are critical to the direct fulfillment of military missions or are otherwise employed in strictly military operations[30] are defined under Public Law as *national security systems*. *National security information* and *national security systems* are outside the scope of this guideline. Information assurance responsibilities are delegated to the Department of Defense for systems that are operated by the Department of Defense, or another entity on behalf of the Department of Defense[31]. Security objectives and impact levels associated with these systems are determined by the Department of Defense.

## D.2 Homeland Security

Homeland Security involves protecting the nation against terrorist attacks. This includes analyzing threats and intelligence, guarding borders and airports, protecting critical infrastructure, and coordinating the response emergencies. The Homeland Security Line of Business is defined by the President's Strategy on Homeland Security. Note: Some of the Critical Mission Areas from the President's strategy are included in other information classes and categories.

### D.2.1 Border and Transportation Security Information Type

Border and Transportation Security includes facilitating or deterring entry and exit of people, goods, and conveyances at and between U.S. ports of entry, as well as ensuring the security of transportation and infrastructure networks, facilities, vehicles, and personnel within the United States. Border control involves enforcing the laws regulating the admission of foreign-born persons (i.e., aliens) to the United States. This includes patrolling and monitoring borders and deportation of illegal aliens. Some border control information is also associated with other mission information types (e.g., criminal apprehension, and criminal investigation and surveillance information). In such cases, the impact levels of the associated mission information may determine impact levels associated with border control information. Some aspects of

[29] Weapons control involves the actions taken to monitor and protect U.S. weaponry, as well as the oversight and control of arms in other countries. Weapons Control applies to conventional, biological, chemical, and nuclear weaponry.

[30] Military operations involve the activities that take place during base trainings, military conflicts, and peacekeeping missions.

[31] *Federal Information Security Management Act of 2002*, Public Law 107-347, Subchapter III – Information Security, Sec. 3543(c)(2), 12/17/02.

ensuring security of transportation and infrastructure networks, facilities, vehicles, and personnel within the United States are also covered under the information types associated with the transportation mission. In some cases the border control information may be classified. Any classified information is treated under separate rules established for *national security information*. The recommended categorization for unclassified border and transportation security information follows:

Security Category = {(confidentiality, Moderate), (integrity, Moderate), (availability, Moderate)}

#### Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of border control information on the ability of responsible agencies to enforce laws regulating the admission of foreign-born persons (i.e., aliens) to the United States. Generally, the effects of unauthorized disclosure of border control information are usually confined to a single geographic region, immigration case, or deportation case. Even so, unauthorized disclosure may have a serious adverse effect on mission functions, cause significant degradation in mission capability, or place the agency at a significant disadvantage with respect to its border control responsibilities. Particularly in the case of immigration, naturalization, and deportation activities, unauthorized disclosure of information can violate privacy policies. Such unauthorized disclosures can have a serious effect on public confidence in the agency.

Special Factors Affecting Confidentiality Impact Determination: Where border control information is also associated with other mission information types (e.g., criminal apprehension, and criminal investigation and surveillance information), the confidentiality impact level associated with the information may be ***high***. Where unauthorized disclosure of border control information may put the physical safety of personnel into serious jeopardy, the confidentiality impact level associated with the information may be ***high***. Unauthorized disclosure of confidentiality of information associated with ensuring security of transportation and infrastructure networks, facilities, vehicles, and personnel within the United States can result in facilitation of terrorist activities that endanger human life. In some cases, the consequent threat to critical infrastructures, key national assets, and human life can be catastrophic. Consequently, the confidentiality impact level associated with information associated with ensuring security of transportation and infrastructure networks, facilities, vehicles, and personnel within the United States is normally ***high***.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for most border control information is ***moderate***.

#### Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations or public confidence in the agency, but the damage to the mission would usually be limited. The consequences of unauthorized modification or destruction of information can be very serious if the information is critical to tactical operations.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information associated with ensuring security of transportation and infrastructure networks, facilities, vehicles, and personnel within the United States may seriously affect mission operations or result in the loss of human life. Unauthorized modification or destruction of information affecting anti-terrorism information may adversely affect mission operations in a manner that results in unacceptable damage to critical infrastructures and/or key national assets or loss of key national assets and/or human life. Consequently, the integrity impact level associated with information that ensures the security of transportation and infrastructure networks, facilities, vehicles, and personnel within the United States is ***high***.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for border control information is ***moderate***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to border control information. Functions and processes supported by most border control information are not time-critical. Also, disruption of access will have only a limited adverse effect on agency operations (including mission functions and public confidence in the agency), agency assets, or individuals.

Special Factors Affecting Availability Impact Determination: There may be time critical cases, for example, information regarding transport of illegal aliens or information about a physical threat posed by aliens that border control personnel have been assigned to interdict. In such cased, the availability impact will be ***high***.

The consequences of disruption of access to information or information systems associated with ensuring security of transportation and infrastructure networks, facilities, vehicles, and personnel within the United States may be severe. Also, anti-terrorism missions are not reliably tolerant of delays. The availability impact level for information systems that ensure the security of transportation and infrastructure networks, facilities, vehicles, and personnel within the United States is ***high***.

Recommended Availability Impact Level: Except for such time-critical cases, cases where impact is driven by information shared with associated missions (e.g., anti-terrorism), the provisional availability impact level recommended for border control information is normally ***moderate***.

### D.2.2 Key Asset and Critical Infrastructure Protection Information Type

Key Asset and Critical Infrastructure Protection involves assessing key asset and critical infrastructure vulnerabilities and taking direct action to mitigate vulnerabilities, enhance security, and ensure continuity and necessary redundancy in government operations and personnel. The Critical Infrastructure Information Protection Act of 2002 (6 U.S.C. 131-134) places specific controls on the dissemination of critical infrastructure information (see Volume I, 3.5.2.3). Under the provisions of Executive Order 13292, some anti-terrorism information is subject to security classification. *National security information* is outside the scope of this guideline. The recommended categorization for unclassified anti-terrorism information follows:

Security Category = {(confidentiality, High), (integrity, High), (availability, High)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of critical infrastructure protection information on the ability of responsible agencies to monitor and assess the leadership, motivations, plans, and intentions of foreign and domestic terrorist groups and their state and non-state sponsors. The effects of unauthorized disclosure of this information can reasonably be expected to jeopardize fulfillment of critical infrastructure protection missions. The consequent threat to critical infrastructures, key national assets, and human life can be catastrophic.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for critical infrastructure protection information is ***high***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. Unauthorized modification or destruction of information affecting critical infrastructure protection operations may adversely affect mission operations and result in unacceptable damage to critical infrastructures, damage to key national assets, or loss of human life.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for critical infrastructure protection information is ***high***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to critical infrastructure protection information. Generally, critical infrastructure protection missions are not reliably tolerant of delays. Significant degradation in mission capability and resultant catastrophic consequences for critical infrastructures, key national assets, and/or human life may occur from disruption of access to critical infrastructure protection information.

Recommended Availability Impact Level: The provisional availability impact level recommended for critical infrastructure protection information is ***high***.

### D.2.3 Catastrophic Defense Information Type

Catastrophic Defense involves the development of technological countermeasures (chemical, biological, radiological and nuclear [CBRN]) to terrorist threats, conducting laboratory testing on new and promising devices, and conducting basic and applied science that can lead to the development of countermeasures. Under the provisions of Executive Order 13292, some anti-terrorism information is subject to security classification. *National security information* is outside the scope of this guideline. The recommended categorization for unclassified anti-terrorism information follows:

Security Category = {(confidentiality, High), (integrity, High), (availability, High)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of catastrophic defense information on the ability of responsible agencies to monitor and assess the leadership, motivations, plans, and intentions of foreign and domestic terrorist groups and their state and non-state sponsors. The effects of unauthorized disclosure of this information can reasonably be expected to jeopardize fulfillment of catastrophic defense missions. The consequent threat to human life, critical infrastructures, and key national assets can be catastrophic.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for catastrophic defense information is normally ***high***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. Unauthorized modification or destruction of information affecting catastrophic defense activities may adversely affect mission operations in a manner that results in loss of human life, unacceptable damage to critical infrastructures, and/or damage to or loss of key national assets.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for catastrophic defense information is ***high***.

Availability

The effects of disruption of access to or use of catastrophic defense information or The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to catastrophic defense information. Generally, disruption of access will have a severe adverse effect on agency operations (including mission functions and public confidence in the agency), agency assets, or individuals. Also, catastrophic defense missions are not tolerant of delays, with consequences of significant degradation in mission capability and resultant catastrophic consequences for human life, critical infrastructures, and/or key national assets.

Recommended Availability Impact Level: The provisional availability impact level recommended for catastrophic defense information is ***high***.

### D.2.4 Executive Functions of the Executive Office of the President (EOP) Information Type

Executive Functions involve the Executive Office of the President (EOP). Subject to exception conditions described below, the recommended provisional security categorization for the executive information type is as follows:

Security Category = {(confidentiality, High), (integrity, Moderate), (availability, High)}

#### Confidentiality

The confidentiality impact level associated with the executive information type is associated with functions of the Executive Office of the President (EOP). The effects of loss of confidentiality of policies and guidance during the formative stage can result in attempts by affected entities and other interested parties to influence and/or impede the policy and guidance development process. Premature public release of formative policies and guidance before internal coordination and review can result in unnecessary damage to public confidence in the EOP. These consequences may occur when the release includes unedited internal commentary and discussion.

Most of the information processed in and by the EOP is classified *national security information* and is outside the scope of this guideline. Other information processed by the EOP is extremely sensitive and applicable to homeland security and law enforcement. The unauthorized disclosure of this extremely sensitive information can seriously imperil human life, key national assets, and critical infrastructures.

Recommended Confidentiality Impact Level: Based on the catastrophic harm that can be suffered by the nation due to unauthorized disclosure of executive information the provisional confidentiality impact level recommended for executive functions information is ***high***.

#### Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information.

Unauthorized modification or destruction of information affecting external communications that contain EOP information (e.g., web pages, electronic mail) may adversely affect public confidence in the government. In the case of the EOP, the impact of such a loss of public confidence may be at least ***moderate***.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for executive information is ***moderate***.

#### Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to the executive information. National defense and critical infrastructure protection aspects of EOP functions are not generally tolerant of delays. Excessive recovery delays can result in loss of coordination of critical defense and public welfare processes.

Recommended Availability Impact Level: The provisional availability impact level recommended for executive functions information is ***high***.

## D.3 Intelligence Operations

Intelligence operations involve the development and management of accurate, comprehensive, and timely foreign intelligence on national security topics. Information systems, the function, operation, or use of, which involve intelligence activities or are critical to the direct fulfillment of intelligence missions[32] are defined under Public Law[33] as *national security systems*. *National security information* and *national security systems* are outside the scope of this guideline. Security objectives and impact levels associated with *national security systems* are determined by the head of each agency exercising control of the system[34].

Intelligence operations are subdivided into the following sub-elements:

- Intelligence Planning Information Type – Intelligence Planning involves developing strategies focused on intelligence requirements, prioritizing these requirements, and managing these requirements (adding, deleting and modifying).
- Intelligence Collection Information Type – Intelligence Collection involves acquiring raw data and provisioning the data to processing elements.
- Intelligence Analysis and Production Information Type – Intelligence Analysis and Production consists of integrating, evaluating, and/or interpreting information from single or multiple sources into intelligence satisfying consumer needs and preparing intelligence products in support of known or anticipated consumers.
- Intelligence Dissemination Information Type – Intelligence Dissemination consists of delivering the intelligence products to consumers.
- Intelligence Processing Information Type – Intelligence processing involves converting collected raw data into forms suitable for analysis.

Some agencies are charged with gathering ***domestic*** intelligence. Much domestic intelligence information is classified. Other domestic intelligence information may not be classified (e.g., some information obtained from state and local government sources). All classified information is treated under separate rules established for *national security information*. The recommended categorization for unclassified domestic intelligence information follows:

Security Category = {(confidentiality, High), (integrity, High), (availability, High)}

[32] Systems that do not involve a) intelligence activities, b) cryptologic activities related to national security, c) command and control of military forces, d) equipment that is an integral part of a weapon or weapons system or 5) information classified by an act of Congress or under an Executive order are not designated as *national security systems* if they are used exclusively for routine business or administrative applications even if they are critical to the direct fulfillment of military or intelligence missions. Routine business or administrative applications are defined as including payroll, finance, logistics, and personnel management applications. [*Federal Information Security Management Act of 2002*, Public Law 107-347, Subchapter III – Information Security, Sec. 3547 – National security systems, 12/17/02]

[33] Clinger-Cohen Act, Public Law 104-106, *National Defense Authorization Act For Fiscal Year 1996*, Division E – Information Technology Reform, Sec. 5142 – National Security Systems Defined, 8/8/96; *Homeland Security Act of 2002*, Public Law 107-296, Title X – Information Security, Subchapter II, Sec. 3532 – Definitions, 11/25/02; and *Federal Information Security Management Act of 2002*, Public Law 107-347, Subchapter III – Information Security, Sec. 3542 – Definitions, 12/17/02.

[34] *Federal Information Security Management Act of 2002*, Public Law 107-347, Subchapter III – Information Security, Sec. 3547 – National security systems, 12/17/02.

### Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of domestic intelligence information on the ability of responsible agencies to develop and manage accurate, comprehensive, and timely domestic intelligence on homeland security topics and other *national* threats. The consequences of unauthorized disclosure of domestic intelligence information may include loss of the ability and/or authorization to collect information necessary to provide warning or to interdict from major threats (e.g., terrorist threats to critical infrastructures and/or key national assets).

Recommended Confidentiality Impact Level: Given the criticality of much domestic intelligence information and the severe or catastrophic consequences to agencies that disclose domestic intelligence information without proper authorization (e.g., Privacy Act provisions, Fourth Amendment issues), the provisional confidentiality impact level recommended for the domestic intelligence information is ***high***.

### Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. Domestic intelligence information is generally associated with other mission-related information (e.g., anti-terrorism, firearms and explosive protection, narcotics interdiction). The consequences of unauthorized modification or destruction of domestic intelligence information is determined to a large extent on the missions being supported by the intelligence information and on whether the intelligence information is time-critical. Unauthorized modification or destruction of intelligence information may adversely affect mission operations in a manner that results in unacceptable damage to critical infrastructures, damage to or loss of key national assets, or loss of human life.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for domestic intelligence information is ***high***.

### Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to domestic intelligence information. Generally, missions supported by domestic intelligence information are not reliably tolerant of delays. Significant degradation in mission capability and resultant catastrophic consequences for critical infrastructures, key national assets, and/or human life may result from disruption of access to domestic intelligence information.

Recommended Availability Impact Level: The provisional availability impact level recommended for domestic intelligence information is ***high***.

## D.4 Disaster Management

Disaster management involves the activities required to prepare for, mitigate, respond to, and repair the effects of all physical and humanitarian disasters whether natural or man-made.

Compromise of much information associated with any of the missions within the disaster management mission area may seriously impact the security of a broad range of critical infrastructures and key national assets.

### D.4.1 Disaster Monitoring and Prediction Information Type

Disaster monitoring and prediction involves the actions taken to predict when and where a disaster may take place and communicate that information to affected parties. [Some disaster management information occurs in humanitarian aid systems under the International Affairs and Commerce line of business (e.g., State Department disaster preparedness and planning).] The recommended provisional categorization of the disaster monitoring and protection information type follows:

Security Category = {(confidentiality, Low), (integrity, High), (availability, High)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of disaster monitoring and prediction information on the ability of responsible agencies to predict when and where a disaster may take place and communicate that information to affected parties. The purpose of disaster monitoring and prediction activities is generally to disseminate information. Sharing of raw information by a diverse group of analysts often improves the quality of predictive analysis.

Special Factors Affecting Confidentiality Impact Determination: The consequences of unauthorized disclosure of some disaster monitoring and prediction information may include public panic or other responses that jeopardize public safety, disaster prevention, emergency response, disaster repair, or restoration missions. For example, attempts of large populations to evacuate in an endangered area before necessary preparations are made for evacuation routes can result in a clogging of the routes and failure to evacuate large parts of the population in time to save them from a life-threatening event. Most of the disaster monitoring and prediction information is critical in terms of potential loss of human life and major property damage. The unauthorized release of this information may interfere with disaster prevention or emergency response missions. The confidentiality impact level recommended for the information cited in the example can be ***moderate*** or ***high***.

The unauthorized disclosure of disaster monitoring and prediction information to terrorists may reveal weak or sensitive points to target, the most effective technique(s use in attacking a target, and information regarding the status, intent, and plans of our adversaries. Where unauthorized disclosure of disaster monitoring and prediction information is expected to be of direct use to terrorists, the confidentiality impact level is recommended to be ***high***.

Recommended Confidentiality Impact Level: The provisional confidentiality impact recommended for most disaster monitoring and prediction information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of disaster monitoring and prediction information usually depends on whether the information is time-critical. Unauthorized modification or destruction of information affecting disaster monitoring and prediction information may jeopardize public safety, disaster prevention, and/or emergency response missions in a manner that results in unacceptable damage to critical infrastructures, damage to key national assets, or loss of human life. For example, an integrity compromise that prevents timely and accurate dissemination of tsunami and earthquake predictions can have life-threatening consequences.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for disaster monitoring and prediction information is ***high***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to disaster monitoring and prediction information. Generally, missions supported by disaster monitoring and prediction information are not reliably tolerant of delays. Delays may cost lives and irreplaceable property, e.g., degradation in mission capability and resultant catastrophic consequences for critical infrastructures, key national assets, and/or human life. For example, a loss of availability of information that prevents timely and accurate dissemination of tsunami and earthquake predictions can have life-threatening consequences.

Recommended Availability Impact Level: The provisional availability impact level recommended for disaster monitoring and prediction information is ***high***.

### D.4.2 Disaster Preparedness and Planning Information Type

Disaster preparedness and planning involves the development of response programs to be used in case of a disaster. This involves the development of emergency management programs and activities as well as staffing and equipping regional response centers. The recommended provisional categorization of the disaster preparedness and planning information type follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of disaster preparedness and planning information on the ability of responsible agencies to develop response programs to be used in case of a disaster. This involves the development of emergency management programs and activities as well as staffing and equipping regional response centers. The consequences of unauthorized disclosure of most disaster preparedness and planning information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: The consequences of unauthorized disclosure of some disaster preparedness and planning information may include revealing weak or sensitive critical infrastructure characteristics or inadequate security of U.S. targets to terrorists or other adversaries. Such information may reveal to an enemy the most effective technique(s) to use in attacking a target, and/or information regarding the capabilities, intent, and plans of our adversaries. Where unauthorized disclosure of disaster preparedness and planning information associated with critical infrastructures, large groups of people, or key national assets is expected to be of direct use to terrorists, the confidentiality impact level is recommended to be ***high***.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for most disaster preparedness and planning information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of disaster preparedness and planning information depend on whether the information is time-critical.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission will usually be limited. The consequences of unauthorized modification or destruction of information can be very serious or catastrophic if the data is time-critical operational information. In such cases, the impact level assigned would be ***moderate*** or ***high***.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for most disaster preparedness and planning information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to disaster preparedness and planning information. Generally, missions supported by disaster preparedness and planning information are not reliably tolerant of delays.

Special Factors Affecting Availability Impact Determination: If emergency responders and those responsible for repair and restoration activities are unable to access preparedness and planning information in the event of an actual emergency the consequences may include confusion and delays. In such cases, the availability impact level can be ***moderate*** or ***high***.

Recommended Availability Impact Level: The provisional availability impact level recommended for disaster preparedness and planning information is ***low***.

### D.4.3 Disaster Repair and Restoration Information Type

Disaster repair and restoration involves the cleanup and restoration activities that take place after a disaster. This involves the cleanup and rebuilding of any homes, buildings, roads, environmental resources, or infrastructure that may be damaged due to a disaster. The recommended provisional categorization of the disaster repair and restoration information type follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of disaster repair and restoration information on the ability of responsible agencies to conduct cleanup and restoration activities that take place after a disaster. This involves the cleanup and rebuilding of any homes, buildings, roads, environmental resources, or infrastructure that may be damaged due to a disaster. The consequences of unauthorized disclosure of most disaster repair and restoration information would have a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for disaster repair and restoration information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of disaster repair and restoration information depends on whether the information is time-critical.

Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations or public confidence in the agency, but the damage to the mission would usually be limited.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for most disaster repair and restoration information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to disaster repair and restoration information. Generally, missions supported by disaster repair and restoration information are tolerant of delay.

Recommended Availability Impact Level: The provisional availability impact level recommended for disaster repair and restoration information is ***low***.

### D.4.4 Emergency Response Information Type

Emergency Response involves the immediate actions taken to respond to a disaster (e.g., wildfire management). These actions include providing mobile telecommunications, operational support, power generation, search and rescue, and medical life saving actions. Impacts to emergency response information and the information systems that process and store emergency response information could result in negative impacts on cross-jurisdictional coordination within the critical emergency services infrastructure and the general effectiveness of organizations tasked with emergency response missions. The recommended provisional categorization of the emergency response information type follows:

Security Category = {(confidentiality, Low), (integrity, High), (availability, High)}

### Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of emergency response information on the ability of responsible agencies to respond to a disaster. These actions include providing mobile telecommunications, operational support, power generation, search and rescue, and medical life saving actions. The consequences of unauthorized disclosure of emergency response information will usually have little or no adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: In cases where an attack is underway, unauthorized disclosure of emergency response information can provide information that might permit terrorists or other adversaries to target emergency response assets, thus jeopardizing emergency response resources and missions and public safety. Given the criticality that much emergency response information has in terms of potential loss of human life and major property damage, where unauthorized release of information can reasonably be expected to facilitate interference with emergency response missions, the confidentiality impact level may be ***moderate*** or ***high***. The unauthorized disclosure of one agency's emergency response by another agency could result in negative impacts on cross-jurisdictional coordination within the critical emergency services infrastructure and the general effectiveness of organizations tasked with emergency response missions.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for emergency response information is ***low***.

### Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of emergency response information usually depends on whether the information is time-critical. Unauthorized modification or destruction of emergency response information may pose a significant threat to major assets and/or human life.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for emergency response information is normally ***high***.

### Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to emergency response information. Generally, missions supported by emergency response information are not tolerant of delays. Delays may cost lives and result in major property damage. Denial of access to emergency response information may result in significant degradation in mission capability and resultant catastrophic consequences for critical infrastructures, key national assets, and/or human life.

Recommended Availability Impact Level: The provisional availability impact level recommended for emergency response information is ***high***.

## D.5 International Affairs and Commerce

International Affairs and Commerce involves the non-military activities that promote U.S. policies and interests beyond our national borders, including the negotiation of conflict resolution, treaties, and agreements. In addition, this function includes: foreign economic development and social/political development; diplomatic relations with other Nations; humanitarian, technical and other developmental assistance to key Nations; and global trade. Information that is protected by procedures established and authorized under criteria specified in an Executive Order or an Act of Congress to be kept classified in the interests of foreign policy are *national security related*[35]. Security objectives and impact levels associated with such *national security information* are determined by the head of each agency exercising control of the system and are outside the scope of this guideline.

### D.5.1 Foreign Affairs Information Type

Foreign Affairs refers to those activities associated with the implementation of foreign policy and diplomatic relations, including the operation of embassies, consulates, and other posts; ongoing membership in international organizations; the development of cooperative frameworks to improve relations with other Nations; and the development of treaties and agreements. Conflict resolution involves the mitigation and prevention of disputes stemming from inter and intra-state disagreements.

Some conflict resolution information is subject to security classification. This classified information is treated under separate rules established for *national security information* and is outside the scope of this guideline.

Treaties and agreements involves the negotiation and implementation of accords with foreign governments and organizations in efforts related to arms reduction and regulation, trade matters, criminal investigations and extraditions, and other various types of foreign policy. When treaties and agreements information affects intelligence gathering and/or law enforcement cooperation, impacts to such information and the information systems that process and store the information could result in negative impacts on protection of a broad range of critical infrastructures and key national assets.

Some information associated with treaties and agreements is subject to security classification. This classified information is treated under separate rules established for *national security information*. The recommended categorization for unclassified foreign affairs information follows:

Security Category = {(confidentiality, High), (integrity, High), (availability, Moderate)}

[35] *Federal Information Security Management Act of 2002*, Public Law 107-347, Subchapter III – Information Security, Sec. 3542(b)(2)(A)(ii), 12/17/02.

### Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of conflict resolution information on the ability of responsible agencies to mitigate and prevent disputes stemming from inter and intra-state disagreements. Unauthorized disclosure of conflict resolution information can reasonably be expected to jeopardize fulfillment of conflict resolution missions. This is particularly true of premature release of resolution factors, personnel profiles, and proposed solutions to adversaries. Some information that has supported a conflict resolution process may undo the results of successful conflict resolution processes. The loss of public confidence in the agency may cause a catastrophic adverse effect on an agency's mission capability. Where information includes candid opinions of agency personnel, or involvement of agency personnel in specific prior activities, the effectiveness of those personnel for many future agency missions may be permanently impaired. The consequences of failed conflict resolution activities may pose threats to human life and major property assets

The level of confidentiality impact assigned to treaties and agreements information is determined by the ability of responsible agencies to negotiate and implement accords with foreign governments and organizations in efforts related to arms reduction and regulation, trade matters, criminal investigations and extraditions, and other types of foreign policy. Unauthorized disclosure of information associated with treaties and agreements can reasonably be expected to prevent successful negotiation and/or ratification of treaties and agreements. This is particularly true of prematurely released resolution factors, personality assessments, and proposed solutions to adversaries. Some information that has supported a treaty or other international agreement process may undo the results of a successfully completed treaty or agreement. The subsequent threat to public confidence in the agency can cause a catastrophic adverse effect on an agency's mission capability. When the disclosed information includes candid opinions of agency personnel, or background information on agency personnel, the effectiveness of those personnel for future agency missions may be permanently impaired. The consequences of failure to successfully conclude treaties and other international agreements often pose threats to human life and major property assets.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for foreign affairs information is ***high***.

### Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of conflict resolution information depend on whether the information is time-critical.

The consequences of unauthorized modification or destruction of information associated with treaties and agreements also depend on the time-critical nature of the information. The unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited.

The unauthorized modification or destruction of information affecting conflict resolution information may adversely affect mission operations in a manner that results in unacceptable consequences such as loss of human life and/or major property assets.

The consequences of unauthorized modification or destruction of information can be very serious if the modification is to time-critical operational information.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for foreign affairs information is ***high***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to foreign affairs information.

Special Factors Affecting Availability Impact Determination: Diplomatic missions are often tolerant of delays. Therefore, the availability impact level assigned to information associated with treaties and agreements that are associated with diplomatic missions is ***low***. Where this is not the case, the availability impact for foreign affairs information associated with treaties and agreements may be ***high***.

Recommended Availability Impact Level: The provisional availability impact level recommended for foreign affairs information is ***moderate***.

### D.5.2 International Development and Humanitarian Aid Information Type

International Development and Humanitarian Aid refers to those activities related to the implementation of development and humanitarian assistance programs to developing and transitioning countries throughout the world. Development and aid may include technical assistance (the transfer of knowledge and expertise), and the delivery of equipment, commodities and humanitarian assistance including food aid. In some cases, international development and humanitarian aid information is subject to security classification. This classified information is treated under separate rules established for *national security information*. The recommended categorization for unclassified international development and humanitarian aid information follows:

Security Category = {(confidentiality, Moderate), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of international development and humanitarian aid information on the ability of responsible agencies to execute programs relating to debt relief, foreign investments, poverty alleviation and food relief, foreign market expansion, and donations, as well as the establishment of policies and procedures to facilitate economic development.

Special Factors Affecting Confidentiality Impact Determination: The unauthorized disclosure of international development and humanitarian aid information may not directly jeopardize foreign socio-economic and political development missions. However, the premature disclosure of this information may adversely affect agency credibility or give unfair competitive advantages to some candidates for mission support activities. These secondary effects may have a negative effect on the intended beneficiaries and can result, in extreme cases, in threats to human life, major assets, or the ability of the agency to perform future missions. Some information that has supported an international development and humanitarian aid process can even undo the results of previously completed foreign socio-economic and political development processes. Where there is a possibility of catastrophic consequences such as threats to human life and major property assets, a ***high*** confidentiality impact level must be assigned.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for international development and humanitarian aid information is ***moderate***.

#### Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of international development and humanitarian aid information depend on whether the information is time-critical. Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited.

Special Factors Affecting Integrity Impact Determination: The consequences of unauthorized modification or destruction of information can be very serious or catastrophic if the modification is to time-critical operational information. In such cases, the impact level assigned would be ***moderate*** or ***high***.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for most international development and humanitarian aid information is ***low***.

#### Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to international development and humanitarian aid information.

Special Factors Affecting Availability Impact Determination: Generally, international development and humanitarian aid missions are tolerant of delays. Where this is not the case, the availability impact associated with international development and humanitarian aid information may be ***moderate*** or ***high***.

Recommended Availability Impact Level: The provisional availability impact level recommended for international development and humanitarian aid information is ***low***.

### D.5.3 Global Trade Information Type

Global Trade refers to those activities the Federal Government undertakes to advance worldwide economic prosperity by increasing trade through the opening of overseas markets and freeing the flow of goods, services, and capital. Trade encompasses all activities associated with the importing and exporting of goods to and from the United States. This includes goods declaration, fee payments, and delivery/shipment authorization. Export promotion involves the development of opportunities for the expansion of U.S. exports. Merchandise inspection includes the verification of goods and merchandise as well as the surveillance, interdiction, and investigation of imports/exports in violation of various Customs laws. Tariffs/quotas monitoring refers to the monitoring and modification of the schedules of items imported and exported to and from the United States. The recommended categorization for the global trade information type follows:

Security Category = {(confidentiality, High), (integrity, High), (availability, High)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of export promotion information on the ability of responsible agencies to advance worldwide economic prosperity by increasing trade through the opening of overseas markets and freeing the flow of goods, services, and capital. Also, the confidentiality impact level is the effect of unauthorized disclosure of merchandise inspection information on the ability of responsible agencies to accurately determine, report, and record the discovered status of imported or exported merchandise as it bears on violations of various Customs laws. Generally, the unauthorized disclosure of merchandise inspection information will not jeopardize the completion of other merchandise inspection missions, as shipment status is generally information of public record. The confidentiality impact level is also the effect of unauthorized disclosure of tariffs/quotas monitoring information on the ability of responsible agencies to enforce various Customs laws, and preserve statistical data concerning the historical compliance with such laws. Typically, the unauthorized disclosure of tariffs/quotas monitoring information will not jeopardize the completion of other tariffs/quotas monitoring missions because the information is publicly available.

Unauthorized disclosure of information that has supported an export promotion process may undo the results of successful export promotion processes. The consequent threat to agency image or reputations can cause a catastrophic adverse effect on an agency's mission capability. Consequently, the general confidentiality impact level associated with export promotion information is ***high***. Some information that has supported a tariffs/quotas monitoring process might be of higher sensitivity, such as intelligence information[36] that might point to a dumping situation. The unauthorized disclosure of this information might jeopardize the success of future

[36] Clinger-Cohen Act, Public Law 104-106, *National Defense Authorization Act For Fiscal Year 1996,* Division E – Information Technology Reform, Sec. 5142 – National Security Systems Defined, 8/8/96; *Homeland Security Act of 2002*, Public Law 107-296, Title X – Information Security, Subchapter II, Sec. 3532 – Definitions, 11/25/02; and *Federal Information Security Management Act of 2002,* Public Law 107-347, Subchapter III – Information Security, Sec. 3542 – Definitions, 12/17/02.

tariffs/quotas monitoring processes. Consequently, the confidentiality impact level associated with tariffs/quotas monitoring information is ***high***.

Intelligence information is included in *national security systems. National security information* and *national security systems* are outside the scope of this guideline.

Some information that has supported a merchandise inspection process might be of higher sensitivity. The unauthorized disclosure of this information might jeopardize the success of future merchandise inspection processes. The consequent threat to agency image or reputations may cause a serious adverse effect on an agency's mission capability. Consequently, the general confidentiality impact level associated with merchandise inspection information is ***high***.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for global trade information is ***high***.

#### Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of global trade information depends on whether the information is time-critical.

Unauthorized modification or destruction of information affecting export promotion information may adversely affect mission operations and result in potentially serious economic repercussions.

Trade agreements that have been implemented are generally matters of public record. Therefore, the specific negotiated terms, etc., must be accurately recorded.

The modification of merchandise inspection information may result in significant financial consequences to an importer or exporter whose shipment is in question and may adversely affect mission operations and result in potentially serious economic repercussions. The results of completed inspections are matters of public record and must be accurately recorded.

For tariffs/quotas monitoring information, the requirement for adequate means to detect data corruption is ***high*.** This information is used in policy and strategic analysis, and the accuracy of this statistical information is critical. Unauthorized modification or destruction of information affecting tariffs/quotas monitoring information may adversely affect mission operations and result in potentially catastrophic economic repercussions.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for global trade information is ***high***.

#### Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to global trade information.

Export promotion and merchandise inspection missions are generally tolerant of significant delays.  If the export promotion and merchandise inspection information are time-critical, the availability impact may be ***high***.  This would be the case where such an occurrence could result in significant financial consequences as a result of uncertainty regarding the status of an imported or exported shipment.

Tariffs/quotas monitoring missions are also tolerant of significant delays.  Typically, this information is used in high level policy and strategic analysis, and denial of access might cause an inconvenience but no significant mission impact.  However, the availability impact associated with tariffs/quotas monitoring information may be ***high***, if denial of access could result in serious damage to the image or reputation of an agency resulting from uncertainty regarding the compliance statistics of a major sovereign trade partner.

Recommended Availability Impact Level:  The provisional availability impact level recommended for global trade information is ***high***.

## D.6 Natural Resources

The Natural Resources mission area includes all activities involved in conservation planning, land management, and national park/monument tourism that affect the nation's natural and recreational resources, both private and federal.  Note: Energy-related natural resources are covered in the Energy Management mission area.

### D.6.1 Water Resource Management Information Type

Water Resource Management includes all activities that promote the effective use and management of the nation’s water resources. Notes: Environmental protection of water resources is included in the Environmental Management Line of Business. Hydroelectric energy production is included under the Energy Production mission.  The recommended provisional categorization of the water resource management information type follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of water resource management information on the ability of responsible agencies to promote the effective use and management of the nation’s water resources. The consequences of unauthorized disclosure of most water resource management information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination:  There may be some cases for which ***moderate*** confidentiality impact is associated with unauthorized disclosure of business/industry development.  For example, unauthorized disclosure of details of current agency water resource management activities and plans may focus opposition and/or give an unfair advantage to competing interests.  Consistent premature disclosure of agency plans may cause significant degradation in mission capability.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for water resource management information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of water resource management information depends on whether the information is time-critical. Unauthorized modification or destruction of information affecting external communications associated with water resource management information (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for most water resource management information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to water resource management information. Generally, missions supported by water resource management information are tolerant of delay.

Recommended Availability Impact Level: The provisional availability impact level recommended for water resource management information is ***low***.

### D.6.2 Conservation, Marine and Land Management Information Type

Conservation, Marine and Land Management involves the responsibilities of surveying, maintaining, and operating public lands and monuments, as well as activities devoted to ensuring the preservation of land, water, wildlife, and natural resources, both domestically and internationally. It also includes the sustainable stewardship of natural resources on federally owned/controlled lands for commercial use (mineral mining, grazing, forestry, fishing, etc.). The recommended provisional categorization of the conservation, marine, and land management information type follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of conservation, marine, and land management information on the ability of responsible agencies to survey, maintain, and operate public lands and monuments, as well as to ensure the preservation of land, water, wildlife, and natural resources, both domestically and internationally. The consequences of unauthorized disclosure of most conservation, marine, and land management information would have a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: There may be some cases for which ***moderate*** confidentiality impact is associated with unauthorized disclosure of private or proprietary information associated with use of federally owned/controlled lands for commercial use (mineral mining, grazing, forestry, fishing, etc.). Additionally, unauthorized disclosure of details of current agency conservation, marine, and land management activities and plans may focus opposition and/or give an unfair advantage to competing interests. Consistent premature disclosure of agency plans may cause significant degradation in mission capability. Also, conservation, marine, and land management include enforcement functions (e.g., the policing of marine fisheries). Confidentiality impacts associated with criminal apprehension, criminal investigation and surveillance, citizen protection, and property protection may cause the confidentiality impact of enforcement-related information to be ***moderate*** or ***high.***

Recommended Confidentiality Impact Level: The provisional confidentiality impact recommended for most conservation, marine, and land management information is ***low***.

### Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of conservation, marine, and land management information depend on whether the information is time-critical.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external communications associated with conservation, marine, and land management information (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited. Conservation, marine, and land management include enforcement functions (e.g., the policing of marine fisheries). Integrity impacts associated with criminal apprehension, criminal investigation and surveillance, citizen protection, and property protection may cause the integrity impact of enforcement-related information to be ***moderate.*** Particularly during fire season, the integrity of land management information critical to fire-fighting operations can affect the safety of human life and large-scale property damage. Such information can have a ***high*** integrity impact level.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for most conservation, marine, and land management information is ***low***.

### Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to conservation, marine, and land management information. Typically, missions supported by conservation, marine, and land management information are tolerant of delay.

Special Factors Affecting Availability Impact Determination: Conservation, marine, and land management include enforcement functions (e.g., the policing of marine fisheries). Availability impacts associated with criminal apprehension, criminal investigation and surveillance, citizen protection, and property protection may cause the availability impact of enforcement-related information to be ***moderate*** or ***high***. Particularly during fire season, the availability of land management information critical to fire-fighting operations can affect the safety of human life and large-scale property damage. Such information can have a ***high*** availability impact level.

Recommended Availability Impact Level: The provisional availability impact level recommended for most conservation, marine, and land management information is ***low***.

### D.6.3 Recreational Resource Management and Tourism Information Type

Recreational Resource Management and Tourism involves the management of national parks, monuments, and tourist attractions as well as visitor centers, campsites, and park service facilities. Impacts to some information and information systems associated with tourism management may affect the security of some key national assets (e.g., some national monuments and icons). The recommended provisional categorization of the recreational resource management and tourism information type follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of recreational resource management and tourism information on the ability of responsible agencies to manage national parks, monuments, and tourist attractions as well as visitor centers, campsites, and park service facilities. The consequences of unauthorized disclosure of most recreational resource management and tourism information would have a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Recreational resource management and tourism include enforcement functions (e.g., protective and enforcement functions of the National Park Service). Confidentiality impacts associated with criminal apprehension, criminal investigation and surveillance, citizen protection, and property protection may cause the confidentiality impact of enforcement-related information to be ***moderate*** or ***high***. The consequences of unauthorized disclosure of property and tourist protection information can be particularly severe in the case of protection of national monuments and icons.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for most recreational resource management and tourism information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of recreational resource management and tourism information depends on whether the information is time-critical. Unauthorized modification or destruction of information affecting external communications associated with recreational resource management and tourism information (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited.

Special Factors Affecting Integrity Impact Determination: Recreational resource management and tourism include enforcement functions (e.g., protective and enforcement functions of the National Park Service). Integrity impacts associated with criminal apprehension, criminal investigation and surveillance, citizen protection, and property protection may cause the integrity impact of enforcement-related information to be ***moderate*** or ***high.*** These types of enforcement-related information are time-critical. Where terrorists or other criminals pose a threat to key national assets, or pose a threat to human life, the integrity impact level recommended for recreational resource management and tourism enforcement information is ***high***.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for most recreational resource management and tourism information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to recreational resource management and tourism information. Generally, missions supported by recreational resource management and tourism information are tolerant of delays.

Special Factors Affecting Availability Impact Determination: Recreational resource management and tourism include enforcement functions (e.g., protective and enforcement functions of the National Park Service). Availability impacts associated with criminal apprehension, criminal investigation and surveillance, citizen protection, and property protection may cause the confidentiality impact of enforcement-related information to be ***moderate*** or ***high***.

There may also be time-critical cases associated with protection of people and key national assets from natural disasters (such as fires, unexpected blizzards, or volcanic eruptions). In such cased, the availability impact may be ***high***. Except for time-critical information, the availability impact level recommended for protection-related information is typically ***moderate***.

Recommended Availability Impact Level: Most recreational resource management and tourism information is routine in nature (not time-critical). Consequently, the provisional availability impact level recommended for most recreational resource management and tourism information is ***low***.

### D.6.4 Agricultural Innovation and Services Information Type

Agricultural Innovation and Services involves the creation and dissemination of better methods for farming and the development of better and healthier crops. The recommended security categorization for the agricultural innovation and service information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

### Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of agricultural innovation and service information on the ability of responsible agencies to create and disseminate of better methods for farming and the development of better and healthier crops. In most cases, unauthorized disclosure of agricultural innovation and service information will have only a limited adverse effect on agency operations, assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: In some cases, unauthorized disclosure of preliminary findings or policies under consideration regarding proposed agricultural products may result in domestic or international public relations problems for the Federal government. In such cases, serious damage can result for agricultural innovation and service operations. Here, the confidentiality impact level may be ***moderate***.

In other cases, unauthorized disclosure of information regarding creation, storage, and transportation of dangerous plant disease vectors, animal disease vectors, pesticides, and herbicides might facilitate malicious activities by terrorists or other criminals. Here, there is a potential for loss of human life, so the confidentiality impact level may be ***high***.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for most agricultural innovation and service information is ***low***.

### Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. Agricultural innovation and service activities are not generally time-critical. In most cases, the adverse effects of unauthorized modification to or destruction of agricultural innovation and service information on agency mission functions and public confidence in the agency can be expected to be limited.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for agricultural innovation and service information is ***low***.

### Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to agricultural innovation and service information. Loan assistance processes are generally tolerant of delay. In most cases, disruption of access to agricultural innovation and service information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The provisional availability impact level recommended for agricultural innovation and service information is ***low***.

## D.7 Energy

Energy refers to all actions performed by the government to ensure the procurement and management of energy resources, including the production, sale and distribution of energy, as well as the management of spent fuel resources. Energy management includes all types of mass-produced energy (e.g., hydroelectric, nuclear, wind, solar, or fossil fuels). Also included in this mission area is the oversight of private industry.

### D.7.1 Energy Supply Information Type

Energy Supply involves all activities devoted to ensuring the availability of an adequate supply of energy for the United States and its citizens. Energy Supply includes the sale and transportation of commodity fuels such as coal, oil, natural gas, and radioactive materials. This function also includes distributing and transferring power, electric generation, and/or storage located near the point of use. Impacts to some information and information systems associated with energy supply may affect the security of critical infrastructures, particularly in the areas of energy transmission and transport. The following recommended provisional categorization of the energy supply information type is particularly subject to change where critical infrastructure elements or nuclear materials are involved:

Security Category = {(confidentiality, Low[37]), (integrity, Moderate[38]), (availability, Moderate[38])}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of energy supply information on the ability of responsible agencies to conduct activities related to the sale and transportation of commodity fuels such as coal, oil, natural gas, and radioactive materials. This function also includes distributing and transferring power, electric generation, and/or storage located near the point of use. Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited.

Special Factors Affecting Confidentiality Impact Determination: The consequences of unauthorized disclosure of energy supply information can have a serious economic impact with respect to competitive advantages and financial and commodity market dynamics. Also, the unauthorized disclosure of supply information may assist terrorists in the theft of energy products or disruption of energy distribution channels. Facilitation of theft of nuclear materials is a particularly catastrophic potential result of unauthorized disclosure of specific types of energy supply information. In these cases, the confidentiality impact must be considered to be ***high***.

[Some information regarding transportation and storage of nuclear materials is classified. The classified information is *national security related* and is outside the scope of this guideline. Other information, such as Nuclear Regulatory Commission "SAFEGUARDS" information is not *national security information*, but must be treated as having ***high*** confidentiality impact.]

[37] Risk level is usually ***high*** where safety of radioactive materials, highly flammable fuels, or major transmission channels or control processes is at risk.

[38] Risk level is usually ***moderate*** or ***high*** where mission-critical procedures are involved.

With respect to possible use by terrorists of energy distribution information regarding petroleum, natural gas, and other flammable or explosive products, a realistic impact assessment must include energy distribution information from private companies. This information is also susceptible to access by terrorists. Where distribution of hazardous energy products is involved, there is a potential unauthorized disclosure consequence of loss of human life and major property. In such cases the confidentiality impact level can be ***moderate*** or ***high***. [Disclosure of transportation routes and storage facilities is often (i) both authorized and necessary to mission accomplishment and (ii) authorized, or even mandated, for public safety reasons.] Also, the unauthorized disclosure of one agency's energy supply information by another agency could result in negative impacts on cross-jurisdictional coordination within the energy distribution infrastructure and the general effectiveness of organizations tasked with energy supply.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for most energy supply information is ***low***.

#### Integrity

The integrity impact level is based on the specific mission and the data and systems supporting that mission, not on the time required to detect the modification to or destruction of information or information system. The consequences of unauthorized modification to or destruction of energy supply information or information systems, usually depends on whether the information is mission-critical.

Special Factors Affecting Integrity Impact Determination:

Mission-critical systems:
Unauthorized modification of mission-critical information or information systems (e.g., electrical power distribution, petroleum or gas pipelines) can result in severe impacts to the environment, service, major assets and/or human safety. Consequently, the integrity impact level associated with these types of mission-critical processes/systems may be ***high***.

Non mission-critical systems:
For information or information systems that do not directly impact mission-critical functions, the integrity impact level may be downgraded to ***low***.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for energy supply information is ***moderate***.

#### Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to energy supply information. Typically, disruption of access will have a limited adverse effect on agency operations (including mission, functions, or public confidence in the agency), agency assets, or individuals. Also, most energy supply information is not time-critical.

Special Factors Affecting Availability Impact Determination:

Mission-critical systems:

Functions supported by mission-critical information or information systems (e.g., electrical power generation, transmission, and/or distribution; petroleum or gas pipelines) are often adversely impacted by lack of availability.  Loss of availability of the information or information system can result in severe impacts to the environment, service, major assets and/or human safety.  Consequently, the availability impact level associated with these types of mission-critical processes/systems may be ***high***.

Non mission-critical systems:

For information or information systems that do not directly impact mission-critical functions, the availability impact level may be downgraded to ***low***.

Recommended Availability Impact Level:  In The availability impact level recommended for most energy supply information is ***moderate***.

### D.7.2 Energy Conservation and Preparedness Information Type

Energy Conservation and Preparedness involves protection of energy resources from over-consumption to ensure the continued availability of fuel resources and to promote environmental protection. This mission also includes measures taken to ensure the provision of energy in the event of an emergency.  The recommended security categorization for the energy conservation and preparedness information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of energy conservation and preparedness information on the ability of responsible agencies to protect energy resources from over-consumption to ensure the continued availability of fuel resources and to promote environmental protection.  In most cases, unauthorized disclosure of energy conservation and preparedness information will have only a limited adverse effect on agency operations, assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination:  In some cases, unauthorized disclosure of preliminary findings or policies under consideration regarding proposed conservation measures or the distribution of energy in the event of an emergency may result in mobilization of special interests.   These groups may successfully oppose necessary conservation measures and be given an unfair advantage for specific commercial interests. Also, the unauthorized disclosure may cause domestic or international loss of confidence in the Federal government.  In such cases, serious damage may result for energy conservation and preparedness operations. Therefore, the confidentiality impact level may be ***moderate***.

In other cases, unauthorized disclosure of information regarding measures taken to ensure the provision of energy in the event of an emergency may facilitate malicious activities of terrorists. Here, there is a potential for loss of human life resulting from extended outages, so the confidentiality impact level may be ***high***.

Recommended Confidentiality Impact Level:  The provisional confidentiality impact level recommended for most energy conservation and preparedness information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. In most cases, the adverse effects of unauthorized modification or destruction of energy conservation and preparedness information on agency mission functions and public confidence in the agency will be limited

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information necessary to mission-critical procedures ensuring the provision of energy in the event of an emergency can result in extended outages. There is some potential for a consequent threat to critical energy infrastructure and to human life. In such cases, the integrity impact level may be ***high***.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for energy conservation and preparedness information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to energy conservation and preparedness information. Loan assistance processes are generally tolerant of delay. In most cases disruption of access to energy conservation and preparedness information will have only a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Availability Impact Determination: Unavailability of information necessary to mission-critical procedures ensuring the provision of energy in the event of an emergency may result in extended outages. There is some potential for a consequent threat to critical energy infrastructure and to human life. In such cases, the availability impact level may be ***high***.

Recommended Availability Impact Level: The provisional availability impact level recommended for energy conservation and preparedness information is ***low***.

### D.7.3 Energy Resource Management Information Type

Energy resource management involves the management of energy producing resources including facilities, land, and offshore resources. The recommended provisional categorization of the energy resource management information type follows:

Security Category = {(confidentiality, Moderate), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of energy resource management information on the activities of responsible agencies with respect to management of energy producing resources including facilities, land, and offshore resources.

Special Factors Affecting Confidentiality Impact Determination: Unauthorized disclosure of much energy resource management information can result in major financial consequences and impact financial markets and have a severe adverse effect on public confidence in the agency. In some cases, the probable consequences of damage to public confidence in the agency can even be ***high***.

Recommended Confidentiality Impact Level: The consequences of unauthorized disclosure of some energy resource management information would have only a limited adverse effect on agency operations. However, the consequences that can be expected to result from unauthorized disclosure of most energy resource management information justify a ***moderate*** provisional confidentiality impact level.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of energy resource management information may depend on the urgency with which the information is typically needed. Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited

Special Factors Affecting Integrity Impact Determination: If the energy resource management information is mission-critical or very sensitive, the integrity impact level may be ***moderate*** or ***high***.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for most energy resource management information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to energy resource management information. Generally, missions supported by energy resource management information are tolerant of delay.

Recommended Availability Impact Level: The provisional availability impact level recommended for energy resource management information is ***low***.

### D.7.4 Energy Production Information Type

Energy production involves the transformation of raw energy resources into useable, deliverable energy. Impacts to some information and information systems associated with energy production may affect the security of the critical energy infrastructure. The recommended provisional categorization of the energy production information type follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

#### Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of energy production information on the activities of responsible agencies with respect to transformation of raw energy resources into useable, deliverable energy. The consequences of unauthorized disclosure of most energy production information would have only a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Unauthorized disclosure of some energy production information can result in major financial consequences. In some cases, premature disclosure of this information can impact financial markets. Unauthorized disclosure to a single institution could damage faith in government institutions, result in adverse financial events, and have a serious adverse effect on public confidence in the agency. Therefore, the confidentiality impact should be at least ***moderate*** for this energy production information.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for most energy production information is ***low***.

#### Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of energy production information may depend on the urgency with which the information is typically needed. Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations or public confidence in the agency, but the damage to the mission would usually be limited.

Special Factors Affecting Integrity Impact Determination: If the energy production information is time-critical or very sensitive, the integrity impact level may be ***moderate*** or ***high***.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for most energy production information is ***low***.

#### Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to energy production information. Missions supported by energy production information are generally tolerant of delays.

Recommended Availability Impact Level: The provisional availability impact level recommended for energy production information is ***low***.

## D.8 Environmental Management

Environmental management includes all functions required to determine proper environmental standards and ensure their compliance.

### D.8.1 Environmental Monitoring and Forecasting Information Type

Environmental Monitoring and Forecasting involves the observation and prediction of environmental conditions. This includes b the monitoring and forecasting of water quality, water levels, ice sheets, air quality, regulated and non-regulated emissions, as well as the observation and prediction of weather patterns and conditions. The following provisional security categorization is recommended for the environmental monitoring and forecasting information type:

Security Category = {(confidentiality, Low), (integrity, Moderate), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of environmental monitoring and forecasting information on the ability of responsible agencies to observe and predict environmental conditions. The consequences of unauthorized disclosure of most environmental monitoring information are unlikely to have a serious adverse effect on agency operations.

Special Factors Affecting Confidentiality Impact Determination: The most serious adverse effects are likely to involve exposure of information that is proprietary to an organization or result in damaging publicity for an organization. [Unauthorized disclosure of some information can have serious economic impact on both individual companies and the broader market place. The consequences of such unauthorized disclosures may have an adverse effect on public confidence in the agency.] In such cases, the potential confidentiality impacts may be at least ***moderate***.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for most environmental monitoring and forecasting information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of environmental monitoring information and forecasting can be serious if the public is exposed to harmful emissions, polluted water, etc.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and public confidence in the agency, but also the agency mission. In some cases, unauthorized modification or destruction of information can result in loss of human life - a ***high***-impact potential.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for environmental monitoring and forecasting information is ***moderate***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to environmental monitoring and forecasting information. Except for cases of emergency bulletins necessary to correct existing threats to public safety, the nature of environmental monitoring and forecasting processes is usually tolerant of reasonable delays.

Recommended Availability Impact Level: The provisional availability impact level recommended for environmental monitoring and forecasting information is ***low***.

### D.8.2 Environmental Remediation Information Type

Environmental remediation supports the immediate and long-term activities associated with the correcting and offsetting of environmental deficiencies or imbalances, including restoration activities. The following security categorization is recommended for the environmental remediation information type:

Security Category = {(confidentiality, Moderate), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of environmental remediation information on the immediate and long-term activities of responsible agencies with respect to correcting and offsetting environmental deficiencies or imbalances. Serious adverse effects are likely to result from 1) exposure of information that is premature and not fully checked for accuracy and that can damage public confidence in an organization targeted for remedial action, 2) unauthorized disclosure of information that is proprietary to an organization, 3) unauthorized disclosure of information concerning proposed remediation that may be used by organizations opposing particular remedial actions, and 4) disclosure of an agency's tactics for enforcing remediation that will have an adverse effect on the enforcement action. The consequences of such unauthorized disclosures may have a serious adverse effect on public confidence in the agency, have a serious adverse effect on agency operations, and place the agency at a significant disadvantage.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for environmental remediation information is ***moderate***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of environmental remediation information may depend on the urgency with which the information is typically needed.

Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations, public confidence in the agency, and the agency mission.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for environmental remediation information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to environmental remediation information. Except for cases of emergency bulletins necessary to correct existing threats to public safety, environmental remediation processes are usually tolerant of reasonable delays.

Recommended Availability Impact Level: The provisional availability impact level recommended for environmental remediation information is ***low***.

### D.8.3 Pollution Prevention and Control Information Type

Pollution prevention and control includes activities associated with the establishment of environmental standards to control the levels of harmful substances emitted into the soil, water and atmosphere. The following security categorization is recommended for the pollution prevention and control information type:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of pollution prevention and control information on the abilities of responsible agencies to establish environmental standards to control the levels of harmful substances emitted into the soil, water and atmosphere. Unauthorized disclosure of pollution prevention and control information can result in incomplete information being published as agency standards or policy, misunderstandings that prevent or increase the difficulty of promulgating standards, or the discrediting of valid proposed standards or policies by exposure of partial information out of context. The consequences of such unauthorized disclosures may have an adverse effect on public confidence in the agency, or agency operations and may place the agency at an operational disadvantage. Most unauthorized disclosure of pollution prevention and control information will have only a limited adverse effect on the affected agency.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for pollution prevention and control information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of pollution prevention and control information may depend on the urgency with which the information is typically needed.

Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations, public confidence in the agency, and the agency mission.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for pollution prevention and control information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to pollution prevention and control information. Except for cases of emergency bulletins necessary to correct existing threats to public safety, pollution prevention and control processes are usually tolerant of delays.

Recommended Availability Impact Level: The provisional availability impact level recommended for pollution prevention and control information is ***low***.

## D.9 Economic Development

Economic Development includes the activities required to promote commercial/industrial development and to regulate the American financial industry to protect investors. It also includes the management and control of the domestic economy and the money supply, and the protection of intellectual property and innovation. Note: The promotion of U.S. business overseas is captured in the function, "International Affairs and Commerce."

### D.9.1 Business and Industry Development Information Type

Business and industry development supports activities related to the creation of economic and business opportunities and stimulus, and the promotion of financial and economic stability for corporations and citizens involved in different types of business. The recommended provisional categorization of the business and industry development information type follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of business and industry development information on the ability of responsible agencies to create economic and business opportunities and stimulus, and promote financial and economic stability for corporations and citizens involved in different types of business. The consequences of unauthorized disclosure of most business and industry development information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: There may be some cases for which ***moderate*** confidentiality impact is associated with unauthorized disclosure of business/industry development. For example, unauthorized disclosure of private information concerning individuals or businesses can result in legal expense and serious effects on public confidence in the agency. Similarly, unauthorized disclosure of details of current agency business and industry development activities and plans can serve to focus opposition and/or give an unfair advantage to competing interests. Additionally, there are legislative mandates prohibiting unauthorized disclosure of trade secrets.  Trade secrets will generally be assigned a ***moderate*** confidentiality impact level.

Recommended Confidentiality Impact Level:  The provisional confidentiality impact level recommended for business/industry development information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information.  The consequences of unauthorized modification or destruction of business and industry development information may depend on the urgency with which the information is typically needed.

Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited.

Recommended Integrity Impact Level:  The provisional integrity impact level recommended for most business and industry development information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to business and industry development information. Missions supported by business and industry development information are generally tolerant of delay.

Recommended Availability Impact Level:  The provisional availability impact level recommended for business and industry development information is ***low***.

### D.9.2 Intellectual Property Protection Information Type

Intellectual property protection involves law enforcement activities involving the enforcement of intellectual property including inventions, literary and artistic works, and symbols, names, images, and designs used in commerce.  Note that intellectual property protection is an exception to the often-close relationship between impacts to law enforcement information and information systems and the security of critical infrastructures and key national assets. The following security categorization is recommended for the intellectual property protection information type:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of intellectual property protection information on the abilities of responsible agencies to enforce intellectual property including inventions, literary and artistic works, and symbols, names, images, and designs used in commerce.  The consequences of unauthorized disclosure of the majority of intellectual property protection information will result in, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: There are legislative mandates prohibiting unauthorized disclosure of trade secrets. Trade secrets will generally be assigned a ***moderate*** confidentiality impact level. In the case of patent activities, technical details of applications involving inventions with military applications and with deliberations concerning withholding patents as a result of *national security* considerations may be sensitive. (In some cases, the patent application information may be classified or to contain information concerning weapons or weapons systems. In such cases, the information would be *national security information,* and outside the scope of this guideline.)

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for intellectual property protection information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of intellectual property protection information depends on the criticality of the information with respect to agency mission capability, protection of agency assets, and safety of individuals. The effects of modification or deletion of this information are generally limited with respect to agency mission capabilities or assets.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for intellectual property protection information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to intellectual property protection information. The nature of intellectual property protection processes is tolerant of reasonable delays.

Recommended Availability Impact Level: The provisional availability impact level recommended for intellectual property protection information is ***low***.

### D.9.3 Financial Sector Oversight Information Type

Financial Sector Oversight involves the regulation of private sector firms and markets (stock exchanges, corporations, etc.) to protect investors from fraud, monopolies, and illegal behavior. This also includes deposit protection. The recommended provisional categorization of the financial sector oversight information type follows:

Security Category = {(confidentiality, Moderate), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of financial sector oversight information on the ability of responsible agencies to regulate private sector firms and markets (stock exchanges, corporations, etc.) to protect investors from fraud, monopolies, and illegal behavior. This also includes deposit protection, creation, regulation, and control of the nation's currency and coinage supply and demand.

Special Factors Affecting Confidentiality Impact Determination: While the consequences of unauthorized disclosure of some financial sector oversight information would have only a limited adverse effect on agency operations, agency assets, or individuals, there are significant exceptions. Unauthorized disclosure of much financial sector oversight information can result in major financial consequences. This can result in assignment of a ***high*** impact level to such information.

In some cases, premature disclosure of regulatory information can impact major financial markets and damage national banking and finance infrastructures. For example, unauthorized disclosure of a decision to increase the money supply or of an ongoing securities fraud investigation can have a dramatic effect on financial markets. This can result in assignment of a ***high*** impact level to such information.

Unauthorized disclosure to a single institution (e.g., a major banking institution or brokerage house), could damage faith in regulatory institutions and result in even more market disruption and have a severe or catastrophic adverse effect on public confidence in the agency. This can result in assignment of a ***high*** impact level to such information.

Even where the consequences are limited to giving an unfair market advantage to a single financial or commercial institution, unauthorized disclosure can have a serious adverse effect on public confidence in the agency and its staff. This can result in assignment of a ***high*** impact level to such information.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for financial sector oversight information is ***moderate.***

### Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. T he consequences of unauthorized modification or destruction of financial sector oversight information depends on whether the information is time-critical. Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations or public confidence in the agency, but the damage to the mission would usually be limited.

Special Factors Affecting Integrity Impact Determination: Where unauthorized modification or destruction of financial sector oversight information facilitates or enables catastrophic consequences, the integrity impact level may be ***high***.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for most financial sector oversight information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to financial sector oversight information. Missions supported by financial sector oversight information are generally tolerant of delay.

Recommended Availability Impact Level: The provisional availability impact level recommended for financial sector oversight information is ***low***.

### D.9.4 Industry Sector Income Stabilization Information Type

Industry Sector Income Stabilization involves all programs and activities devoted to assisting adversely impacted industrial sectors (farming, commercial transportation, etc.) to ensure the continued availability of their services for the American public and the long-term economic stability of these sectors. The provisional recommended security categorization for the industry sector income stabilization information type is as follows:

Security Category = {(confidentiality, Moderate), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of industry sector income stabilization information on the ability of responsible agencies to assist adversely impacted industrial sectors (farming, commercial transportation, etc.) to ensure the continued availability of their services for the American public and the long-term economic stability of these sectors. In most cases, unauthorized disclosure of industry sector income stabilization information will have only a limited adverse effect on agency operations, assets, or individuals. However, unauthorized premature disclosure of Federal government plans for industry sector income stabilization actions (e.g., grants or subsidies) as well as of government economic forecasts and commentary preliminary to formulation of plans may result in major financial consequences. Unauthorized and premature disclosure to a single institution (e.g., a major manufacturing institution, a major agribusiness institution, or a commodity brokerage house), could damage confidence in economic stabilization institutions and have a severe adverse effect on public confidence in the government.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for industry sector income stabilization information is ***moderate.***

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. Industry sector income stabilization activities are not generally time-critical. In most cases, the adverse effects of unauthorized modification or destruction of industry sector income stabilization information on agency mission functions and public confidence in the agency will be limited.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for industry sector income stabilization information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to industry sector income stabilization information. Industry sector income stabilization processes are generally tolerant of delay. In most cases, disruption of access to industry sector income stabilization information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The provisional availability impact level recommended for industry sector income stabilization information is ***low***.

## D.10 Community and Social Services

Community and Social Services includes all activities aimed at creating, expanding, or improving community and social development, social relationships, and social services in the United States. This includes all activities aimed at locality-specific or nationwide social development and general social services and general community development and social services programs, as well as earned and unearned benefit programs that promote these objectives.

### D.10.1 Homeownership Promotion Information Type

Homeownership Promotion includes activities devoted to assisting citizens interested in buying homes and educating the public as to the benefits of homeownership. Note: Activities devoted to the provision of housing to low-income members of the public are covered under the Housing Assistance mission. The recommended provisional categorization of the homeownership promotion information type follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of homeownership promotion information on the ability of responsible agencies to assist citizens interested in buying homes and educating the public as to the benefits of homeownership. The consequences of unauthorized disclosure of most homeownership promotion information would have a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Exceptions that might have a potential for more serious consequences are based on privacy information processed in training and employment systems (e.g., information required by the Privacy Act of 1974 or other statutes and executive orders to receive special handling to protect the privacy of individuals). The Privacy Act Information provisional impact levels are documented in the Personal Identity and Authentication information type. This can result in assignment of a ***moderate*** impact level to such information.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for homeownership promotion information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of homeownership promotion information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals. Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited

Recommended Integrity Impact Level: The provisional integrity impact level recommended most homeownership promotion information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to homeownership promotion information. The effects of disruption of access to most homeownership promotion information or information systems would have a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Integrity Impact Level: The provisional availability impact level recommended for homeownership promotion information is ***low***.

### D.10.2 Community and Regional Development Information Type

The Community and Regional Development mission involves activities designed to assist communities in preventing and eliminating blight and deterioration, assist economically distressed communities, and encourage and foster economic development through improved public facilities and resources. The recommended provisional categorization of the community and regional development information type follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of community and regional development information on the ability of responsible agencies to assist communities in preventing and eliminating blight and deterioration, assist economically distressed communities, and encourage and foster economic development through improved public facilities and resources. The consequences of unauthorized disclosure of most community and regional development information would have a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Exceptions that might have a potential for more serious consequences are based on privacy information processed in training and employment systems (e.g., information required by the Privacy Act of 1974 or other statutes and executive orders to receive special handling to protect the privacy of individuals). The Privacy Act Information provisional impact levels are documented in the Personal Identity and

Authentication information type. Another exception might be unauthorized disclosure of information that gives an individual or corporate entity an unfair competitive advantage in obtaining contracts or other funding for development activities. This can result in assignment of a ***moderate*** impact level to such information.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for community and regional development information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of community and regional development information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited

Recommended Integrity Impact Level: The provisional integrity impact level recommended for most community and regional development information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to community and regional development information. The effects of disruption of access to most community and regional development information or information systems would have a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The provisional availability impact level recommended for community and regional development information is ***low***.

### D.10.3 Social Services Information Type

Social Services are designed to provide meaningful opportunities for social and economic growth of the disadvantaged sector of the population in order to develop individuals into productive and self-reliant citizens and promote social equity. Included in this category are social welfare services extended to children and adults with special needs, such as the orphaned, neglected, abandoned, disabled, etc. Such services include family life education and counseling, adoption, guardianship, foster family care, rehabilitation services, etc. Note: This mission does not include services that are primarily for income support (Income Security) or are an integral part of some other mission area (e.g., Health, Workforce Management, etc.). The recommended provisional categorization of the social services information type follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

### Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of social services information on the ability of responsible agencies to provide meaningful opportunities for social and economic growth of the disadvantaged sector of the population in order to develop individuals into productive and self-reliant citizens and promote social equity. The consequences of unauthorized disclosure of most social services information would have a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Exceptions that might have a potential for more serious consequences include privacy information processed in training and employment systems (e.g., information required by the Privacy Act of 1974 or other statutes and executive orders to receive special handling to protect the privacy of individuals). The Privacy Act Information provisional impact levels are documented in the Personal Identity and Authentication information type. Other exceptions include unauthorized disclosure of information that might assist criminals to perpetrate fraud, particularly with respect to income security disbursements. This can result in assignment of a ***moderate*** impact level to such information.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for social services information is ***low***.

### Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of social services information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited. Another threat is that of unauthorized modification of information to support fraudulent activities. This might result in harm to individuals, but not to agency operations or missions.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for most social services information is ***low***.

### Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to social services information. The effects of disruption of access to most social services information or information systems would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The provisional availability impact level recommended for social services information is ***low***.

### D.10.4 Postal Services Information Type

Postal Services provide for the timely and consistent exchange and delivery of mail and packages between businesses, organizations, and residents of the United States or between businesses, organizations, and residents of the United States and the rest of the world. It also includes the nation-wide retail infrastructure required to make Postal Services easily accessible to customers. (Note: The commercial function of mail is more closely aligned with the "Business and Industry Development" mission in the "Economic Development mission area." The international commercial function of mail is more closely aligned with the "Global Trade" mission in the "International Affairs" mission area). The recommended provisional categorization of thee postal services information type follows:

Security Category = {(confidentiality, Low), (integrity, Moderate), (availability, Moderate)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of postal services information on the ability of responsible agencies to provide for the timely and consistent exchange and delivery of mail and packages between businesses, organizations, and residents of the United States or between businesses, organizations, and residents of the United States and the rest of the world. The consequences of unauthorized disclosure of most postal services information would have a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Exceptions that might have a potential for more serious consequences include privacy information (e.g., information required by the Privacy Act of 1974 or other statutes and executive orders to receive special handling to protect the privacy of individuals). The Privacy Act Information provisional impact levels are documented in the Personal Identity and Authentication information type. Other exceptions include unauthorized disclosure of information that might assist criminals to perpetrate fraud, particularly with respect to income security disbursements. Because registered mail can be employed to transmit classified information, information regarding some registered mail can facilitate unauthorized access to *national security* information. This can result in assignment of a ***moderate*** impact level to such information.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for most postal services information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of postal services information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals. Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited.

Special Factors Affecting Integrity Impact Determination: The consequences of unauthorized modification or destruction of postal information might provide terrorists the tools to carry out an attack. The consequences in terms of critical infrastructure protection and risk to human life may be severe. In such cases, the integrity impact of compromise would be ***high***. Another threat is that of unauthorized modification of information to support fraudulent activities (e.g., misdirection of monetary instruments, execution of fraudulent financial transactions). This might result in harm to individuals, but not to agency operations or missions.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for most postal services information is ***moderate***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to postal services information. The effects of disruption of access to most postal services information or information systems would have an adverse effect on agency operations. Because most postal services information is time critical, extended widespread outages could seriously affect the commerce of the United States.

Recommended Availability Impact Level: The provisional availability impact level recommended for postal services information is ***moderate***.

## D.11 Transportation

Transportation involves all federally supported activities related to the safe passage, conveyance, or transportation of goods and/or people. Note that impacts to some information and many information systems associated with transportation activities may affect the security of, not only the transportation infrastructure, but also to a broad range of other critical infrastructures and key national assets.

### D.11.1 Ground Transportation Information Type

Ground Transportation involves the activities related to ensuring the availability of transit and the safe passage of passengers and goods over land. Water and fuel pipelines are included among ground transportation assets. Note: The protection of ground transportation from deliberate attack is included in the Transportation Security information type under the Homeland Security mission area. The recommended provisional security categorization for the ground transportation information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of ground transportation information on the ability of responsible agencies to ensure the availability of transit and the safe passage of passengers and goods over land. The protection of ground transportation from deliberate attack is included in the Transportation Security information type under the Homeland

Security mission area. For most cases, unauthorized disclosure of ground transportation information will have only a limited adverse effect on agency operations, assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Some regulatory and tariff enforcement functions associated with the safe passage of passengers and goods over land involve relatively sensitive information. These are included in Law Enforcement. Unauthorized disclosure of accident investigation information that has not yet been adequately researched, coordinated, or edited can result in serious economic harm to individuals and to corporations. Loss in public confidence is a further potential consequence. Additionally, some information associated with ground transportation functions is proprietary to corporations or subject to privacy laws (e.g., the Privacy Act of 1974). (The Privacy Act Information provisional impact levels are documented in the Personal Identity and Authentication information type.) In such cases, the confidentiality impact resulting from unauthorized disclosure may be ***moderate***.

Some military ground transportation information is *national security information* and is outside the scope of this guideline.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for ground transportation information is ***low***.

#### Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. In most cases, the adverse effects of unauthorized modification or destruction of ground transportation information on agency mission functions and public confidence in the agency will be limited.

Special Factors Affecting Integrity Impact Determination: Some ground transportation functions are time-critical (e.g., track switching functions associated with rail travel). Unauthorized modification or destruction of time-critical information necessary to these functions can result in large-scale property loss and in loss of human lives. Such information will have a ***high*** integrity impact level.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for ground transportation information is ***low***.

#### Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to ground transportation information. Most ground transportation processes are tolerant of reasonable delays. In most cases, disruption of access to ground transportation information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Availability Impact Determination: Some ground transportation functions are time-critical (e.g., track switching functions associated with rail travel). Loss of availability of time-critical information necessary to these functions can result in large-scale property loss and in loss of human lives.  Such information will have a ***high*** integrity impact level.

Recommended Availability Impact Level:  The provisional availability impact level recommended for ground transportation information is ***low***.

### D.11.2 Water Transportation Information Type

Water Transportation involves the activities related to ensuring the availability of transit and the safe passage of passengers and goods over sea and water.  Note: The protection of maritime transportation from deliberate attack is included in the Transportation Security information type under the Homeland Security mission area. The general recommended security categorization for the water transportation information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of water transportation information on the ability of responsible agencies to ensure the availability of transit and the safe passage of passengers and goods over sea and water.  The protection of water transportation from deliberate attack is included in the Transportation Security information type under the Homeland Security mission area.  Some regulatory and tariff enforcement functions associated with the safe passage of passengers and goods over sea and water involve relatively sensitive information. These are included in Law Enforcement. In most cases, unauthorized disclosure of water transportation information will have only a limited adverse effect on agency operations, assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Unauthorized disclosure of accident investigation information that has not been adequately researched, coordinated, or edited can result in serious economic harm to individuals and to corporations.  Loss in public confidence is a further potential consequence.  Additionally, some information associated with water transportation functions is proprietary to corporations or subject to privacy laws.  In such cases, the confidentiality impact resulting from unauthorized disclosure can be ***moderate***.

Some military sea and water transportation information is *national security information* and is outside the scope of this guideline.

Recommended Confidentiality Impact Level:  The provisional confidentiality impact level recommended for water transportation information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information.   In most cases, the adverse effects of unauthorized modification or destruction of water transportation information on agency mission functions and public confidence in the agency will be limited.

Special Factors Affecting Integrity Impact Determination: Some water and sea transportation functions are time-critical (e.g., distress signals, docking operations, collision avoidance, warnings of hazardous weather or sea conditions). Unauthorized modification or destruction of time-critical information necessary to these functions can result in large-scale property loss and in loss of human lives. Such information would have a ***high*** integrity impact level. Communications management (e.g., frequency management) information also needs to be included in water transportation integrity impact considerations. There may be circumstances when errors in frequency assignment information can result in an inability for Federal government agencies to communicate with state or local government activities. The subsequent loss of communications capabilities can result in life-threatening situations. Such information would have a ***high*** integrity impact level.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for water transportation information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to water transportation information. Most water transportation processes are tolerant of reasonable delays. In most cases, disruption of access to water transportation information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Availability Impact Determination: Some water and sea transportation functions are time-critical (e.g., distress signals, docking operations, collision avoidance, warnings of hazardous weather or sea conditions). Loss of availability of time-critical information necessary to these functions can result in large-scale property loss and in loss of human lives. Such information would have a ***high*** integrity impact level.

Recommended Availability Impact Level: The provisional availability impact level recommended for water transportation information is ***low***.

### D.11.3 Air Transportation Information Type

Air Transportation involves the activities related to the safe passage of passengers or goods through the air. It also includes command and control activities related to the safe movement of aircraft through all phases of flight for commercial and military operations. Note: The protection of air transportation from deliberate attack is included in the Transportation Security information type under the Homeland Security mission area. The general recommended security categorization for the air transportation information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of air transportation information on the ability of responsible agencies to ensure the safe passage of passengers and goods through the air. The protection of air transportation from deliberate attack is included in the Transportation Security information type under the Homeland Security mission area. Some regulatory and tariff enforcement functions associated with the safe passage of passengers and goods over land involve sensitive information. These are treated under Law Enforcement. In most cases, unauthorized disclosure of air transportation information will have only a limited adverse effect on agency operations, assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Unauthorized disclosure of information (e.g., investigations, maintenance) that has not been adequately researched, coordinated, or edited can result in serious economic harm to individuals and to corporations. Loss in public confidence is a further potential consequence. Additionally, some information associated with air transportation functions is proprietary to corporations or subject to privacy laws. In such cases, the confidentiality impact resulting from unauthorized disclosure can be ***moderate***. The sensitivity of air transportation information (e.g., aircraft positioning data)can be time or event-driven. For example, passenger lists are not releasable to the general public before a flight takes off, but are placed in the public domain in the event of a crash. In such cases, the confidentiality impact resulting from unauthorized disclosure can be ***moderate***.

Also, much military air transport information is *national security information* and is outside the scope of this guideline.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for air transportation information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. Many air transportation functions do not process time-critical information.

Special Factors Affecting Integrity Impact Determination: Some air transportation functions are time-critical (e.g., air traffic control instructions, position reports, situational awareness, separation, weather reports for the terminal area, microburst tracking, maintenance trouble reports). Communications management (e.g., frequency management) information also needs to be included in air transportation integrity impact considerations. There may be circumstances under which erroneous frequency assignment information can result in a loss of communications with aircraft that are affected by hazardous conditions (e.g., loss of communications with an aircraft in a crowded air space.) Unauthorized modification or destruction of time-critical information necessary to these functions can result in large-scale property loss and in loss of human lives. The Wide Area Augmentation System (WAAS) supplements the availability and integrity of position information available from the DoD's Global Positioning Systems (GPS). Because of the potential system-wide impacts from a loss of integrity of this system, a ***high*** integrity impact level is recommended.

The following example illustrates the use of controls to address a ***high*** integrity impact level: Systems designed for command and control for air traffic control (e.g., the NAS systems) have been designed for robust operations. In the NAS, integrity and availability issues are closely linked. The loss of integrity in a system is monitored continuously, and the loss of integrity is treated as a loss of availability, and in general, loss of availability for the majority of systems does not cause derogation in safety. That is, if the operational parameters for an Instrument Landing System are detected to be out of established tolerances, the system is immediately removed from service - it is powered down and users are notified that the particular service is not available. In most cases, a loss of availability is preferred to continued availability with degraded integrity. The impacts of the loss of availability due to the loss of integrity include system-wide air traffic delays, diversion of traffic to alternate airports - and the economic losses related to those delays, diversions, etc. Severe impacts are not the norm because the loss of availability is assumed to be inevitable, and the systems have been designed to accommodate failures. In light of the above, the Recommended Integrity Impact Level is ***moderate.***

Recommended Integrity Impact Level: The provisional integrity impact level recommended for most air transportation information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to air transportation information.

Special Factors Affecting Availability Impact Determination: Some air transportation functions are time-critical (e.g., air traffic control instructions, position reports, situational awareness, separation, weather reports for the terminal area, microburst tracking, maintenance trouble reports). Loss of availability of time-critical information necessary to these functions can result in large-scale property loss and in loss of human lives. Timing plays a large part in the availability impact of air transportation information. For example, the time criticality of weather information may be measured in minutes or hours in the case of pre-flight and mid-flight operations. However, on final landing approach, up to the second availability may be required (e.g., detection of microbursts in the terminal area). Air operations are not tolerant of information loss. The Wide Area Augmentation System (WAAS) supplements the availability of information available from the Department of Defense's Global Positioning Systems (GPS). Because of the potential system-wide impacts from a loss of availability of this system, it would be appropriately categorized as having a ***high*** availability impact.

The following example illustrates the use of controls to address a ***high*** integrity impact level: The systems designed for command and control for air traffic control (e.g., the NAS systems) have been designed for robust operations. However, in general, loss of availability for the majority of systems does not cause derogation in safety. The impacts of a loss of availability (or the loss of availability due to the loss of integrity) include local or system-wide air traffic delays, diversion of traffic to alternate airports, etc., and the economic losses related to those delays, diversions, etc. Severe impacts are not the norm because the loss of availability is inevitable, and the systems have been designed to accommodate failures. In light of the above, the Recommended Availability Impact Level is ***moderate.***

Recommended Availability Impact Level: The provisional availability impact level recommended for most air transportation information is ***low***.

### D.11.4 Space Operations Information Type

Space Operations involves the activities related to the safe launches/missions of passengers or goods into aerospace and includes commercial, scientific, and military operations. The recommended provisional security categorization for the space operations information type is as follows:

Security Category = {(confidentiality, Low), (integrity, High), (availability, High)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of space operations information on the ability of responsible agencies to conduct safe launches/missions of passengers or goods into space and includes commercial, scientific, and military operations. The protection of space operations from deliberate attack involves military operations (D.1), homeland security operations (D.2), and law enforcement operations (D.16). In most cases, unauthorized disclosure of space operations information will have only a limited adverse effect on agency operations, assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Civilian space operations are intended to be conducted in the open. Administrative and business functions associated with space operations may involve proprietary, procurement-sensitive, and Privacy Act information. The Privacy Act Information provisional impact levels are documented in the Personal Identity and Authentication information type. In such cases, the confidentiality impact resulting from unauthorized disclosure can be ***moderate***.

Some information regarding space operations (particularly military operations) is classified *national security information* and is outside the scope of this guideline.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for space operations information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. Space operations are typically characterized by critical operational timing and safety parameters, and low tolerance for error. Unauthorized modification or destruction of time-critical information necessary to these functions may result in significant property loss and loss of human lives. Communications management (e.g., frequency management) information also needs to be included in integrity impact determination for space operations. Erroneous frequency assignment information can result in loss of communications with spacecraft that can endanger mission operations and human safety.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for space operations information is ***high***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to space operations information. Space operations are typically characterized by critical operational timing and safety parameters and low tolerance for error. Loss of availability of time-critical information necessary to these functions can result in large-scale property loss and in loss of human lives. Also, air operations are not tolerant of information loss.

Recommended Availability Impact Level: The provisional availability impact level recommended for space operations information is ***high***.

## D.12 Education

Education refers to those activities that impart knowledge or understanding of a particular subject to the public. Education can take place at a formal school, college, university or other training program. This mission area includes all government programs that promote the education of the public, including both earned and unearned benefit programs.

### D.12.1 Elementary, Secondary, and Vocational Education Information Type

Elementary, secondary, and vocational education refers to the provision of education in elementary subjects (reading and writing and arithmetic); education provided by a high school or college preparatory school; and vocational and technical education and training. The recommended provisional categorization of the elementary, secondary, and vocational education information type follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of elementary, secondary, and vocational education information on the ability of responsible agencies to provide guidance and consultative services. The consequences of unauthorized disclosure of most elementary, secondary, and vocational education information would have a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for elementary, secondary, and vocational education information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of elementary, secondary, and vocational education information would have a limited adverse effect on agency operations, agency assets, or individuals. Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for elementary, secondary, and vocational education information is ***low***.

Availability

The effects of disruption of access to most elementary, secondary, and vocational education information or information systems would have a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The provisional availability impact level recommended for elementary, secondary, and vocational education information is ***low***.

### D.12.2 Higher Education Information Type

Higher Education refers to education beyond the secondary level; specifically, education provided by a college or university. It includes external higher educational activities performed by the government (e.g., Military Academies, ROTC, and USDA Graduate School). The recommended provisional categorization of the higher education information type follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of higher education information on the ability of responsible agencies to support education beyond the secondary level (e.g., Military Academies, ROTC, USDA Graduate School, and other public and private universities and colleges). The consequences of unauthorized disclosure of most higher education information would have a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Exceptions are based on the mission supported by the external training and education activity. In such cases, the impact on the system is defined by the information associated with the supported mission. This can result in assignment of a ***moderate*** or ***high*** impact level to such information.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for higher education information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of higher education information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals. Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited

Special Factors Affecting Integrity Impact Determination: Exceptions that might result in more serious consequences are based on the mission supported by the higher education activity (e.g., undetected modification of weapons training information at a service academy where the modification could result in harm to the student or other individuals). In such cases, the impact is determined by the information associated with the supported mission. This can result in assignment of a ***moderate*** or ***high*** impact level to such information.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for higher education information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to higher education information. The effects of disruption of access to most higher education information or information systems would have a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The provisional availability impact level recommended for higher education information is ***low***.

### D.12.3 Cultural and Historic Preservation Information Type

Cultural and Historic Preservation involves all activities performed by the Federal Government to collect and preserve information and artifacts important to the culture and history of the United States and its citizenry and the education of U.S. citizens and the world. The recommended provisional categorization of the cultural and historic preservation information type follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of cultural and historic preservation information on the ability of responsible agencies to collect and preserve information and artifacts important to the culture and history of the United States and its citizenry and the education of U.S. citizens and the world. The consequences of unauthorized disclosure of most cultural and historic preservation information would have a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: In cases where disclosure of information might be useful to an individual or organization intent on destruction of historical materials, the potential consequences to key national assets could be serious to severe. In such cases, the confidentiality impact could be ***moderate*** to ***high***.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for cultural and historic preservation information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of cultural and historic preservation information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals. Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited.

Special Factors Affecting Integrity Impact Determination: In cases where undetected modification of information might be useful to an individual or organization intent on destruction of historical materials, the potential consequences to key national assets could be serious to severe. Consequently, the integrity impact could be ***moderate*** to ***high***.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for cultural and historic preservation information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to cultural and historic preservation information. The effects of disruption of access to most cultural and historic preservation information or information systems would have a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The provisional availability impact level recommended for cultural and historic preservation information is ***low***.

### D.12.4 Cultural and Historic Exhibition Information Type

Cultural and Historic Exhibition includes all activities undertaken by the U.S. government to promote education through the exhibition of cultural, historical, and other information, archives, art, etc. The recommended provisional categorization of the cultural and historic exhibition information type follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of cultural and historic exhibition information on the ability of responsible agencies to promote education through the exhibition of cultural, historical, and other information, archives, art, etc. The consequences of unauthorized disclosure of most cultural and historic exhibition information would have a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: In cases where disclosure of information might be useful to an individual or organization intent on destruction of historical materials or archives, the potential consequences to key national assets could be serious to severe. Consequently, the confidentiality impact could be ***moderate*** to ***high***.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for cultural and historic exhibition information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of cultural and historic exhibition information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals. Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited.

Special Factors Affecting Integrity Impact Determination: In cases where undetected modification of information might be useful to an individual or organization intent on the destruction of historical materials or archives, the potential consequences to key national assets could be serious to severe. Consequently, the integrity impact could be ***moderate*** to ***high***.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for cultural and historic exhibition information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to cultural and historic exhibition information. The effects of disruption of access to most cultural and historic exhibition information or information systems would have a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The provisional availability impact level recommended for cultural and historic exhibition information is ***low***.

## D.13 Workforce Management

Workforce Management includes those activities that promote the welfare and effectiveness of the Nation’s workforce by improving their proficiency, working conditions, advancing opportunities for profitable employment, and strengthening free collective bargaining.

### D.13.1 Training and Employment Information Type

Training and Employment includes programs of job or skill training, employment services and placement, and programs to promote the hiring of marginal, unemployed, or low-income workers. Additionally, training information can include special training for personnel involved in Federal government operations (e.g., astronaut training). The recommended provisional categorization of the training and employment information type follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of training and employment information on the ability of responsible agencies to provide job or skill training, employment services and placement, and programs to promote the hiring of marginal, unemployed, or low-income workers. The consequences of unauthorized disclosure of most training and employment information would have a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Exceptions that might have a potential for more serious consequences are based on privacy information processed in training and employment systems (e.g., information required by the Privacy Act of 1974 or other statutes and executive orders to receive special handling to protect the privacy of individuals). The Privacy Act Information provisional impact levels are documented in the Personal Identity and Authentication information type. This can result in assignment of a ***moderate*** impact level to such information.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for training and employment information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of training and employment information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals. Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited.

Special Factors Affecting Confidentiality Impact Determination: In the case of training aimed at achieving or improving proficiency in specialty occupations (e.g., astronaut training), the consequences of integrity compromises can threaten missions, or even human safety. In such cases, the integrity impact level can range from ***moderate*** to ***high***.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for training and employment information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to training and employment information. The effects of disruption of access to most training and employment information or information systems would have a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The provisional availability impact level recommended for training and employment information is ***low***.

### D.13.2 Labor Rights Management Information Type

Labor Rights Management refers to those activities undertaken to ensure that employees and employers are aware of and comply with all statutes and regulations concerning labor rights, including those pertaining to wages, benefits, safety and health, whistleblower, and nondiscrimination policies. The recommended provisional categorization of the labor rights management information type follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

#### Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of labor rights management information on the ability of responsible agencies to ensure that employees and employers are aware of and comply with all statutes and regulations concerning labor rights, including those pertaining to wages, benefits, safety and health, whistleblower, and nondiscrimination policies. In some cases, premature release of draft labor rights bulletins might adversely affect the effectiveness of agency operations. In general, the consequences of unauthorized disclosure of most labor rights management information would have, a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for labor rights management information is ***low***.

#### Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited. The consequences of unauthorized modification or destruction of labor rights management information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for labor rights management information is ***low***.

#### Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to labor rights management information. The effects of disruption of access to most labor rights management information or information systems would have a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The provisional availability impact level recommended for labor rights management information is ***low***.

### D.13.3 Worker Safety Information Type

Worker Safety refers to those activities undertaken to save lives, prevent injuries, and protect the health of America's workers. The recommended provisional categorization of the worker safety information type follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of worker safety information on the ability of responsible agencies to protect the health and safety of America's workers. In some cases, premature release of draft worker safety bulletins might adversely affect the effectiveness of agency operations. In general, the consequences of unauthorized disclosure of worker safety information would have a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for worker safety information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of worker safety information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals. Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for worker safety information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to worker safety information. The effects of disruption of access to most worker safety information or information systems would have a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The provisional availability impact level recommended for worker safety information is ***low***.

## D.14 Health

Public Health involves Federal programs and activities charged with ensuring and providing for the health and well being of the public. This includes the direct provision of health care services and immunizations as well as the monitoring and tracking of public health indicators for the detection of trends and identification of widespread illnesses/diseases. It also includes both earned and unearned health care benefit programs. Note that impacts to some public health information and information systems may affect the security of critical elements of the public health infrastructure.

### D.14.1 Access to Care Information Type

Access to Care focuses on the access to appropriate care. This includes streamlining efforts to receive care; ensuring care is appropriate in terms of type, care, intensity, location and availability; providing seamless access to health knowledge, enrolling providers; performing eligibility determination, and managing patient movement. The recommended provisional security categorization for access to care information is as follows:

Security Category = {(confidentiality, Low), (integrity, Moderate), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of access to care information on the ability of responsible agencies to focus on the access to appropriate care. This includes streamlining efforts to receive care; ensuring care is appropriate in terms of type, care, intensity, location and availability; providing seamless access to health knowledge, enrolling providers; performing eligibility determination, and managing patient movement will have only a limited adverse effect on agency operations, assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Some information associated with health care involves confidential patient information subject to the Privacy Act and to HIPAA. The Privacy Act Information provisional impact levels are documented in the Personal Identity and Authentication information type. Other information (e.g., information proprietary to hospitals, pharmaceutical companies, insurers, and care givers) must be protected under rules governing proprietary information and procurement management. In some cases, unauthorized disclosure of this information such as privacy-protected medical records can have serious consequences for agency operations. In such cases, the confidentiality impact level may be ***moderate***.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for disclosure of access to care information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information.

Many activities associated with access to care information are not time critical and the adverse effects of unauthorized modification or destruction of health care information on agency mission functions and/or public confidence in the agency will be limited. However, the consequences of unauthorized modification or destruction of health care information may result in incorrect, inappropriate, or excessively delayed treatment of patients. In these cases, serious adverse effects can include legal actions and danger to human life. Unauthorized modification or destruction of information affecting external communications that contain health care information (e.g., web pages, electronic mail) may adversely affect operations and public confidence in the agency and the agency mission.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for access to care information is ***moderate***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to care. Access to care is generally tolerant of delay. Typically, disruption of access to care information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Availability Impact Determination: Some access to care information could be deemed time-critical and is dependent on the severity of the health issue requiring immediate access to care, patient movements, etc.. Delays in the communication of specific situations may cause serious impacts to the patient or care provide. This can result in assignment of a ***moderate*** impact level to such information.

Recommended Availability Impact Level: The provisional availability impact level recommended for access to care information is ***low***.

### D.14.2 Population Health Management and Consumer Safety Information Type

Population Health Management and Consumer Safety assesses health indicators and consumer products as a means to protect and promote the health of the general population. This includes monitoring of health, health planning, and health management of humans, animals, animal products, and plants, as well as tracking the spread of diseases and pests. It also includes evaluation of consumer products, drug, and foods to assess the potential risks and dangers; education of the consumer and the general population; and facilitation of health promotion and disease and injury prevention. The recommended provisional security categorization for population health management and consumer safety information is as follows:

Security Category = {(confidentiality, Low), (integrity, Moderate), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of population health management and consumer safety information on the ability of responsible agencies to assess health indicators and consumer products as a means to protect and promote the health of the general population that will have only a limited adverse effect on agency operations, assets, or individuals. The basic nature of this information type is to support the public and consumer market with information and supporting education.

Special Factors Affecting Confidentiality Impact Determination: The most serious adverse effects are likely to involve premature release of health planning and management information, disclosure of sensitive mission support information [agencies' means to combat spread of diseases or reacting to terrorist attacks on food, water, and other public consumables], or the exposure of information that is proprietary to an organization being evaluated by the agency [Unauthorized disclosure of some information can have serious economic impact on both individual companies and the broader market place. The consequences of such unauthorized disclosures may have an adverse effect on public confidence in the agency.] This can result in assignment of a ***moderate*** impact level to such information.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for disclosure of Health Management and Consumer Safety information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of population health management and consumer safety information can be serious if the public is exposed to mislabeled, tainted, or otherwise harmful food, drugs, or consumer products.

Special Factors Affecting Integrity Impact Determination: Impacts to some population health management and consumer safety information and supporting information systems associated with quality assurance of food, animal, plant and pharmaceuticals may affect the security of critical agriculture and food and public health infrastructures. Additionally, unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and public confidence in the agency and the agency mission. In such cases, unauthorized modification or destruction of information can result in loss of human life. This can result in assignment of a ***high*** impact level to such information.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for population health management and consumer safety information is ***moderate***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish population health management and consumer safety. Population health management and consumer safety are generally tolerant of delay. Typically, disruption of population health management and consumer safety information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Availability Impact Determination: Delays in the communication of product deficiencies or issues associated with food, plant and animal sources may be life threatening. Delays in agency response to public health issues involving humans, animals, animal products, and plants, as well as tracking the spread of diseases and pests may also be life threatening or significantly degrade public safety. This can result in assignment of a ***high*** impact level to such information.

Recommended Availability Impact Level: The provisional availability impact level recommended for population health management and consumer safety information is ***low***.

### D.14.3 Health Care Administration Information Type

Health Care Administration assures that federal health care resources are expended effectively to ensure quality, safety, and efficiency. This includes managing health care quality, cost, workload, utilization, and fraud/abuse efforts.

Security Category = {(confidentiality, Low), (integrity, Moderate), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of Health Care Administration on the ability of responsible agencies to assure that federal health care resources are expended effectively to ensure quality, safety, and efficiency will have only a limited adverse effect on agency operations, assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Much information associated with public health monitoring involves confidential patient information subject to the Privacy Act and to HIPAA. The Privacy Act Information provisional impact levels are documented in the Personal Identity and Authentication information type. In some cases, unauthorized disclosure of this information such as privacy-protected medical records can have serious consequences for agency operations. In such cases, the confidentiality impact level may be ***moderate***.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for disclosure of Health Care Administration information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. Unauthorized modification or destruction of information affecting external communications that contain Health Care Administration information (e.g., web pages, electronic mail) may adversely affect operations and public confidence in the agency and also the agency mission.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of Health Care Administration information can result in inappropriate allocation or deployment of health care services and possible loss of human life. This can result in assignment of a ***high*** impact level to such information.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for Health Care Administration information is ***Moderate***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish Health Care Administration information. Health Care Administration information is generally tolerant of delay. Typically, disruption of Health Care Administration information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The provisional availability impact level recommended for Health Care Administration information is ***low***.

### D.14.4 Health Care Delivery Services Information Type

Health Care Delivery Services provides and supports the delivery of health care to its beneficiaries. This includes assessing health status; planning health services; ensuring quality of services and continuity of care; and managing clinical information and documentation. The recommended provisional security categorization for health care delivery services information is as follows:

Security Category = {(confidentiality, Low), (integrity, High), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of health care delivery services on the ability of responsible agencies to provide and support the delivery of health care to its beneficiaries will have only a limited adverse effect on agency operations, assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Some information associated with health care involves confidential patient information subject to the Privacy Act and to HIPAA. The Privacy Act Information provisional impact levels are documented in the Personal Identity and Authentication information type. Other information (e.g., information proprietary to hospitals, pharmaceutical companies, insurers, and care givers) must be protected under rules governing proprietary information and procurement management. In some cases, unauthorized disclosure of this information such as privacy-protected medical records can have serious consequences for agency operations. In such cases, the confidentiality impact level may be ***moderate***.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for disclosure of health care delivery services information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information.

Many activities associated with health care delivery services are not time critical and the adverse effects of unauthorized modification or destruction of health care information on agency mission functions and/or public confidence in the agency will be limited. However, the consequences of unauthorized modification or destruction of health care information may result in incorrect, inappropriate, or excessively delayed treatment of patients. In these cases, serious adverse effects can include legal actions and danger to human life. Unauthorized modification or destruction of information affecting external communications that contain health care information (e.g., web pages, electronic mail) may adversely affect operations and public confidence in the agency and the agency mission.

Recommended Integrity Impact Level: Because of the potential for the loss of human life, the provisional integrity impact level recommended for health care delivery services information is ***high***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish Health Care Administration information. Except for cases of emergency actions necessary to correct urgent threats to patient health, health care processes are usually tolerant of reasonable delays.

Special Factors Affecting Availability Impact Determination: Some health care delivery services information is time-critical and is dependent on the severity of the health threat(s) and the rapidity with which the threat is spreading/ growing. Delays in the communication of specific situations may be life threatening. This can result in assignment of a ***moderate*** or ***high*** impact level to such information.

Recommended Availability Impact Level: The provisional availability impact level recommended for health care delivery services information is ***low***.

### D.14.5 Health Care Research and Practitioner Education Information Type

Health Care Research and Practitioner Education fosters advancement in health discovery and knowledge. This includes developing new strategies to handle diseases; promoting health knowledge advancement; identifying new means for delivery of services, methods, decision models and practices; making strides in quality improvement; managing clinical trials and research quality; and providing for practitioner education. The recommended provisional security categorization for health care research and practitioner education information is as follows:

Security Category = {(confidentiality, Low), (integrity, Moderate), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of health care research and practitioner education on the ability of responsible agencies to fosters advancement in health discovery and knowledge will have only a limited adverse effect on agency operations, assets, or individuals.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for disclosure of health care research and practitioner education information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. Unauthorized modification or destruction of information affecting external communications that contain health care research and practitioner education information (e.g., web pages, electronic mail) may adversely affect operations and public confidence in the agency and also the agency mission.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for health care research and practitioner education information is ***moderate***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish health care research and practitioner education. Health care research and practitioner education information are generally tolerant of delay. Typically, disruption of health care research and practitioner education information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The provisional availability impact level recommended for health care research and practitioner education information is ***low***.

## D.15 Income Security

Income Security includes activities designed to ensure that members of the public are provided with the necessary means – both financial and otherwise – to sustain an adequate level of existence. This includes all benefit programs, both earned and unearned, that promote these goals for members of the public.

### D.15.1 General Retirement and Disability Information Type

General Retirement and Disability involves the development and management of retirement benefits, pensions, and income security for those who are retired or disabled. Related information types affecting qualification and disbursement of benefits are discussed in Appendix C's Sections C.2.8.8, C.2.8.9, C.2.8.10, C.2.8.11, and C.3.2.5. The recommended provisional categorization of the general retirement and disability information type follows:

Security Category = {(confidentiality, Moderate), (integrity, Moderate), (availability, Moderate)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of general retirement and disability information on the ability of responsible agencies to develop and manage retirement benefits, pensions, and income security for those who are retired or disabled. The consequences of limited unauthorized disclosure of retirement and disability information would have a limited adverse effect on agency operations, agency assets, or individuals.

The disclosure of privacy information (e.g., information required by the Privacy Act of 1974 or other statutes and executive orders to receive special handling to protect the privacy of individuals) may have serious consequences. The Privacy Act Information provisional impact levels are documented in the Personal Identity and Authentication information type. Unauthorized disclosure of large amounts of general retirement and disability information may result in significant damage to an agency's image or operation.

Recommended Confidentiality Impact Level: The confidentiality impact recommended for general retirement and disability information is ***moderate***.

#### Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited.
Generally, the consequences of unauthorized modification or destruction of general retirement and disability information would have a limited adverse effect on agency operations, agency assets, or individuals. However, where provision of retirement and/or disability benefits is a primary agency service delivery mission, the consequences can be more severe.

Special Factors Affecting Integrity Impact Determination: Integrity compromises may result in reduction of benefits– and in extreme cases can be life threatening. This can result in assignment of a ***high*** impact level to such information.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for general retirement and disability information is ***moderate***.

#### Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to general retirement and disability information. The effects of disruption of access to general retirement and disability information or information systems would have, in many cases, a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Availability Impact Determination: Where provision of retirement and/or disability benefits is a primary agency service delivery mission, the consequences can be more severe. Availability compromises may result in reduction of benefits – and in extreme cases can be life threatening. This can result in assignment of a ***high*** impact level to such information.

Recommended Availability Impact Level: The provisional availability impact level recommended for general retirement and disability information is ***moderate***.

### D.15.2 Unemployment Compensation Information Type

Unemployment Compensation provides income security to those who are no longer employed, while they seek new employment. The recommended provisional categorization of the unemployment compensation information type follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

#### Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of unemployment compensation information on the ability of responsible agencies to provide income security to those who are no longer employed, while they seek new employment. The consequences of unauthorized disclosure of most unemployment compensation information would have a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Exceptions that might have a potential for more serious consequences are based on privacy information (e.g., information required by the Privacy Act of 1974 or other statutes and executive orders to receive special handling to protect the privacy of individuals). The Privacy Act Information provisional impact levels are documented in the Personal Identity and Authentication information type. This can result in assignment of a ***moderate*** impact level to such information.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for unemployment compensation information is ***low***.

#### Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of unemployment compensation information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals. Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for unemployment compensation information is ***low***.

#### Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to unemployment compensation information. The effects of disruption of access to unemployment compensation information or information systems would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The provisional availability impact level recommended for unemployment compensation information is ***low***.

### D.15.3 Housing Assistance Information Type

Housing Assistance involves the development and management programs that provide housing to those who are unable to provide housing for themselves including the rental of single-family or multifamily properties, and the management and operation of federally supported housing properties. The recommended provisional categorization of the housing assistance information type follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of housing assistance information on the ability of responsible agencies to develop and manage programs that provide housing to those who are unable to provide housing for themselves including the rental of single-family or multifamily properties, and the management and operation of federally supported housing properties. The consequences of unauthorized disclosure of most housing assistance information would have a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Exceptions that might have a potential for more serious consequences are based on privacy information (e.g., information required by the Privacy Act of 1974 or other statutes and executive orders to receive special handling to protect the privacy of individuals). The Privacy Act Information provisional impact levels are documented in the Personal Identity and Authentication information type. This can result in assignment of a ***moderate*** impact level to such information.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for housing assistance information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of housing assistance information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals. Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for housing assistance information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to housing assistance information. The effects of disruption of access to most housing assistance information or information systems would have a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The provisional availability impact level recommended for housing assistance information is ***low***.

### D.15.4 Food and Nutrition Assistance Information Type

Food and Nutrition Assistance involves the development and management of programs that provide food and nutrition assistance to those members of the public who are unable to provide for these needs themselves. The recommended provisional categorization of the food and nutrition assistance information type follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of food and nutrition assistance information on the ability of responsible agencies to develop and manage of programs that provide food and nutrition assistance to those members of the public who are unable to provide for these needs themselves. The consequences of unauthorized disclosure of most food and nutrition assistance information would have a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Exceptions that might have a potential for more serious consequences are based on privacy information (e.g., information required by the Privacy Act of 1974 or other statutes and executive orders to receive special handling to protect the privacy of individuals). The Privacy Act Information provisional impact levels are documented in the Personal Identity and Authentication information type. This can result in assignment of a ***moderate*** impact level to such information.

Recommended Confidentiality Impact Level: The provisional confidentiality impact recommended for food and nutrition assistance information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of food and nutrition assistance information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals. Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for food and nutrition assistance information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to food and nutrition assistance information. The effects of disruption of access to most food and nutrition assistance information or information systems would have a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The provisional availability impact level recommended for food and nutrition assistance information is ***low***.

### D.15.5 Survivor Compensation Information Type

Survivor Compensation provides compensation to the survivors of individuals currently receiving or eligible to receive benefits from the Federal Government. This includes survivors such as spouses or children of veterans or wage earners eligible for social security payments. The recommended provisional categorization of the survivor compensation information type follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of survivor compensation information on the ability of responsible agencies to provide compensation to the survivors of individuals currently receiving or eligible to receive benefits from the Federal Government. The consequences of unauthorized disclosure of most survivor compensation information would have a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Exceptions that might have a potential for more serious consequences are based on privacy information (e.g., information required by the Privacy Act of 1974 or other statutes and executive orders to receive special handling to protect the privacy of individuals). The Privacy Act Information provisional impact levels are documented in the Personal Identity and Authentication information type. This can result in assignment of a ***moderate*** impact level to such information.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for survivor compensation information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of survivor compensation information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals. Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for survivor compensation information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to survivor compensation information. The effects of disruption of access to most survivor compensation information or information systems would have a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The provisional availability impact level recommended for survivor compensation information is ***low***.

## D.16 Law Enforcement

Law enforcement involves the protection of people, places, and things from criminal activity resulting from non-compliance with U.S. laws. This includes patrols, undercover operations, response to emergency calls, as well as arrests, raids, and seizures of property. Impacts to some information and information systems associated with law enforcement missions may affect the security of a broad range of critical infrastructures and key national assets. Some information associated with Federal law enforcement is categorized as *national security information*. Rules governing establishment of impact levels and controls associated with *national security information* are governed by a separate set of policies and are outside the scope of this guideline. Confidentiality and integrity impacts are often determined by statutory and regulatory requirements that vary by violation.

### D.16.1 Criminal Apprehension Information Type

Criminal apprehension supports activities associated with the tracking and capture of groups or individuals believed to be responsible for committing Federal crimes. The recommended provisional categorization of the criminal apprehension information type follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Moderate)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of criminal apprehension information on the ability of responsible agencies to track and capture groups or individuals believed to be responsible for committing Federal crimes, on public safety, and on the safety of law enforcement officers. The consequences of unauthorized disclosure of criminal apprehension information depend 1) on the seriousness of the crime involved, 2) on the capability and predisposition of the criminal to injure or kill civilians or law enforcement officials, 3) timing (e.g., the ability of the criminal to access the information and use it to facilitate a crime or evade capture), and 4) statutory and regulatory requirements which vary by violation.

Special Factors Affecting Confidentiality Impact Determination: In cases where 1) the crimes are not violent and do not involve large property losses, and 2) there is no history of violence on the part of the criminal, the confidentiality impact may be ***low*** or ***moderate***. For many crimes that are the responsibility of Federal law enforcement agencies, the consequences associated with unauthorized disclosure of criminal apprehension information must often be assumed to pose a threat to human life or result in a loss of major assets.  In such cases, confidentiality impact level is ***high***.

Recommended Confidentiality Impact Level:  For most Federal law enforcement systems that support criminal apprehension activities the harm that results from unauthorized disclosure will be limited. Therefore, the provisional confidentiality impact level recommended for criminal apprehension information is ***low***.

### Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information.  The consequences of unauthorized modification or destruction of criminal apprehension information may depend on the urgency with which the information is needed and on the success of subsequent prosecution of the apprehended criminal(s).  Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited.

Special Factors Affecting Integrity Impact Determination:  Unauthorized modification or destruction of criminal apprehension information may have an adverse effect on the subsequent prosecution of the apprehended criminal.  Consequently, a serious adverse effect on agency operations can result.  This can place the agency at a significant disadvantage.  In such cases, the integrity impact level recommended for criminal apprehension information is at least ***moderate***.  When the criminal apprehension information is time-critical, the unauthorized modification or destruction of this information may have a severe or catastrophic effect on public confidence in the agency, pose a significant threat to major assets, and/or pose a threat to human life.  This is applicable for many crimes that are the responsibility of Federal law enforcement agencies. For this criminal apprehension information, the Recommended Integrity Impact Level is ***high***.

Recommended Integrity Impact Level: For most Federal law enforcement systems that support criminal apprehension activities the harm that results from unauthorized modification or destruction will be limited.  Therefore, the provisional integrity impact level recommended for criminal apprehension information is ***low***.

### Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to criminal apprehension information. Missions supported by criminal apprehension information are not typically tolerant of delay. While there are many cases in which elements of criminal apprehension information are not urgent, there are many in which relatively short periods of unavailability can pose a threat to human life and/or result in a loss of major assets.

Recommended Availability Impact Level:  The provisional availability impact level recommended for most criminal apprehension information is ***moderate***.

### D.16.2 Criminal Investigation and Surveillance Information Type

Criminal investigation and surveillance includes the collection of evidence required to determine responsibility for a crime and the monitoring and questioning of affected parties. The recommended provisional categorization of the criminal investigation and surveillance information type follows:

Security Category = {(confidentiality, Moderate), (integrity, Moderate), (availability, Moderate)}

#### Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of criminal investigation and surveillance information on the ability of responsible agencies to collect evidence required to determine responsibility for a crime, to monitor and question affected parties, and to protect the safety of witnesses and law enforcement officers. The consequences of unauthorized disclosure of criminal investigation and surveillance information depend 1] on the seriousness of the crime involved, 2] timing (e.g., the ability of the criminal[39] to access the information and use it to facilitate a crime, to evade detection or surveillance, or eliminate probable cause for searches and warrants), and 3] on the capability and predisposition of the criminal to injure witnesses or law enforcement officials.

Special Factors Affecting Confidentiality Impact Determination: In cases where 1) the crimes are not violent and do not involve large property losses, and 2) there is no history of violence on the part of the criminal, the confidentiality impact may be ***low*** or ***moderate***. Given the nature of many of the crimes that are the responsibility of Federal law enforcement agencies, the consequences associated with unauthorized disclosure of criminal investigation and surveillance information must often be assumed to pose a threat to human life or result in a loss of major assets. Information that reveals the identity and/or location of informants may be of particular concern. In such cases, the confidentiality impact level is ***high***.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for criminal investigation and surveillance information is ***moderate***.

#### Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of criminal investigation and surveillance information depends on the urgency with which the information is needed and on the success of subsequent prosecution of the apprehended criminal(s). Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations or public confidence in the agency, but the damage to the mission would usually be limited.

Where unauthorized modification or destruction of criminal investigation and surveillance information can have an adverse effect on the granting or execution of a search or wiretap

[39] In this case, the term “criminal entity” includes both the criminal and legal representative(s) of the criminal (i.e., council).

warrant or on the success of subsequent prosecution of the apprehended criminal a serious adverse effect on agency operations can result. This can place the agency at a significant disadvantage.

Special Factors Affecting Integrity Impact Determination: In some cases, major investigations can be jeopardized when the time-critical criminal investigation and surveillance information is modified or destroyed. Where the criminal case under investigation involves major property losses, large-scale financial frauds that have serious implications for financial markets, poses a threat to key national assets or human life, the Recommended Integrity Impact Level is ***high***. In international matters, such as trade enforcement, tariff agreements, etc., or where foreign nationals might be involved, the integrity impact level for criminal investigation and surveillance information will be ***high***. Any compromise of such information could result in catastrophic adverse effects on future operations, individual and agency reputations, and on human life.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for criminal investigation and surveillance information is ***moderate***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to criminal investigation and surveillance information. Missions supported by criminal investigation and surveillance information are not always tolerant of delay.

Special Factors Affecting Availability Impact Determination: There are some cases in which relatively short periods of unavailability of criminal investigation and surveillance information may result in lost surveillance opportunities or opportunities to make an arrest. Where the crimes involved pose a threat to human life and/or result in a loss of major assets, the availability impact level recommended for criminal investigation and surveillance information is ***high***.

Recommended Availability Impact Level: The provisional availability impact level recommended for criminal investigation and surveillance information is ***moderate***.

### D.16.3 Citizen Protection Information Type

Citizen protection involves all activities performed to protect the general population of the United States from criminal activity. The following security categorization is recommended for the citizen protection information type:

Security Category = {(confidentiality, Moderate), (integrity, Moderate, (availability, Moderate)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of citizen protection information on the ability of responsible agencies to protect the general population of the United States from criminal activity. In some cases, the criminal activity is terrorist activity intended to cause mass casualties. While the results of unauthorized disclosure of most citizen protection information are unlikely to have a serious adverse effect on agency operations, the exceptions can have catastrophic consequences.

Special Factors Affecting Confidentiality Impact Determination: The consequences of unauthorized disclosure of citizen protection information could be severe. If detailed intelligence information regarding a planned terrorist act was disclosed, the terrorists might succeed in countering the protection measures and carry out a devastating attack. The confidentiality impacts associated with information concerning defensive dispositions would be ***high***. While the adverse effects of unauthorized disclosure of some citizen protection information on law enforcement operations, assets, and individuals are limited; the stakes are usually higher. Federal citizen protection activities often seek to protect the public against life-threatening situations or against loss of major assets.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for most citizen protection information is ***moderate***.

### Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of citizen protection information may pose a potential threat to public safety particularly if the protective measures are compromised.

Special Factors Affecting Integrity Impact Determination: In some cases (e.g., terrorist threats), unauthorized modification or destruction of citizen protection information can result in loss of human life - a ***high***-impact potential.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for citizen protection information is ***moderate***.

### Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to citizen protection information. Many citizen protection missions are usually tolerant of reasonable delays. Most criminal activity against citizen protection information is not life threatening but can result in serious property loss.

Special Factors Affecting Availability Impact Determination: Emergency situations or elevated terrorist threat conditions are not tolerant of delays. Where systems support time-sensitive operations for life-threatening situations, the availability impact level for citizen protection information is ***high***.

Recommended Availability Impact Level: In the case of most systems that support delivery of citizen protection services, the provisional availability impact level recommended for citizen protection information is ***moderate***.

### D.16.4 Leadership Protection Information Type

Leadership protection involves all activities performed to protect the health and well being of the president, vice-president, their families, and other high-level government officials. Some leadership protection information may be classified. All classified information is treated under separate rules established for *national security information* and is outside the scope of this guideline. The recommended provisional categorization for unclassified leadership protection information follows:

Security Category = {(confidentiality, Moderate), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of leadership protection information on the abilities of responsible agencies to protect the health and well being of the president, vice-president, their families, and other high-level government officials. The consequences of unauthorized disclosure of most leadership protection information are not directly life-threatening but can have serious consequences.

Special Factors Affecting Confidentiality Impact Determination: For the unauthorized disclosure of information that can facilitate efforts to assassinate Federal leadership, the consequences not only pose a threat to human life, but can also have a disruptive effect on the continuity of Federal government operations. In such cases, the confidentiality impact level is ***high***.

Recommended Confidentiality Impact Level: Given the nature of most leadership protection information, the provisional confidentiality impact level recommended for the information is ***moderate***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. That is, the consequences of unauthorized modification or destruction of leadership protection information may be determined by the specific operation(s) supported by the information. In addition, the consequences may depend on the urgency with which the intelligence information is needed.

Special Factors Affecting Integrity Impact Determination: In the case of Secret Service operations, unauthorized modification or destruction of information affecting leadership protection information may adversely affect mission operations in a manner that results in loss of human life and disruption of government operations. In such cases, the integrity impact level is ***high***.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for most leadership protection information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to leadership protection information.

Special Factors Affecting Integrity Impact Determination: In the case of Secret Service operations, missions supported by leadership protection information are not tolerant of delays with resultant catastrophic consequences for mission capability and human life. In such cases, the availability impact level is ***high***.

Recommended Availability Impact Level: The provisional availability impact level recommended for most leadership protection information is ***low***.

### D.16.5 Property Protection Information Type

Property protection entails all activities performed to ensure the security of civilian and government property. The recommended provisional categorization of the property protection information type follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of property protection information on the ability of responsible agencies to ensure the security of civilian and government property. The consequences of unauthorized disclosure of property protection information are generally dependent on the nature of the property being protected. Where the property being protected is neither critical to agency operations nor of such value that its loss would degrade mission capability or place the agency at a significant disadvantage, unauthorized disclosure would have a limited adverse effect.

Special Factors Affecting Confidentiality Impact Determination: Where critical infrastructure facilities or key national assets are being protected, the consequences of unauthorized disclosure of property protection information might reveal vulnerabilities in protection measures to terrorists or other adversaries. Where unauthorized disclosure of property protection information associated with critical infrastructures, large groups of people, or key national assets is expected to be of direct use to terrorists, the confidentiality impact level is ***high***.

Most protected facilities are not part of *national security,* the critical infrastructure, or key national asset categories. If unauthorized disclosure of property protection information resulted in damage to these facilities, serious adverse effects on agency operations and assets could reasonably be expected to result. This can result in assignment of a ***moderate*** or ***high*** impact level to such information.

Where the property being protected involves classified information, the property protection information itself might be classified. Some examples include command and control and other military facilities, foreign intelligence collection or processing facilities, weapons or weapons facilities, and cryptographic activities. *National security information* is outside the scope of this guideline.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for property protection information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of property protection information depends on the type of property being protected and on the immediacy with which the information is expected to be used. In most cases, unauthorized disclosure can be expected to have limited adverse consequences.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations or public confidence in the agency. However, the potential damage to the protection mission will usually be of greater concern. If the modified or destroyed information is tactical i.e., time-critical, there is a greater potential for actions being taken based on incomplete or false information. This can have serious adverse effects on protection operation. This can result in assignment of a ***moderate*** impact level to such information. .

Recommended Integrity Impact Level: The provisional integrity impact level recommended for most property protection information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to property protection information. Missions supported by property protection information are not typically tolerant of delays, but the consequences of loss of availability of most property protection information are limited.

Special Factors Affecting Availability Impact Determination: The consequences of inability of guard forces and other emergency responders to receive property protection information in a timely manner may result in catastrophic consequences for properties that could include critical infrastructures and key national assets. In general, the availability impact level assigned to property protection information is dependent on what is being protected. This can result in assignment of a ***moderate*** or ***high*** impact level to such information.

Recommended Availability Impact Level: The provisional availability impact recommended for most property protection information is ***low***.

### D.16.6 Substance Control Information Type

Substance control supports activities associated with the enforcement of legal substances (i.e., alcohol and tobacco) and illegal narcotics laws including trafficking, possession, sale, distribution, and other related activities. The provisional security categorization recommended for the substance control information type is as follows:

Security Category = {(confidentiality, Moderate), (integrity, Moderate), (availability, Moderate)}

### Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of substance control information on the ability of responsible agencies to enforce legal substances (i.e., alcohol and tobacco) and illegal narcotics laws including trafficking, possession, sale, distribution, and other related activities. Unauthorized disclosure of a significant proportion of substance control information can compromise investigations, cause apprehension operations to fail, and compromise prosecutions. This can have a serious adverse effect on agency operations and place the agency at a significant disadvantage.

Special Factors Affecting Confidentiality Impact Determination: Unauthorized disclosure of some routine substance control information is unlikely to have more than a limited adverse effect on agency operations, agency assets, or individuals. The confidentiality impact associated with such information is ***low***.

Where the unauthorized disclosure of information exposes sensitive information sources or compromises investigative or interdiction operations, the consequences of unauthorized disclosure of substance control information may have a serious adverse effect on agency operations, significantly degrade mission capability, and/or pose a threat to human life. Where unauthorized disclosure endangers investigations in process, investigative or intelligence information sources, or information regarding witnesses or other critical case file elements, the danger to human life and key agency missions can be significant. Where unauthorized disclosure endangers witnesses or law enforcement officers, the impact level must be rated as ***high***.

Other factors affecting confidentiality impacts associated with substance control information are discussed under Section D.16.1 (Criminal Apprehension) and Section D.16.2 (Criminal Investigation and Surveillance).

Some substance control information is classified (e.g., some intelligence-derived information). Classified information and other *national security information* are outside the scope of this guideline.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for most substance control information is ***moderate***.

### Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The amount of money available to perpetrators significantly increases the insider threat. The consequences of unauthorized modification or destruction of information can be serious if the information is critical to tactical operations i.e., is time-critical. Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations or public confidence in the agency, but the damage to most missions would usually be limited

Special Factors Affecting Confidentiality Impact Determination: Unauthorized modification or destruction of information (particularly time-critical information) affecting internal communications can jeopardize investigations, prosecutions, the lives of witnesses, and the safety of enforcement officers. In some cases, unauthorized modification or destruction of information can result in loss of human life. In such cased, the integrity impact level is ***high***.

Other factors affecting integrity impacts associated with substance control information are discussed under Section D.16.1 (Criminal Apprehension) and Section D.16.2 (Criminal Investigation and Surveillance).

Recommended Integrity Impact Level: Because the consequences of unauthorized modification or destruction of information can be serious if the information is critical to tactical operations (i.e., is time-critical), the provisional integrity impact level recommended for substance control information is ***moderate***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to substance control information. Most substance control processes are usually tolerant of reasonable delays.

Special Factors Affecting Availability Impact Determination: The consequences of unavailability of information can be serious if the information is critical to tactical operations i.e., is time-critical. Failure of some processes during tactical operations can result in both threats to human life and severe harm to public confidence in the agency. The impact level assigned to information and information systems associated with these tactical processes is ***high***.

Recommended Availability Impact Level: The provisional availability impact level recommended for most substance control information is ***moderate***.

### D.16.7 Crime Prevention Information Type

Crime prevention entails all efforts designed to create safer communities through the control and reduction of crime by addressing the causes of crime and reducing the opportunities of crime. The recommended provisional security categorization for the crime prevention information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of crime prevention information on the ability of responsible agencies to create safer communities through the control and reduction of crime by addressing the causes of crime and reducing the opportunities of crime. Generally, the unauthorized disclosure of crime prevention information will have only a limited adverse effect on agency operations, assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: In a few cases, details of crime prevention programs are sensitive (e.g., location of actively monitored surveillance cameras where only a fraction of camera feeds are monitored). In such cases, unauthorized disclosure of crime prevention information might have a serious adverse effect on crime prevention operations by eliminating uncertainty regarding surveillance patterns. Therefore, the confidentiality impact might be ***moderate***.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for crime prevention information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. Crime prevention activities are not generally time-critical. In most cases, the adverse effects of unauthorized modification or destruction of crime prevention information on agency mission functions and/or public confidence in the agency would be limited.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for crime prevention information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to crime prevention information. Most crime prevention processes are tolerant of delay. In most cases, disruption of access to crime prevention information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Availability Impact Determination: In exceptional cases (e.g., orders associated with deployment of officers to provide a crime-discouraging presence in developing threat situations), loss of availability of information can have a serious adverse effect on crime prevention operations. In such cases, the availability impact might be ***moderate***.

Recommended Availability Impact Level: The provisional availability impact level recommended for crime prevention information is ***low***.

### D.16.8 Trade Law Enforcement Information Type

Trade law enforcement refers to the enforcement of anti-boycott, international loan, and general trade laws. The security categorization recommended for the trade law enforcement information type is as follows:

Security Category = {(confidentiality, Moderate), (integrity, Moderate), (availability, Moderate)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of trade law enforcement information on the ability of responsible agencies to enforce various Customs laws. Unauthorized disclosure of trade law enforcement information could potentially jeopardize fulfillment of other trade law enforcement missions. Some information that has supported a trade law enforcement process might be of higher sensitivity, and unauthorized disclosure of this information might jeopardize the success of future trade law enforcement processes. The subsequent threat to agency image or reputation can cause a serious adverse effect on an agency's mission capability. Where information includes names of informants, informant contacts, or agency personnel, the effectiveness of those personnel in future enforcement activities can be permanently impaired, or their lives threatened.

Intelligence information falls under *national security systems. National security information* and *national security systems* are outside the scope of this guideline.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for most trade law enforcement information is ***moderate***.

### Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of trade law enforcement information may depend on whether the information is time-critical. The compromise of trade law enforcement information can be serious or, in some cases, catastrophic if the information is time-critical. Also, the results of trade law enforcement activities may become matters of public record, and thus must be accurately recorded.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting trade law enforcement information may adversely affect mission operations and result in unacceptable consequences such as loss of human life. The compromise of trade law enforcement information can be serious or catastrophic if the information is time-critical. This can result in assignment of a ***high*** impact level to such information.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for most trade law enforcement information is ***moderate***.

### Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to trade law enforcement information. The effects of disruption of access to trade law enforcement information or information systems can be serious or, in some cases, catastrophic if the information is time-critical. Trade law enforcement missions are typically intolerant of significant time delays.

Recommended Availability Impact Level: The provisional availability impact level recommended for most trade law enforcement information is ***moderate***.

## D.17 Litigation and Judicial Activities

Litigation and judicial activities involve all activities necessary for the development and oversight of Federal programs.

### D.17.1 Judicial Hearings Information Type

Judicial hearings include activities associated with conducting a hearing in a court of law to settle a dispute. The general recommended security categorization for the judicial hearings information type is as follows:

Security Category = {(confidentiality, Moderate), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of judicial hearings information on the ability of responsible entities to conducting a hearing in a court of law to settle a dispute. While much information associated with judicial hearings is public, some information is sealed by the court and unauthorized disclosure is punishable by law, fine and/or imprisonment. In the vast majority of cases, unauthorized disclosure of judicial hearings information will have only a limited adverse effect on agency operations, assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Where the life of a victim, witness, or informant may be endangered by unauthorized disclosure, the confidentiality impact is ***high***. Also, where the consequences are likely to endanger public safety, the confidentiality impact is ***high***.

Recommended Confidentiality Impact Level: Given the consequences of unauthorized disclosure, the provisional confidentiality impact level recommended for judicial hearings information is ***moderate***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. Judicial hearings activities are not typically time-critical. Modification or destruction of court records can result in disruption or jeopardy to legal proceedings. In most cases, the adverse effects of unauthorized modification or destruction of judicial hearings information on agency mission functions and/or public confidence in the agency will be limited.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for judicial hearings information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to judicial hearings information. Most judicial hearings processes are tolerant of delay. In most cases, disruption of access to judicial hearings information can be expected to have only a limited adverse effect on government operations, agency assets, or individuals.

Special Factors Affecting Availability Impact Determination: In exceptional cases (e.g., orders associated with wiretap or search warrants), loss of availability of information can have a serious or severe adverse effect. In such cases, the availability impact might be ***moderate*** or ***high***.

Recommended Availability Impact Level: The provisional availability impact level recommended for judicial hearings information is ***low***.

### D.17.2 Legal Defense Information Type

Legal defense refers to the representation of a defendant in a criminal/civil court of law in an attempt to provide constitutional guarantees to legal representation. The sensitivity of much legal information is highly lifecycle-dependent. From a confidentiality perspective, most information associated with litigation and judicial activities is in the public record after the information has been presented in court. The recommended provisional security categorization for the legal defense information type is as follows:

Security Category = {(confidentiality, Moderate), (integrity, High), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of legal defense information on the representation of a defendant in a criminal/civil court of law and on the ability of the government to provide constitutional guarantees to legal representation. Dissemination of legal defense information is governed by privacy laws and by Rules of Criminal Procedure, Rules of Civil Procedure, and other laws governing adversarial legal proceedings. While much information associated with legal defense is public, some information is sealed by the court or is otherwise protected from disclosure. Violation of rules regarding unauthorized disclosure is punishable by law, disbarment, fine, and/or imprisonment. Generally, the unauthorized disclosure of legal defense information will have only a limited adverse effect on agency operations, assets, or individuals. Where unauthorized disclosure of information might have a serious adverse effect on legal defense, there is a presumption of a miscarriage of justice. If an unauthorized disclosure is discovered, the legal proceeding may be jeopardized (e.g., a mistrial may be declared). The cost to the government and others in terms of finance, time, and disruption to normal operations can be severe. If suspicion is raised concerning government complicity or negligence, serious loss of public confidence in government agencies or the legal process may result.

Special Factors Affecting Confidentiality Impact Determination: Where the life of a victim, witness, or informant may be endangered by disclosure, the confidentiality impact will be ***high***. Also, where the consequences of a miscarriage of justice are likely to endanger public safety (e.g., release of a terrorist or other murderer), the confidentiality impact will be ***high***.

Recommended Confidentiality Impact Level: Given legal consequences of unauthorized disclosure, the provisional confidentiality impact level recommended for legal defense information is ***moderate***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. Legal defense activities are not typically time-critical. In most cases, unauthorized modification or destruction of legal defense information will have only a limited adverse effect on government operations, government assets, or individuals.

Special Factors Affecting Integrity Impact Determination: For legal defense information, when evidence or other defense information has been compromised the legal proceedings can be jeopardized. As a consequence, the cost to the government and other entities in terms of finance, time, and disruption to normal operations may be severe. If suspicion is raised concerning government complicity or negligence, serious loss of public confidence in government agencies or the legal process may result. In this case, the integrity impact level will be ***moderate***.

When the modification or destruction of legal defense information endangers public safety (e.g., release of a terrorist or other murderer), the integrity impact will be ***high***. Even if public safety is not endangered, the modification or destruction of legal defense information may result in expensive and disruptive civil or criminal proceedings.

Recommended Integrity Impact Level: Given the legal consequences of unauthorized modification or destruction and potential consequences for human life, the provisional integrity impact level recommended for legal defense information is ***high***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to legal defense information. Most legal defense processes are tolerant of delay. Delays can impact court schedules, cause significant taxpayer expense, and potentially jeopardize legal proceedings (see C17.2.2). In most cases, disruption of access to legal defense information can be expected to have only a limited adverse effect on government operations, agency assets, or individuals.

Special Factors Affecting Availability Impact Determination: In exceptional cases (e.g., information affecting a ruling regarding an impending execution), loss of availability of information can have a severe adverse effect. The consequent availability impact level would be ***high***.

Special Factors Affecting Availability Impact Determination: The provisional availability impact level recommended for legal defense information is ***low***.

### D.17.3 Legal Investigation Information Type

Legal investigation supports activities associated with gathering information about a given party (government agency, citizen, corporation) that would be admissible in a court of law, in an attempt to prove guilt or innocence. The recommended provisional categorization of the legal investigation information type follows:

Security Category = {(confidentiality, Moderate), (integrity, Moderate), (availability, Moderate)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of legal investigation information on the ability of responsible agencies to gather information about a given party (government agency, citizen, corporation) that would be admissible in a court of law, in an attempt to prove guilt or innocence.

Special Factors Affecting Confidentiality Impact Determination: The consequences of unauthorized disclosure of legal investigation information depend 1] on the seriousness of the crime involved, 2] timing (e.g., the ability of the criminal[40] to access the information and use it to commit a crime or to evade detection or surveillance), and 3] on the capability criminal to injure witnesses or law enforcement officials. In cases where 1) the crimes are not violent and do not involve extraordinarily large property losses, and 2) there is no indication of a record of violence on the part of the criminal, the confidentiality impact may be ***low*** or ***moderate***.

Given the nature of many of the crimes that are the responsibility of Federal law enforcement agencies, the consequences associated with unauthorized disclosure of legal investigation information will pose a threat to human life or result in a loss of major assets. Additionally, when the disclosure concerns matters of multi-national interest, such as trade enforcement, tariff agreements, etc., or where foreign nationals might be involved, the confidentiality impact will be ***high***. Information that reveals the identity and/or location of informants may be of particular concern.

Recommended Confidentiality Impact Level: Given potentially serious to severe legal consequences of unauthorized disclosure, the provisional confidentiality impact level recommended for legal investigation information is ***moderate***.

#### Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of legal investigation information may depend on whether the information is time-critical. Unauthorized modification or destruction of information affecting external communications associated with legal investigative organizations (e.g., web pages, electronic mail) may adversely affect operations or public confidence in the agency, but the damage to the mission would usually be limited.

Where unauthorized modification or destruction of information has an adverse effect on the granting/executing of a search or wiretap warrant or on the success of the subsequent prosecution, a serious adverse effect on agency operations may result. This can place the agency at a significant disadvantage.

Special Factors Affecting Integrity Impact Determination: Legal investigation mission requirements may include time-critical information. In such cases, major investigations can be jeopardized by the unauthorized modification or destruction of legal investigation information. Where the criminal case under investigation involves major property losses, large-scale financial frauds, poses a threat to key national assets or human life, the integrity impact level recommended for legal investigation information is ***high***.

[40] In this case, the term "criminal entity" includes both the criminal and legal representative(s) of the criminal (i.e., council).

When legal investigation information addresses international matters, such as trade enforcement or tariff agreements or when foreign nationals are involved, the integrity level is ***high***. Any deliberate or inadvertent corruption of such information could result in catastrophic adverse effects on future operations, individual or agency reputations, and human life.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for legal investigation information is ***moderate***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to legal investigation information. Missions supported by legal investigation information are not typically tolerant of delay with resultant serious consequences for ongoing investigations.

Special Factors Affecting Availability Impact Determination: Where the crimes involved pose a threat to human life and/or result in a loss of major assets, the availability impact level recommended for legal investigation information is ***high***.

Recommended Availability Impact Level: The provisional availability impact level recommended for legal investigation information is ***moderate***.

### D.17.4 Legal Prosecution and Litigation Information Type

Legal prosecution/litigation includes all activities involved with presenting a case in a legal proceeding both in a criminal or civil court of law in an attempt to prove guilt/responsibility. The recommended provisional security categorization for the legal prosecution/litigation information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Moderate), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of legal prosecution/litigation information on the ability of responsible agencies to present a case in a legal proceeding either in a criminal or civil court of law in an attempt to prove guilt/responsibility. Dissemination of legal prosecution/litigation information is governed by privacy laws and by Rules of Criminal Procedure, Rules of Civil Procedure, and other laws governing adversarial legal proceedings. While most information associated with legal prosecution/litigation is public, some information is sealed by the court or is otherwise protected from disclosure. Violation of rules regarding unauthorized disclosure is punishable by law, disbarment, fine, and/or imprisonment. Generally, the unauthorized disclosure of legal prosecution/litigation information will have only a limited adverse effect on agency operations, assets, or individuals. In criminal cases, the consequences of unauthorized disclosure of legal prosecution information are affected by 1] the seriousness of the crime involved, 2] timing (e.g., the ability of the criminal to access the information and use it to commit a crime or evade detection or surveillance), and 3] the capability of the criminal to injure witnesses or law enforcement officials.

Special Factors Affecting Confidentiality Impact Determination: Where unauthorized disclosure of information might have a serious adverse effect on legal prosecution/ litigation, there is a presumption of a miscarriage of justice. If an unauthorized disclosure is discovered, the legal proceeding is jeopardized (e.g., a mistrial may be declared). The cost to the government and others in terms of finance, time, and disruption to normal operations can be severe. If suspicion is raised concerning government complicity or negligence, serious loss of public confidence in government agencies or the legal process may result. In this case, the confidentiality impact of unauthorized disclosure will be ***moderate***.

Where the life of a complainant, victim, witness, or informant may be endangered by disclosure, the confidentiality impact will be ***high***. Also, where the consequences of a miscarriage of justice are likely to endanger public safety (e.g., release of a terrorist or other murderer), the confidentiality impact will be ***high***.

Given the nature of many of the crimes that are the responsibility of Federal law enforcement agencies, the consequences associated with unauthorized disclosure of legal prosecution information must be assumed to pose a threat to human life or result in a loss of major assets. Additionally, when a legal proceeding concerns matters of trans-national interest, such as trade enforcement, tariff agreements, etc., or where foreign nationals might be involved, the confidentiality impact will be ***high***. Information that reveals the identity and/or location of informants may be of particular concern.

[The impact of unauthorized disclosure of *national security information* is outside the scope of this guideline.]

Recommended Confidentiality Impact Level: Given the public nature of and disclosure rules associated with most prosecution/litigation information, the provisional confidentiality impact level recommended is ***low***. In cases where 1) the crimes are not violent and do not involve extraordinarily large property losses, and 2) there is no indication of a record of violence on the part of the criminal, the confidentiality impact may be ***low***.

### Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. Legal prosecution/litigation activities are not typically time-critical. Unauthorized modification or destruction of information affecting external communications associated with legal prosecution/litigation organizations (e.g., web pages, electronic mail) may adversely affect operations or public confidence in the agency, but the damage to the mission would usually be limited. In general, the unauthorized modification or destruction of legal prosecution/litigation information will have only a limited adverse effect on government operations, government assets, or individuals. However, if evidence or other defense information has been compromised, legal proceedings may be affected (e.g., a mistrial may be declared). The subsequent cost to the government in terms of finance, time, and disruption to normal operations may be severe. If suspicion is raised concerning government complicity or negligence, serious loss of public confidence in government agencies or the legal process may result.

Special Factors Affecting Integrity Impact Determination: Where the life of a victim, witness, or informant may be endangered, the integrity impact will be ***high***. Also, where the consequences of a miscarriage of justice are likely to endanger public safety (e.g., release of a terrorist or other murderer), the integrity impact will be ***high***.

Recommended Integrity Impact Level: Given the legal consequences of the unauthorized modification or destruction of legal prosecution/litigation information, the provisional integrity impact level recommended for legal prosecution/litigation information is ***moderate***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to legal prosecution/litigation information. Most legal prosecution/litigation processes are tolerant of delay even though the delays can impact court schedules, cause significant taxpayer expense, and potentially jeopardize legal proceedings (see C17.4.2). Typically, the disruption of access to legal prosecution/litigation information can be expected to have only a limited adverse effect on government operations, agency assets, or individuals.

Special Factors Affecting Availability Impact Determination: In exceptional cases (e.g., information affecting a ruling regarding an impending execution), loss of availability of information can have a severe adverse effect. The availability impact level recommended for this legal prosecution/litigation information is ***high***.

Recommended Availability Impact Level: The provisional availability impact level recommended for legal prosecution/litigation information is ***low***.

### D.17.5 Resolution Facilitation Information Type

Resolution facilitation involves all activities outside of a court of law that may be used in an attempt to settle a dispute between two or more parties (government, citizen, corporation). The general recommended security categorization for the resolution facilitation information type is as follows:

Security Category = {(confidentiality, Moderate), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of resolution facilitation information on the ability of responsible entities to settle a dispute between two or more parties (government, citizen, corporation) outside of a court of law. While some information associated with resolution facilitation is public, much of the information is private and/or proprietary. Unauthorized disclosure of such information can disrupt or defeat the dispute resolution process. The consequences typically depend on the nature of the dispute. Jeopardy to the resolution process will not usually involve threats to critical infrastructures, key national assets, or human life. Typically, the unauthorized disclosure of resolution facilitation information will have only a limited adverse effect on agency operations, assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Where large monetary amounts and/or violent crimes are involved, the confidentiality impact of unauthorized disclosure of resolution facilitation information is at least ***moderate***.

In exceptional cases human lives may be jeopardized by failure of the resolution facilitation process. Additionally, when resolution facilitation concerns matters of trans-national interest, such as trade enforcement, tariff agreements, etc., or where foreign nationals might be involved, the confidentiality impact will be ***high***.

Recommended Confidentiality Impact Level: Given the legal consequences of unauthorized disclosure, the provisional confidentiality impact level recommended for resolution facilitation information is ***moderate***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. Resolution facilitation activities are not typically time-critical. The modification or destruction of court records may result in disruption or jeopardy of legal proceedings. In most cases, the adverse effects of unauthorized modification or destruction of resolution facilitation information on agency mission functions and/or public confidence in the agency can be expected to be limited.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for resolution facilitation information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to resolution facilitation information. Most resolution facilitation processes are tolerant of delay. In most cases, disruption of access to resolution facilitation information can be expected to have only a limited adverse effect on government operations, agency assets, or individuals.

Recommended Availability Impact Level: The provisional availability impact level recommended for resolution facilitation information is ***low***.

## D.18 Federal Correctional Activities

Correctional Activities involves all Federal activities that ensure the effective incarceration and rehabilitation of convicted criminals.

### D.18.1 Criminal Incarceration Information Type

Criminal incarceration includes activities associated with the housing, custody and general care of criminals sentenced to serve time in penitentiaries. The following security categorization is recommended for the criminal incarceration information type:

Security Category = {(confidentiality, Low), (integrity, Moderate), (availability, Low)}

### Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of criminal incarceration information on the ability of responsible agencies to provide housing, custody, and general care for criminals sentenced to serve time in a Federal penitentiary. The consequences of unauthorized disclosure of most criminal incarceration information are unlikely to have a serious adverse effect on agency operations. The most serious adverse effects are likely to involve exposure of information that is proprietary to prisoners that can result in damaging publicity for an organization. (Unauthorized disclosure of some information can conceivably have serious impact on the status or resolution of appeal actions). The consequences of unauthorized disclosures may have an adverse effect on public confidence in the agency.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for most criminal incarceration information is normally ***low***.

### Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of criminal incarceration information can be serious if the information is time-critical and results in the premature release of a criminal, unjust retention of an individual in the prison system, or harm to a citizen's reputation or public confidence in the government.

Special Factors Affecting Integrity Impact Determination: In some cases (e.g., instructions regarding a need to isolate a prisoner from the general prison population for personal safety reasons), the unauthorized modification or destruction of criminal incarceration information can result in loss of human life a ***high*** impact potential.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for criminal incarceration information is ***moderate***.

### Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to criminal incarceration information. Criminal incarceration processes are usually tolerant of reasonable delays.

Special Factors Affecting Availability Impact Determination: There may be cases (e.g. emergency bulletins affecting prisoner health and/or safety) in which emergency dissemination of information regarding life-threatening situations is delayed for excessive periods. Such cases can result in a ***high*** availability impact level.

Recommended Availability Impact Level: The provisional availability impact level recommended for criminal incarceration information is ***low***.

### D.18.2 Criminal Rehabilitation Information Type

Criminal Rehabilitation includes all government activities devoted to providing convicted criminals with the educational resources and life skills necessary to rejoin society as responsible and contributing members. The recommended provisional categorization of the criminal rehabilitation information type follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of criminal rehabilitation information on the ability of responsible agencies to provide convicted criminals with the educational resources and life skills necessary to rejoin society as responsible and contributing members. The consequences of unauthorized disclosure of most criminal rehabilitation information would have a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Exceptions that might have a potential for more serious consequences are based on privacy information processed in criminal rehabilitation systems (e.g., information required by the Privacy Act of 1974 (The Privacy Act Information provisional impact levels are documented in the Personal Identity and Authentication information type) or other statutes and executive orders to receive special handling to protect the privacy of individuals). This can result in assignment of a ***moderate*** impact level to such information.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for criminal rehabilitation information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of criminal rehabilitation information would have a limited adverse effect on agency operations, agency assets, or individuals. Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for most criminal rehabilitation information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to criminal rehabilitation information. The effects of disruption of access to most criminal rehabilitation information or information systems would have a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The provisional availability impact level recommended for criminal rehabilitation information is ***low***.

## D.19 General Sciences and Innovation

General Science and Innovation includes all Federal activities to meet the national need to advance knowledge in this area. This includes general research and technology programs, space exploration activities, and other research and technology programs that have diverse goals and cannot be readily classified into another mission area or information type.

### D.19.1 Scientific and Technological Research and Innovation Information Type

Scientific and Technological Research and Innovation includes all federal activities whose goal is the creation of new scientific and/or technological knowledge as a goal in itself, without a specific link to the other mission areas or information types identified in the BRM. Most sensitive information is developed under research and development programs that directly support another of the mission areas described in this Appendix and are not included here. Some information associated with scientific and technical research and innovation is *national security information* and is outside the scope of this guideline. The recommended provisional categorization for the scientific and technical research and innovation information type follows:

Security Category = {(confidentiality, Low), (integrity, Moderate), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of scientific and technical research and innovation information on the ability of responsible agencies to create new scientific and/or technological knowledge as a goal in itself, without a specific link to other program areas or information types. Many scientific and technical research and innovation activities are conducted in association with public institutions of higher learning, and the findings resulting from those activities are intended for publication.

Special Factors Affecting Confidentiality Impact Determination: The pre-publication disclosure or other unauthorized disclosure of information associated with competition for funding and recognition (e.g., grants, development contract, patent rights, and copyrights) can have a serious adverse effect on agency operations, agency assets, or individuals. In such cases, the confidentiality impact level associated for scientific and technical research and innovation information will be ***moderate***.

In some cases, the information associated with scientific and technical research and innovation is classified or otherwise qualified as *national security information*. Such information is outside the scope of this guideline.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for most scientific and technical research and innovation information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of most information associated with scientific and technical research and innovation can be seriously disruptive to the progress of research activities. The effects on future funding can be quite serious and can have a serious adverse effect on agency operations, agency assets, or individuals. Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be more limited.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for scientific and technical research and innovation information is ***moderate***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to scientific and technical research and innovation information. Most research processes are tolerant of delay. In most cases, disruption of access to research and innovation information can be expected to have only a limited adverse effect on government operations, agency assets, or individuals.

Recommended Availability Impact Level: The provisional availability impact level recommended for scientific and technical research and innovation information is ***low***.

### D.19.2 Space Exploration and Innovation Information Type

Space Exploration and Innovation includes all activities devoted to innovations directed at human and robotic space flight and the development and operation of space launch and transportation systems, and the general research and exploration of outer space. While some space exploration and innovation is *national security information*, most sensitive information is developed under research and development programs that directly support another of the mission areas described in this Appendix and are not included here. The recommended provisional categorization of the research and development information type follows:

Security Category = {(confidentiality, Low), (integrity, Moderate), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of space exploration and innovation information on the ability of responsible agencies to conduct activities devoted to [1] innovations directed at human and robotic space flight and the development and operation of space launch and transportation systems, and [2] the general research and exploration of outer space. Many space exploration and innovation activities are conducted with public institutions of higher learning, and the findings resulting from those activities are intended for publication.

Special Factors Affecting Confidentiality Impact Determination: The pre-publication disclosure or other unauthorized disclosure of information associated with competition for funding and recognition (e.g., grants, development contract, patent rights, and copyrights) can have a serious adverse effect on agency operations, agency assets, or individuals. In such cases, the confidentiality impact associated with space exploration and innovation is ***moderate***.

In some cases, the space exploration and innovation information is classified or otherwise qualifies as *national security information.* This information is outside the scope of this guideline.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for most space exploration and innovation information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of most space exploration and innovation information can be seriously disruptive to the progress of research activities. The effects on future funding can be quite serious and can have a serious adverse effect on agency operations, agency assets, or individuals. Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for space exploration and innovation information is ***moderate***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to space exploration and innovation information. Most research and innovation processes are tolerant of delay. In most cases, disruption of access to research and innovation information will have only a limited adverse effect on government operations, agency assets, or individuals.

Recommended Availability Impact Level: The provisional availability impact level recommended for space exploration and innovation information is ***low***.

## D.20 Knowledge Creation and Management

Knowledge Creation and Management involves the programs and activities in which the Federal Government creates or develops a body or set of knowledge, the manipulation and analysis of which can provide inherent benefits for both the Federal and private sector.

### D.20.1 Research and Development Information Type

Research and Development involves the gathering and analysis of data, dissemination of results, and development of new products, methodologies, and ideas. The sensitivity and criticality of most research and development information depends on the subject matter involved. The recommended provisional categorization of the research and development information type follows:

Security Category = {(confidentiality, Low), (integrity, Moderate), (availability, Low)}

#### Confidentiality

The confidentiality impact level depends on the effect of unauthorized disclosure of research and development information on the ability of responsible agencies to gather and analyze data, disseminate results, and develop new products, methodologies, and ideas, and on the degree to which unauthorized disclosure of the information can assist hostile institutions to do harm to the interests of the government of the United States. Many research and development activities are conducted in association with public institutions of higher learning, and the findings resulting from those activities are intended for publication. Unauthorized disclosure of most research and development information can be expected to have only limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Most research and development information is proprietary. Unauthorized disclosure of proprietary information violates several statures and Federal regulations (see Appendix E). Pre-publication disclosure or other unauthorized disclosure of research findings can have a serious adverse effect on agency operations, agency assets, or individuals. In such cases, the confidentiality impact level associated with research and development is ***moderate***.

Premature and/or partial release of preliminary research and development information can lead to misleading conclusions by policy makers, funding entities, news organizations, and/or the general public. Where the research and development activities are associated with security measures or law enforcement tools, potential adversaries may derive insights on countermeasures development. In extreme cases, the resulting confidentiality impact can be ***high***.

In some cases, the research and development information is classified or otherwise qualifies as *national security information*). Such information is outside the scope of this guideline.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for most government research and development information is ***low***.

#### Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of most research and development information can be seriously disruptive to the progress of research activities. The effects on future funding can be serious and can have a serious adverse effect on agency operations, agency assets, or individuals. Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be more limited.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for research and development information is ***moderate***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to research and development information. Most research and innovation processes are tolerant of delay. In most cases, disruption of access to research and innovation information will have only a limited adverse effect on government operations, agency assets, or individuals.

Recommended Availability Impact Level: The provisional availability impact level recommended for research and development information is ***low***.

### D.20.2 General Purpose Data and Statistics Information Type

General purpose data and statistics includes activities performed in providing empirical, numerical, and related data and information pertaining to the current state of the nation in areas such as the economy, labor, weather, international trade, etc. The recommended provisional categorization of the General Purpose Data and Statistics information type follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of general purpose data and statistics information on the ability of responsible agencies to provide empirical, numerical, and related data and information pertaining to the current state of the nation in areas such as the economy, labor, weather, international trade, etc. The consequences of unauthorized disclosure of most general-purpose data and statistics information would have only a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Unauthorized premature disclosure of much economic (e.g., agricultural commodity, economic indicators) data and statistics information can result in major financial consequences. In some cases, premature disclosure of this information can impact major financial markets and damage national banking and finance infrastructures. Unauthorized and premature disclosure to a single institution (e.g., a major commodity brokerage house), could damage faith in general-purpose data and statistics gathering and development institutions, result in even more market disruption, and have a severe or catastrophic adverse effect on public confidence in the agency. Even when the consequences are limited to giving an unfair market advantage to a single financial or commercial institution, unauthorized disclosure can have a serious adverse effect on public confidence in the agency and its staff. This can result in assignment of a ***moderate*** impact level to such information.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for most general-purpose data and statistics information is ***low.***

#### Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of general-purpose data and statistics information may depend on whether the information is time-critical. Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations or public confidence in the agency, but the damage to the mission would usually be limited.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for general-purpose data and statistics information is ***low***.

#### Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to general-purpose data and statistics information. Missions supported by general-purpose data and statistics information are generally tolerant of delay.

Recommended Availability Impact Level: The provisional availability impact level recommended for general-purpose data and statistics information is ***low***.

### D.20.3 Advising and Consulting Information Type

Advising and Consulting activities involve the guidance and consultative services provided by the Federal Government to support the implementation of a specific service provided to citizens. The recommended provisional categorization of the advising and consulting information type follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

#### Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of advising and consulting information on the ability of responsible agencies to provide guidance and consultative services to support the implementation of a specific service to citizens. The consequences of unauthorized disclosure of advising and consulting information depends on the nature of the service being provided and on the sensitivity of the information with which advisory or consulting entities are working. The consequences of unauthorized disclosure of most advising and consulting information would have a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Where consulting support involves classified or other *national security information*, the consequences of unauthorized disclosure can be severe but are outside the scope of this guideline. In other cases, such as consultative services provided to law enforcement institutions, the consequences of unauthorized disclosure can be serious or even life threatening. This can result in assignment of a ***moderate*** or ***high*** impact level to such information.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for advising and consulting information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of advising and consulting information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals. Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for advising and consulting information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to advising and consulting information. The effects of disruption of access to most advising and consulting information or information systems would have limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The provisional availability impact level recommended for advising and consulting information is ***low***.

### D.20.4 Knowledge Dissemination Information Type

Knowledge Dissemination addresses those instances where the primary method used in delivering a service is through the publishing or broadcasting of information, such as the Voice of America or web-based museums maintained by the Smithsonian. Knowledge Dissemination is not intended to address circumstances where the publication of information is a by-product of a mission rather than the mission itself. The recommended provisional security categorization of the knowledge dissemination information type follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of knowledge dissemination information on the ability of responsible agencies to publish or broadcast information. Premature and unauthorized disclosure of information being considered for broadcast can be harmful if the information is subsequently determined to be false or counterproductive to the knowledge dissemination mission. However, the consequences of unauthorized disclosure of most knowledge dissemination information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Unauthorized disclosure of some policies governing knowledge dissemination missions can be harmful to the agency mission (e.g., some internal Voice of America editorial policies). This can result in assignment of a ***moderate*** impact level to such information.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for knowledge dissemination information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of knowledge dissemination information may depend on whether the information is time-critical. Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited. In most cases, the consequences of unauthorized modification or destruction of knowledge dissemination information would have a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Integrity Impact Determination: In cases of dissemination of erroneous/defamatory information, an agency mission can be seriously harmed and the impact level will be ***moderate***.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for knowledge dissemination information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to knowledge dissemination information. The effects of disruption of access to most knowledge dissemination information or information systems would have a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Availability Impact Determination: An exception is the extended disruption of broadcast capabilities (e.g., Voice of America). Here, the agency mission is seriously harmed and the impact of the consequences will be ***moderate***.

Recommended Availability Impact Level: The provisional availability impact level recommended for most knowledge dissemination information is ***low***.

## D.21 Regulatory Compliance and Enforcement

Regulatory Compliance and Enforcement involves the direct monitoring and oversight of a specific individual, group, industry, or community participating in a regulated activity via market mechanisms, command and control features, or other means to control or govern conduct or behavior.

### D.21.1 Inspections and Auditing Information Type

Inspections and Auditing involves the methodical examination and review of regulated activities to ensure compliance with standards for regulated activity. The recommended security categorization for the inspections and auditing information type is as follows:

Security Category = {(confidentiality, Moderate), (integrity, Moderate), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of inspections and auditing information on the ability of responsible agencies to methodically examine and review regulated activities to ensure compliance with standards for regulated activity. If the inspections and auditing data belongs to one of the information types described in this guideline, the confidentiality impact assigned the data and system is dependent on the nature of the regulated activity.

Special Factors Affecting Confidentiality Impact Determination: Unauthorized disclosure of inspections and auditing information can alert personnel associated with programs being monitored to the focus of inspection or auditing activities. With this information, program personnel may divert attention from questionable program attributes or hide unfavorable information. Where a major program or human safety is at stake, actions taken based on unauthorized disclosure of inspections and auditing information can pose a threat to human life or a loss of major assets. In such cases, the confidentiality impact is ***high***.

*National security information* and *national security systems* are outside the scope of this guideline.

Recommended Confidentiality Impact Level: Although there are many Federal environments in which unauthorized disclosure will have only a limited adverse effect, there are enough circumstances in which serious adverse effects on agency operations, agency assets, or individuals can result to justify recommendation of a ***moderate*** provisional confidentiality impact level for inspections and auditing information.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of inspections and auditing information can compromise the effectiveness of the program. The damage likely to be caused by unauthorized modification or destruction may affect inspection or audit results with subsequent serious adverse effects on agency operations or public confidence in the agency. The consequences can be particularly serious if the destruction or modification of information invalidates oversight of major programs or the information threatens human safety. The integrity impact level depends on the laws or policies with which compliance is being determined and on the criticality of the processes being monitored (e.g., correctness of contract expenditure reporting versus safety regulations affecting manned space flight).

Recommended Integrity Impact Level: Although there are regulatory environments in which a ***low*** impact level is appropriate, the circumstances associated with most inspections and auditing support information require at least a ***moderate*** provisional integrity impact level.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to inspections and auditing information. In most cases, disruption of access to inspections and auditing information is expected to have only a limited adverse effect on agency operations, agency assets, or individuals. Not many inspection or auditing operations involve activities for which temporary loss of availability is likely to cause significant degradation in mission capability, place the agency at a significant disadvantage, result in major damage to major assets, or pose a threat to human life.

Recommended Availability Impact Level: For most inspection and audit functions, the recommended provisional availability impact level is ***low***.

### D.21.2 Standards Setting/Reporting Guideline Development Information Type

Standard Setting/Reporting Guideline Development involves the establishment of allowable limits associated with a regulated activity and the development of reporting requirements necessary to monitor and control compliance with allowable limits. This includes the development of requirements for product sampling and testing, emissions monitoring and control, incident reporting, financial filings, etc. The following provisional security categorization is recommended for the standards setting/reporting guideline development information type:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of standards setting/reporting guideline development information on the abilities of responsible agencies to establish allowable limits associated with a regulated activity and to develop reporting requirements necessary to monitor and control compliance with allowable limits. In a few cases, the unauthorized public dissemination of standards or guidelines

information can harm the effectiveness of the function being supported (e.g., public dissemination of Internal Revenue Service audit thresholds for certain deductions). However, most Federal standards and guidelines are intended for public dissemination. The consequences of unauthorized disclosure of the majority of standards setting/reporting guideline development information will result in a limited adverse effect on agency operations, agency assets, or individuals.

There are some cases for which standards or guidelines include classified or other *national security information*. Such cases are outside the scope of this guideline.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for standards setting/reporting guideline development information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of standards setting/reporting guideline development information depends primarily on the criticality of the information with respect to agency mission capability, protection of agency assets, and safety of individuals. In general, the effects of modifications or deletions of standards setting/reporting guideline development information are limited with respect to agency missions or assets.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for standards setting/reporting guideline development information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to standards setting/reporting guideline development information. The nature of standards setting/reporting guideline development processes is tolerant of reasonable delays.

Recommended Availability Impact Level: The provisional availability impact level recommended for standards setting/reporting guideline development information is ***low***.

### D.21.3 Permits and Licensing Information Type

Permits and Licensing involves activities associated with granting, revoking, and the overall management of the documented authority necessary to perform a regulated task or function. The following security categorization is recommended for the permits and licensing information type:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of permits and licensing information on the abilities of responsible agencies to manage the documented authority necessary to perform a regulated task or function. The consequences of unauthorized disclosure of the majority of permits and licensing information will result in a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Where more sensitive information is involved, it will typically be personal information subject to the Privacy Act of 1974, the Health Insurance Portability and Accountability Act of 1996, or other laws and executive orders affecting the dissemination of information regarding individuals. The Privacy Act Information provisional impact levels are documented in the Personal Identity and Authentication information type. In such cases, the consequences of unauthorized disclosure of permits and licensing information could be serious. In such cases, the confidentiality impact level might be ***moderate***.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for most permits and licensing information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of permits and licensing information depends primarily on the criticality of the regulated activity with respect to protection of government assets, and safety of individuals. Typically, the effects of modification or deletion of permits and licensing information are limited with respect to agency missions or assets.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for permits and licensing information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to permits and licensing information. The nature of permits and licensing processes is tolerant of reasonable delays.

Recommended Availability Impact Level: The provisional availability impact level recommended for permits and licensing information is ***low***.

## D.22 Public Goods Creation and Management

The construction, manufacturing, administration, and/or management of goods, structures, facilities, common resources, etc. used for the general well being of the American public or society at large.

### D.22.1 Manufacturing Information Type

Manufacturing involves all programs and activities in which the Federal Government produces both marketable and non-marketable goods. The following provisional security categorization is recommended for the manufacturing information type:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of manufacturing information on the abilities of responsible agencies to produce both marketable and non-marketable goods. In a few cases, unauthorized disclosure of details of the products or manufacturing processes can give adversaries opportunities (e.g., terrorism, industrial espionage). However, in most cases, the consequences of unauthorized disclosure of manufacturing information will result in a limited adverse effect on agency operations, agency assets, or individuals.

There are some cases for which manufacturing or product information includes classified or other *national security information*. Such cases are outside the scope of this guideline.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for manufacturing information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of manufacturing information depends primarily on the criticality of the information with respect to a manufacturing process and on the volume and use of the end product. Typically, the effects of modification or deletion of manufacturing information are generally limited with respect to agency missions or assets.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for manufacturing information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to manufacturing information. The nature of most government manufacturing processes is tolerant of reasonable delays.

Recommended Availability Impact Level: The provisional availability impact level recommended for manufacturing information is ***low***.

### D.22.2 Construction Information Type

Construction involves all programs and activities in which the Federal Government builds or constructs facilities, roads, dams, etc. The following security categorization is recommended for the construction information type:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of construction information on the abilities of responsible agencies to build or construct facilities, roads, dams, etc. In most cases, the consequences of unauthorized disclosure of construction information will result in a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: In some cases, construction details can be of use to terrorists or other criminals who seek to penetrate or destroy government installations. Unauthorized disclosure of some construction details (e.g., alarm designs, points of vulnerability to the structural integrity of a dam or building) can result in danger to critical infrastructures, key national assets, or human life. In such cases, the confidentiality impact may be ***high***.

There are some cases for which construction information includes classified or other *national security information*. Such cases are outside the scope of this guideline.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for construction information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of construction information depends primarily on the criticality of the information. Typically, the effects of modification or deletion of construction information are limited with respect to agency missions or assets.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for construction information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to construction information. The nature of most government construction processes is tolerant of reasonable delays.

Recommended Availability Impact Level: The provisional availability impact level recommended for construction information is ***low***.

### D.22.3 Public Resources, Facility and Infrastructure Management Information Type

Public Resources, Facility and Infrastructure Management involves the management and maintenance of government-owned capital goods and resources (natural or otherwise) on behalf of the public, usually with benefits to the community at large as well as to the direct user. Examples of facilities and infrastructure include schools, roads, bridges, dams, harbors, and public buildings. Examples of resources include parks, cultural artifacts and art, endangered species, oil reserves, etc. The following security categorization is recommended for the public resources, facilities, and infrastructure management information type:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of public resources, facilities, and infrastructure management information on the abilities of responsible agencies to manage and maintain government-owned capital goods and resources (natural or otherwise) on behalf of the public, usually with benefits to the community at large as well as to the direct user. In most cases, the consequences of unauthorized disclosure of public resources, facilities, and infrastructure management information will result in a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: In some cases, premature unauthorized disclosure of management information can give an unfair competitive advantage to a commercial interest (e.g., proposed changes for management of petroleum reserves). The confidentiality impact of consequent loss of public confidence and/or serious economic disruption might be ***moderate***.

In other cases, public resources, facilities, and infrastructure management details can be of use to terrorists or other criminals who seek to penetrate the security of government property or to harm populations. Unauthorized disclosure of some public resources, facilities, and infrastructure management details to criminals (e.g., facilities security dispositions, building alarm designs), can result in danger to critical infrastructures, key national assets, or human life. In such cases, the confidentiality impact can be ***high***

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for most public resources, facilities, and infrastructure management information is ***low***.

### Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of public resources, facilities, and infrastructure management information depends primarily on the criticality of the information with respect to management of public resources, facilities, and infrastructures. Typically, the effects of modification or deletion of public resources, facilities, and infrastructure information are limited with respect to agency missions or assets.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for public resources, facilities, and infrastructure management information is ***low***.

### Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to public resources, facilities, and infrastructure management information. The nature of most government public resources, facilities, and infrastructure management processes is tolerant of reasonable delays.

Recommended Availability Impact Level: The provisional availability impact level recommended for public resources, facilities, and infrastructure management information is ***low***.

## D.22.4 Information Infrastructure Management Information Type

Information Infrastructure Management involves the management and stewardship of a type of information by the Federal Government and/or the creation of physical communication infrastructures on behalf of the public in order to facilitate communication. This includes the management of large amounts of information (e.g., environmental and weather data, criminal records, etc.), the creation of information and data standards relating to a specific type of information (patient records), and the creation and management of physical communication infrastructures (networks) on behalf of the public.

Note: Information infrastructures for government use are not included in this information type because the impact levels associated with information infrastructure maintenance information are primarily a function of the information processed in that infrastructure. The recommended provisional security categorization for the information infrastructure maintenance information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

#### Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of information infrastructure maintenance information on the ability of responsible agencies to manage a type of information and/or to create physical communication infrastructures on behalf of the public in order to facilitate communication. The disclosure of most information infrastructure maintenance information can be expected to result in a limited adverse effect on agency operations, assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: In some cases, information infrastructure maintenance details can be of use to terrorists or other criminals who seek to destroy government data bases or communications infrastructures, or deny access to information needed by the public. Unauthorized disclosure of some information infrastructure maintenance details to criminals can result in danger to critical infrastructures, key national assets, or human life. In such cases, the confidentiality impact can be ***high***. In other cases, premature unauthorized disclosure of management information can give an unfair competitive advantage to a commercial interest (e.g., proposed outsourcing of system administration or details of a proposed communications system acquisition). This can result in assignment of a ***moderate*** impact level to such information.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for information infrastructure maintenance information is ***low***.

#### Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. That is, the consequences of unauthorized modification or destruction of information infrastructure maintenance information typically depend on the criticality of the data processed by the infrastructure and whether this data is time-critical. In most cases, the data will not be urgently needed or acted upon immediately.

Special Factors Affecting Integrity Impact Determination: In a relatively few cases, the consequences of unauthorized modification or destruction of information infrastructure maintenance information might result in serious damage to agency operations, assets, or human safety. This may require a ***moderate*** or ***high*** integrity impact level for information infrastructure maintenance information.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for information infrastructure maintenance information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to information infrastructure maintenance information. Disruption of access to information infrastructure maintenance information or information systems will typically result in denial of access to resources for all affected agencies. Typically, disruption of access will have a limited adverse effect on agency operations (including mission functions and public confidence in the agency), agency assets, or individuals.

Special Factors Affecting Availability Impact Determination: Exceptions may include emergency response aspects of disaster management or other time critical functions (e.g., some systems that support air traffic control functions). The availability impact level associated with unauthorized modification or destruction of information infrastructure maintenance information needed to respond to emergencies or critical to public safety may be ***high***.

Recommended Availability Impact Level: The provisional availability impact level recommended for information infrastructure maintenance information is ***low***.

## D.23 Federal Financial Assistance

Federal Financial Assistance is the provision of earned and unearned financial or monetary-like benefits to individuals, groups, or corporations.

### D.23.1 Federal Grants (Non-State) Information Type

Federal Grants involve the disbursement of funds by the Federal Government to a non-Federal entity to help fund projects or activities. This includes the processes associated with grant administration, including the publication of funds availability notices, development of the grant application guidance, determination of grantee eligibility, coordination of the peer review/evaluation process for competitive grants, the transfer of funds, and the monitoring/oversight as appropriate. The recommended provisional security categorization for the federal grants information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of federal grants information on the ability of responsible agencies to disburse funds to non-Federal entities to fund projects or activities. Typically, unauthorized disclosure of federal grants information will have only a limited adverse effect on agency operations, assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: In a few cases, records associated with grants may include information subject to privacy restrictions (e.g., the Privacy Act of 1974). The Privacy Act Information provisional impact levels are documented in the Personal Identity and Authentication information type. In many cases, premature and unauthorized disclosure can affect the integrity of the grants process, giving an unfair competitive advantage to one or more applicants. In such cases, punitive consequences and/or loss of public confidence can have a seriously disruptive effect on an agency's operations and mission. In such cases, the confidentiality impact level would be ***moderate***.

In some cases, federal grants information might be ***moderate*** to ***high*** impact. Also, details of programs for which grants are awarded may be sensitive (e.g., research grants for weapons systems project activities). Some federal grants information and some grant program details may be classified and outside the scope of this guideline.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for federal grants information is ***low***.

### Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. Federal grants activities are not generally time-critical and multiple individuals in multiple organizations are usually involved in the grants process. Therefore, the information maintained by all the individuals/agencies may be necessary to alter a grants decision. In most cases, the adverse effects of unauthorized modification or destruction of federal grants information on agency mission functions or public confidence in the agency is limited.

Special Factors Affecting Integrity Impact Determination: There are significant differences between the ability to modify a document authorizing a payment and the modification of the payment itself. The unauthorized modification of a document authorizing a payment is less time critical than the modification of the payment itself while the payment is in transit. Modifications to payments in transit will result in *immediate* inaccurate payments. This can result in assignment of a ***moderate*** impact level to such information.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for federal grants information is ***low***.

### Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to federal grants information. Federal grants processes are generally tolerant of delay. In most cases, disruption of access to federal grants information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The provisional availability impact level recommended for federal grants information is ***low***.

### D.23.2 Direct Transfers to Individuals Information Type

Direct Transfers to Individuals involves the disbursement of funds from the Federal Government directly to beneficiaries (individuals or organizations) who satisfy Federal eligibility requirements with no restrictions imposed on the recipient as to how the money is spent. Direct Transfers include both earned and unearned Federal Entitlement programs such as Medicare, Social Security, unemployment benefits, etc. The recommended provisional security categorization for the direct transfers to individuals information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of direct transfers to individuals information on the ability of responsible agencies to disburse funds from the Federal Government directly to beneficiaries (individuals or organizations) who satisfy Federal eligibility requirements with no restrictions imposed on the recipient as to how the money is spent. In the majority of cases, unauthorized disclosure of direct transfers to individuals will have only a limited adverse effect on agency operations, assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Many of the records associated with the disbursements may include information subject to privacy restrictions (e.g., the Privacy Act of 1974, HIPAA of 1996). (The Privacy Act Information provisional impact levels are documented in the Personal Identity and Authentication information type.) In such cases, punitive consequences and/or loss of public confidence can have a seriously disruptive effect on an agency's operations and mission. The consequent confidentiality impact level could be ***moderate***.

Recommended Confidentiality Impact Level: Therefore, the provisional confidentiality impact level recommended for direct transfers to individuals is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. Federal disbursement activities are not generally time-critical. In most cases, the monetary amounts involved are not large (on a governmental budgetary scale). Also, the adverse effects of unauthorized modification or destruction of direct transfers to individuals on agency mission functions or public confidence in the agency will be limited.

Special Factors Affecting Integrity Impact Determination: There are significant differences between the ability to modify a document authorizing a payment and the modification of the payment itself. The unauthorized modification of a document authorizing a payment is less time critical than the modification of the payment itself while the payment is in transit. Modifications to payments in transit will result in *immediate* inaccurate payments. This can result in assignment of a ***moderate*** impact level to such information.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for direct transfers to individuals is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to direct transfers to individuals information. Federal disbursement processes are generally tolerant of delay. In most cases, disruption of access to information regarding direct transfers to individuals can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Availability Impact Determination: Disruption of disbursements to large populations can do serious harm to public confidence in the agency and have a harmful impact on the nation's economy (e.g., affect consumer confidents and retail sales for a month or quarter). In such cases, the availability impact would be ***moderate***.

Recommended Availability Impact Level: The provisional availability impact level recommended for direct transfers to individuals is ***low***.

### D.23.3 Subsidies Information Type

Subsidies involve Federal Government financial transfers that reduce costs and/or increase revenues of producers. Subsidies include the payment of funds from the government to affect the production or prices of various goods to benefit the public. The recommended provisional security categorization for the subsidies information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of subsidies information on the ability of responsible agencies to pay government funds to affect the production or prices of various goods to benefit the public benefit. In many cases, unauthorized disclosure of subsidies information will have only a limited adverse effect on agency operations, assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Some information associated with applications for subsidies includes information covered by the provisions of the Privacy Act of 1974. (The Privacy Act Information provisional impact levels are documented in the Personal Identity and Authentication information type.) Unauthorized disclosure of large volumes of information protected under the Privacy Act can be expected to have a serious effect on public confidence in the agency. Also, premature unauthorized disclosure of planned subsidies policies can affect financial/commodities markets, with associated potential adverse effects on the U.S. economy and serious adverse effects on public confidence in the agency. This can result in assignment of a ***moderate*** impact level to such information.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for most subsidies information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. Subsidies activities are not typically time-critical. In most cases, the adverse effects of unauthorized modification or destruction of subsidies information on agency mission functions, image or public confidence in the agency will be limited.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for subsidies information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to subsidies information. Subsidies processes are generally tolerant of delay. In most cases, disruption of access to subsidies information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The provisional availability impact level recommended for subsidies information is ***low***.

### D.23.4 Tax Credits Information Type

Tax Credits allow a special exclusion, exemption, or deduction from gross income or which provide a special credit, a preferential rate of tax, or a deferral of tax liability designed to encourage certain kinds of activities or to aid taxpayers in special circumstances. The recommended provisional security categorization for the tax credits information type is as follows:

Security Category = {(confidentiality, Moderate), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of tax credit information on the ability of responsible agencies to allow special exclusions, exemptions, or deductions from gross income or which provide special credits, a preferential rate of tax, or a deferral of tax liability designed to encourage certain kinds of activities or to aid taxpayers in special circumstances. Many of the records associated with disbursements may include information subject to privacy restrictions (e.g., the Privacy Act of 1974, the Internal Revenue Code and Manual, or the Economic Espionage Act). (The provisional impact levels for personnel information are documented in the Personal Identity and Authentication, Income, Representative Payee, and Entitlement Event information types.) In such cases, punitive consequences and/or loss of public confidence can have a seriously disruptive effect on an agency's operations and mission. In many cases, unauthorized disclosure of tax credit information can have a serious adverse effect on agency operations, assets, or individuals.

Recommended Availability Impact Level: The provisional confidentiality impact level recommended for tax credit information is ***moderate***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information.  Tax credits are not generally time-critical.  In most cases, the adverse effects of unauthorized modification or destruction of tax credits on agency mission functions or public confidence in the agency will be limited.

Recommended Integrity Impact Level:  The provisional integrity impact level recommended for tax credits is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to tax credits information. Taxation processes are generally tolerant of delay. In most cases, disruption of access to tax credit information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level:  The provisional availability impact level recommended for tax credit information is ***low***.

## D.24  Credit and Insurance

Credit and Insurance involves the use of government funds to cover the subsidy cost of a direct loan or loan guarantee or to protect/indemnify members of the public from financial losses.

### D.24.1  Direct Loans Information Type

Direct loans involve a disbursement of funds by the Government to a non-Federal borrower under a contract that requires the repayment of such funds with or without interest. The recommended provisional security categorization for the direct loan information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of direct loan information on the ability of responsible agencies to disburse Federal funds to non-Federal borrowers under contract terms that require the repayment of such funds with or without interest. Much direct loan information includes information covered by the provisions of the Privacy Act of 1974.  (The Privacy Act Information provisional impact levels are documented in the Personal Identity and Authentication information type.)  In most cases, unauthorized disclosure of direct loan information will have only a limited adverse effect on agency operations, assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Unauthorized disclosure of large volumes of information protected under the Privacy Act can be expected to have a serious to severe effect on public confidence in the agency.  In such cases, the confidentiality impact can be ***moderate***.

Recommended Confidentiality Impact Level:  The provisional confidentiality impact level recommended for direct loan information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information.  Loan assistance activities are not generally time-critical.  In most cases, the adverse effects of unauthorized modification or destruction of direct loan information on agency mission functions and public confidence in the agency will be limited.

Special Factors Affecting Integrity Impact Determination: There are significant differences between the ability to modify a document authorizing a payment and the modification of the payment itself.  The unauthorized modification of a document authorizing a payment is less time critical than the modification of the payment itself while the payment is in transit.  Modifications to payments in transit will result in *immediate* inaccurate payments. This can result in assignment of a ***moderate*** impact level to such information.

Recommended Integrity Impact Level:  The provisional integrity impact level recommended for direct loan information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to direct loan information. Loan assistance processes are generally tolerant of delay.  In most cases, disruption of access to direct loan information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level:  The provisional availability impact level recommended for direct loan information is ***low***.

### D.24.2  Loan Guarantees Information Type

Loan guarantees involve any guarantee, insurance, or other pledge with respect to the payment of all or a part of the principal or interest on any debt obligation of a non-Federal borrower to a non-Federal lender, but does not include the insurance of deposits, shares, or other withdrawable accounts in financial institutions.  The general recommended security categorization for the loan guarantees information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of loan guarantee information on the ability of responsible agencies to execute guarantees, insurance, or other pledges with respect to the payment of all or a part of the principal or interest on any debt obligation of a non-Federal borrower to a non-Federal lender. In most cases, unauthorized disclosure of loan guarantee information will have only a limited adverse effect on agency operations, assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Much loan guarantee information includes information covered by the provisions of the Privacy Act of 1974. (The Privacy Act Information provisional impact levels are documented in the Personal Identity and Authentication information type.) Unauthorized disclosure of large volumes of information protected under the Privacy Act can be expected to have a serious to severe effect on public confidence in the agency. In such cases, the confidentiality impact can be ***moderate.***

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for loan guarantee information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. Loan guarantee activities are not generally time-critical. In most cases, the adverse effects of unauthorized modification or destruction of loan guarantee information on agency mission functions and public confidence in the agency will be limited.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for loan guarantee information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to loan guarantee information. Loan processes are generally tolerant of delay. In most cases, disruption of access to loan guarantee information will have only a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Availability Impact Determination: The provisional availability impact level recommended for loan guarantee information is ***low***.

### D.24.3 General Insurance Information Type

General Insurance involves providing protection to individuals or entities against specified risks. The specified protection generally involves risks that private sector entities are unable or unwilling to assume or subsidize and where the provision of insurance is necessary to achieve social objectives. The following provisional security categorization is recommended for the general insurance information type:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

### Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of general insurance information on the abilities of responsible agencies to provide protection to individuals or entities against specified risks. General insurance activities include both insurance issuing and insurance servicing. Insurance issuing is any activity such as provider approval, underwriting, and endorsements. The consequences of unauthorized disclosure of insurance issuing information will generally result in a limited adverse effect on agency operations, agency assets, or individuals.

Insurance servicing supports activities associated with administering and processing insurance include payment processing, initial and final closings, loss mitigation, claims management, and retiring insurance. The confidentiality impact level is the effect of unauthorized disclosure of insurance servicing information on the abilities of responsible agencies to administer and process insurance. The consequences of unauthorized disclosure of insurance servicing information will generally result in a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: The more serious consequences may result from 1) unauthorized disclosure of provider's proprietary information, or 2) premature disclosure of agency plans or changes under consideration for contracts, plans, or policies. Unauthorized disclosure of information that can affect contract arrangements to the detriment of the interests of the government, and of the public at large (e.g., planned or anticipated termination of a major contract insurer), can result in damaging increases in public expense and exposure to impact. In the case of unauthorized disclosure to an individual private sector organization, unfair competitive advantage may result – with major financial consequences. In the case of unauthorized disclosure of preliminary and unsubstantiated data that is both incorrect and pessimistic (e.g., Medicare budget projections,), the consequent unwarranted alarm of the public may have serious political and operational consequences for affected agencies. In the more serious cases, the confidentiality impact will be at least ***moderate***.

The more serious consequences of unauthorized disclosure of insurance servicing information may result from unauthorized disclosure of private information concerning the insured (e.g., Privacy Act information). (The Privacy Act Information provisional impact levels are documented in the Personal Identity and Authentication information type.) In the more serious cases, the confidentiality impact will be at least ***moderate***.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for general insurance information is ***low***.

### Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of general insurance information may depend on the urgency with which the information is typically needed. Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) typically has a limited adverse effect on agency operations and/or public confidence in the agency.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for general insurance information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to general insurance information. The nature of general insurance processes is usually tolerant of reasonable delays.

Special Factors Affecting Availability Impact Determination: Extensive delays in insurance servicing activities can result in financial harm for individuals and businesses and in public alarm and repercussions in the financial markets. In more serious cases, delays may have serious political and operational consequences for affected agencies. In such cases, the confidentiality impact may be at least ***moderate***.

Recommended Availability Impact Level: The provisional availability impact level recommended for general insurance information is ***low***.

## D.25 Transfers to State/Local Governments

Transfers to States and Local Governments involve the transfer of funds or financial assistance from the Federal government to State and Local governments and Indian tribes.

### D.25.1 Formula Grants Information Type

Formula Grants involves the allocation of money to States or their subdivisions in accordance with distribution formulas prescribed by law or administrative regulation, for activities of a continuing nature. The recommended provisional security categorization for the formula grants information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of formula grants information on the ability of responsible agencies to allocate money to States or their subdivisions in accordance with distribution formulas prescribed by law or administrative regulation, for activities of a continuing nature. Typically, unauthorized disclosure of most formula grants information will have only a limited adverse effect on agency operations, assets, or individuals. In most cases, information associated with formula grants is public knowledge.

Special Factors Affecting Confidentiality Impact Determination: In a few cases, details of programs for which formula grants are awarded may be sensitive (e.g., some Federal/State cooperative programs intended to support Homeland Security operations). This can result in assignment of a ***moderate*** or ***high*** impact level to such information. Some formula grants information might be classified (hence outside the scope of this guideline).

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for formula grants information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. Formula grants activities are not generally time-critical and multiple individuals in multiple organizations are usually involved in the grants process. Therefore, the information maintained by all the individuals/agencies is probably necessary to alter a grants decision. In most cases, the adverse effects of unauthorized modification or destruction of formula grants information on agency mission functions or public confidence in the agency will be limited.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for formula grants information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to formula grants information. Formula grants processes are generally tolerant of delay. In most cases, disruption of access to formula grants information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The provisional availability impact level recommended for formula grants information is ***low***.

### D.25.2 Project/Competitive Grants Information Type

Project/Competitive Grants involves the funding, for fixed or known periods, of projects. Project/Competitive grants can include fellowships, scholarships, research grants, training grants, traineeships, experimental and demonstration grants, evaluation grants, planning grants, technical assistance grants, survey grants, and construction grants. The general recommended security categorization for the project/competitive grants information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of project/competitive grants information on the ability of responsible agencies to award fellowships, scholarships, research grants, training grants, traineeships, experimental and demonstration grants, evaluation grants, planning grants, technical assistance grants, survey grants, and/or construction grants. In most cases, unauthorized disclosure of project/competitive grants information will have only a limited adverse effect on agency operations, assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: In some cases, project/competitive grants information may be sensitive with ***moderate*** to ***high*** impact. In a few cases, details of programs for which grants are awarded may be classified and outside the scope of this guideline.

In a few cases, records associated with the grants may include information subject to privacy restrictions (e.g., the Privacy Act of 1974). (The Privacy Act Information provisional impact levels are documented in the Personal Identity and Authentication information type.) In many cases, premature and unauthorized disclosure can affect the integrity of the grants process, giving an unfair competitive advantage to one or more applicants. In such cases, punitive consequences and/or loss of public confidence can have a seriously disruptive effect on an agency's operations and mission. In such cases, the confidentiality impact level would be ***moderate***.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for most project/competitive grants information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. Project/competitive grants activities are not generally time-critical. In most cases, the adverse effects of unauthorized modification or destruction of project/competitive grants information on agency mission functions or public confidence in the agency will be limited.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for project/competitive grants information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to project/competitive grants information. Project/competitive grants processes are generally tolerant of delay. In most cases, disruption of access to project/competitive grants information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The provisional availability impact level recommended for project/competitive grants information is ***low***.

### D.25.3 Earmarked Grants Information Type

Earmarked Grants involves the distribution of money to State and Local Governments for a named purpose or service usually specifically noted by Congress in appropriations language, or other program authorizing language. The recommended provisional security categorization for the earmarked grants information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of earmarked grants information on the ability of responsible Federal government entities to distribute money to State and Local Governments for a named purpose or service usually specifically noted by Congress in appropriations language, or other program authorizing language. In the majority of cases, earmarked grants information is public knowledge.  Typically, unauthorized disclosure of most earmarked grants information will have only a limited adverse effect on agency operations, assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination:  In some cases, project/competitive grants information may be sensitive with ***moderate*** to ***high*** impact.  In a few cases, details of programs for which grants are awarded may be classified and outside the scope of this guideline.

Recommended Confidentiality Impact Level:  The provisional confidentiality impact level recommended for earmarked grants information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information.  Earmarked grants activities are not generally time-critical and multiple individuals in multiple organizations are usually involved in the grants process.  Therefore, the information maintained by all the individuals/agencies is probably necessary to alter a grants decision. In most cases, the adverse effects of unauthorized modification or destruction of earmarked grants information on agency mission functions or public confidence in the agency will be limited.

Recommended Integrity Impact Level:  The provisional integrity impact level recommended for earmarked grants information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to earmarked grants information.  Earmarked grants processes are generally tolerant of delay.  In most cases, disruption of access to earmarked grants information will have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The provisional availability impact level recommended for earmarked grants information is ***low***.

### D.25.4  State Loans Information Type

State Loans involve all disbursement of funds by the Government to a State or Local Government (or Indian Tribe) entity under a contract that requires the repayment of such funds with or without interest. The recommended provisional security categorization for the state loan information type is as follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of state loan information on the ability of responsible agencies to disburse Federal funds a State or Local Government (or Indian Tribe) entity under a contract that requires the repayment of such funds with or without interest.   In most cases, unauthorized disclosure of state loan information will have only a limited adverse effect on agency operations, assets, or individuals.

Recommended Confidentiality Impact Level:  The provisional confidentiality impact level recommended for state loan information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information.  Loan assistance activities are not generally time-critical.  In most cases, the adverse effects of unauthorized modification or destruction of state loan information on agency mission functions and public confidence in the agency will be limited.

Special Factors Affecting Integrity Impact Determination: There are significant differences between the ability to modify a document authorizing a payment and the modification of the payment itself.  The unauthorized modification of a document authorizing a payment is less time critical than the modification of the payment itself while the payment is in transit.  Modifications to payments in transit will result in *immediate* inaccurate payments.    This can result in assignment of a ***moderate*** impact level to such information.

Recommended Integrity Impact Level:  The provisional integrity impact level recommended for state loan information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to state loan information. Loan assistance processes are generally tolerant of delay.  In most cases, disruption of access to state loan information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level:  The provisional availability impact level recommended for state loan information is ***low***.

## D.26  Direct Services for Citizens

Direct Services for Citizens refers to the delivery of a good or service to (or on behalf of) the citizenry by the federal government with no other intervening persons, conditions, or organizations.

### D.26.1  Military Operations Information Type

The BRM provided in the *FEA Consolidated Reference Model Document, Version 2.3*, October 2007 does not define the Military Operations information type.  For the purpose of this document, Military Operations describes the direct provision of military service for the citizens. Further, the BRM specifies Military Operations as a Mode of Delivery business area or a vehicle by which the federal government delivers it services to citizens.  Therefore, agency personnel should consider the Military Operations information type as delivery mechanisms of the mission-based services information types [e.g., Catastrophic Defense, Emergency Response, Key Asset and Critical Infrastructure Protection] described heretofore.

### D.26.2 Civilian Operations Information Type

Civilian Operations describes the direct provision of a non-military service for the citizen by government employees.

The BRM provided in the *FEA Consolidated Reference Model Document, Version 2.3*, October 2007 specifies Civilian Operations as a Mode of Delivery business area or a vehicle by which the federal government delivers it services to citizens. Therefore, agency personnel should consider the Civilian Operations information type as delivery mechanisms of the mission-based services information types [e.g., Health Care, Emergency Response, and Environmental Remediation] described heretofore.

**[This Page Intentionally Left Blank]**

# APPENDIX E: LEGISLATIVE AND EXECUTIVE SOURCES ESTABLISHING SENSITIVITY/CRITICALITY

Some information has been established in law, by Executive Order, or by agency regulation as requiring protection from disclosure. Those information types that are national security information are outside the scope of this guideline. Each individual responsible for security categorization of an organization's information or information system should search his own department or agency's regulations for specific information protection requirements.

## E.1 Legislative Mandates

Some legislatively mandated prohibitions against disclosure of information (other than national security information) are identified in Table 6. The table gives the title or subject of the section in the United States Code (U.S.C.) in which the prohibition occurs, the U.S.C. citation for the prohibition, and the Department, agency, or generic information type to which the law applies, and the legal source. Note that the information contained in the table is intended only as an aid and will not always be current. Independent law searches by analysts will generally be necessary.

**Table 6: Legal Information Disclosure Prohibitions**

| Subject/Title of Provision | United States Code Citation | Agency/Activity [Reference] |
|---|---|---|
| *Access to Information; Confidentiality* | 22 U.S.C., Chapter 46A, Section 3144 | Foreign Direct Investment in United States<br>[Foreign Direct Investment and International Financial Data Improvements Act of 1990, Public Law 101-533, Sec. 8, Nov. 7, 1990, 104 Stat. 2350] |
| *Access to Records* | 42 U.S.C., Chapter 114, Subchapter I, Part A, Section 10806 | Department of Health and Human Services/Public Health Service<br>[Public Law 99-319, Title I, Sec. 106, May 23, 1986, 100 Stat. 481; Public Law 100-509, Sec. 6(b), Oct. 20, 1988, 102 Stat. 2544; and Public Law 102-173, Sec. 10(2), Nov. 27, 1991, 105 Stat. 1219.] |
| *Administrative Enforcement; Preliminary Matters* | 42 U.S.C., Chapter 45, Subchapter I, Section 3610 | Housing and Urban Development<br>[Public Law 90-284, title VIII, Sec. 810, as added Public Law 100-430, Sec. 8(2), Sept. 13, 1988, 102 Stat. 1625] |
| *Administrative Simplification* | 42 U.S.C., Chapter 7, Subchapter XIX, Part C | [Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191] |

## Table 6: Legal Information Disclosure Prohibitions

| Subject/Title of Provision | United States Code Citation | Agency/Activity [Reference] |
|---|---|---|
| *Administrative Subpoenas* | 18 U.S.C., Part II, Chapter 223, Section 3486(a)(6) | Health Care Investigations/Law Enforcement/Courts<br>[HIPAA, Public Law 104-191, Title II, Sec. 248(a), Aug. 21, 1996, 110 Stat. 2018] |
| *Application of Other Laws* | 39 U.S.C., Part I, Chapter 4, Section 410(c) | US Postal Service<br>[Postal Reorganization Act, Public Law 91-375, Aug. 12, 1970, 84 Stat. 725 amended by the Federal Pay Comparability Act of 1970, Public Law 91-656, Sec. 8(a), Jan. 8, 1971, 84 Stat. 1955] |
| *Approval of Retail Food Stores and Wholesale Food Concerns* | 7 U.S.C., Chapter 51, Section 2018(c) | Department of Agriculture Food Stamps<br>[Food Security Act of 1985, Public Law 99-198, Title XV, Sec. 1521, 1532(b), Dec. 23, 1985, 99 Stat. 1579, 1583; amended by the Food Stamp Program Improvements Act of 1994, Public Law 103-225, Title II, Sec. 202, 203, Mar. 25, 1994, 108 Stat. 108; Better Nutrition and Health for Children Act of 1994, Public Law 103-448, Title II, Sec. 204(w)(2)(A), Nov. 2, 1994, 108 Stat. 4746; and Public Law 104-193, Title VIII, Sec. 831-834, Aug. 22, 1996, 110 Stat. 2328] |
| *Assessment Procedures* | 7 U.S.C., Chapter 80, Section 4908 | Department of Agriculture<br>[Food Security Act of 1985, Public Law 99-198, Title XVI, Sec. 1649, Dec. 23, 1985, 99 Stat. 1626] |
| *Assessments (Confidential Nature)* | 7 U.S.C., Chapter 58, Section 2619(c) | Department of Agriculture/<br>*National Potato Promotion Board*<br>[Potato Research and Promotion Act, Public Law 91-670, Title III, Sec. 310, Jan. 11, 1971, 84 Stat. 2044; amended by Public Law 101-624, Title XIX, Sec. 1942, Nov. 28, 1990, 104 Stat. 3867] |

## Table 6: Legal Information Disclosure Prohibitions

| Subject/Title of Provision | United States Code Citation | Agency/Activity [Reference] |
|---|---|---|
| *Authorization for Disclosure and Use of Intercepted Wire, Oral, or Electronic Communications* | 18 U.S.C., Part I, Chapter 119, Section 2517(6) | Law Enforcement<br>[Omnibus Crime Control and Safe Streets Act of 1968, Public Law 90-351, Title III, Sec. 802, June 19, 1968, 82 Stat. 217; amended by the Organized Crime Control Act of 1970, Public Law 91-452, Title IX, Sec. 902(b), Oct. 15, 1970, 84 Stat. 947; Electronic Communications Privacy Act of 1986, Public Law 99-508, Title I, Sec. 101(c)(1)(A), Oct. 21, 1986, 100 Stat. 1851; and the USA Patriot Act, Public Law 107-56, Title II, Sec. 203(b)(1), Oct. 26, 2001, 115 Stat. 280] |
| *Blood Donor Locator Service* | 42 U.S.C., Chapter 7, Subchapter XI, Part A, Section 1320b-11 | Social Security Administration<br>[Social Security Act of Aug. 14, 1935, Ch. 531, Title XI, Sec. 1141, as added to by Public Law 100-647, Title VIII, Sec. 8008(b)(1), Nov. 10, 1988, 102 Stat. 3784; and amended by Public Law 103-296, Title I, Sec. 108(b)(13), Aug. 15, 1994, 108 Stat. 1484] |
| *Books and Records* | 7 U.S.C., Chapter 26, Subchapter III, Section 608d | Department of Agriculture<br>[Agricultural Adjustment Act, May 12, 1933, C h. 25, Title I, Sec. 8d, as added to by the Miller Act of Aug. 24, 1935, Ch. 641, Sec. 6, 49 Stat. 761; and amended by the Agricultural Marketing Agreement Act of 1937, June 3, 1937, Ch. 296, Sec. 1, 50 Stat. 246; the Food Security Act of 1985 Public Law 99-198, Title XVI, Sec. 1663, Dec. 23, 1985, 99 Stat. 1631; and the Livestock Mandatory Reporting Act of 1999, Public Law 106-78, Title VII, Sec. 757(b), Oct. 22, 1999, 113 Stat. 1171] |
| *Bureau of Transportation Statistics – Prohibition of Certain Disclosures* | 49 U.S.C., Subtitle I, Chapter 1, Section 111(i) | Bureau of Transportation Statistics/Department of Transportation<br>[Public Law 102-240, Title VI, Sec. 6006(a), Dec. 18, 1991, 105 Stat. 2172; amended by the Transportation Equity Act for the 21st Century, Public Law 105-178, Title V, Sec. 5109(a), June 9, 1998, 112 Stat. 437] |

## Table 6: Legal Information Disclosure Prohibitions

| Subject/Title of Provision | United States Code Citation | Agency/Activity [Reference] |
|---|---|---|
| *Chronic Hazard Advisory Panels – Information Disclosure* | 15 U.S.C., Chapter 47, Section 2077(g) and (h) | Consumer Product Safety Commission<br>[Consumer Product Safety Act of 1972, Public Law 92-573, Sec. 28, as added to by Public Law 97-35, Title XII, Sec. 1206(a), Aug. 13, 1981, 95 Stat. 716] |
| *Civil Damages for Unauthorized Inspection or Disclosure of Returns and Return Information* | 26 U.S.C., Subtitle F, Chapter 76, Subchapter B, Section 7431 | Treasury Department/ Internal Revenue Service<br>[Tax Equity and Fiscal Responsibility Act of 1982, Public Law 97-248, Title III, Sec. 357(a), Sept. 3, 1982, 96 Stat. 645; amended by the Interest and Dividend Tax Compliance Act of 1983, Public Law 98-67, Title I, Sec. 104(b), Aug. 5, 1983, 97 Stat. 379; Taxpayer Relief Act of 1997, Public Law 105-34, Title XII, Sec. 1205(c)(2), Aug. 5, 1997, 111 Stat. 998; Taxpayer Browsing Protection Act of 1997, Public Law 105-35, Sec. 3(a)-(d)(4), (6), Aug. 5, 1997, 111 Stat. 1105, 1106; and the Taxpayer Bill of Rights 3, Public Law 105-206, Title III, Sec. 3101(f), Title VI, Sec. 6012(b)(3), July 22, 1998, 112 Stat. 729, 819] |
| *Collection of Assessments; Refunds Confidentiality of Information; Disclosures* | 7 U.S.C., Chapter 77, Section 4608 (f)(3) and (g) | Department of Agriculture/ Honey Board<br>[Agricultural Research, Extension, and Education Reauthorization Act of 1998, Public Law 105-185, Title VI, Sec. 605(h), June 23, 1998, 112 Stat. 597] |
| *Confidential Information* | 12 U.S.C., Chapter 6A, Subchapter I, Section 635i-3(g)(3) | Treasury Department/ Bank of the Tied Aid Credit Fund<br>[Export- Import Bank Act of 1945, July 31, 1945, Ch. 341, Sec. 10, formerly Sec. 15, as added to by the Export-Import Bank Act Amendments of 1986, Public Law 99-472, Sec. 19, Oct. 15, 1986, 100 Stat. 1205] |
| *Confidential Information* | 15 U.S.C., Chapter 16C, Section 796 | Department of Commerce/ Federal Energy Administration<br>[Energy Supply and Environmental Coordination Act, Public Law 93-319, Sec. 11, June 22, 1974, 88 Stat. 262] |

## Table 6: Legal Information Disclosure Prohibitions

| Subject/Title of Provision | United States Code Citation | Agency/Activity [Reference] |
|---|---|---|
| *Confidential Information* | 19 U.S.C., Chapter 14, Section 2605(i) | Treasury Department/ Cultural Property Advisory Committee [Convention on Cultural Property Implementation Act, Public Law 97-446, Title III, Sec. 306, Jan. 12, 1983, 96 Stat. 2356] |
| *Confidential Information* | 21 U.S.C., Chapter 9, Subchapter VII, Part A, Section 379 | Department of Health and Human Services<br>[Fair Labor Standards Act, June 25, 1938, Ch. 675, Sec. 708, as added to by Medical Device Amendments, Public Law 94-295, Sec. 8, May 28, 1976, 90 Stat. 582] |
| *Confidential Information* | 25 U.S.C., Chapter 29, Section 2716(a) | Department of Justice/ Department of the Interior/ Bureau of Indian Affairs/ National Indian Gaming Commission<br>[Indian Gaming Regulatory Act, Public Law 100-497, Sec. 17, Oct. 17, 1988, 102 Stat. 2484] |
| *Confidential Information* | 30 U.S.C., Chapter 25, Subchapter V, Section 1262(b) | Environmental Protection Agency<br>[Surface Mining Control and Reclamation Act, Public Law 95-87, Title V, Sec. 512, Aug. 3, 1977, 91 Stat. 483] |
| *Confidential Information* | 42 U.S.C., Chapter 99, Section 9122(b) | Department of Commerce/ National Oceanic and Atmospheric Administration<br>[Ocean Thermal Energy Conversion Act of 1980, Public Law 96-320, Title I, Sec. 112, Aug. 3, 1980, 94 Stat. 989; as amended by the National Fishing Enhancement Act of 1984, Public Law 98-623, Title VI, Sec. 602(e)(3), (18), Nov. 8, 1984, 98 Stat. 3412] |
| *Confidential Information; Circumstances Permitting Disclosure* | 42 U.S.C., Chapter 23, Division A, Subchapter XII, Section 2181(e) | Department of Energy/ Department of Commerce/ Patent Office<br>[Public Law 87-206, Sec. 9] |
| *Confidential Information; Disclosure* | 42 U.S.C., Chapter 65, Section 4912(b) | Environmental Protection Agency<br>[Federal Noise Control Act, Public Law 92-574, Sec. 13, Oct. 27, 1972, 86 Stat. 1244] |
| *Confidential Information; Disclosure Prohibited* | 12 U.S.C., Chapter 7A, Section 1141j(c) | Treasury Department/ Farm Credit Administration<br>[Agricultural Marketing Act, June 15, 1929, Ch. 24, Sec. 15, 46 Stat. 18] |

## Table 6: Legal Information Disclosure Prohibitions

| Subject/Title of Provision | United States Code Citation | Agency/Activity [Reference] |
|---|---|---|
| *Confidential Information; Trade Secrets and Secret Processes; Information Disclosure* | 42 U.S.C., Chapter 6A, Subchapter XII, Part E, Section 300j-4(d)(1) | Environmental Protection Agency [Safety of Public Water Systems, July 1, 1944, Ch. 373, Title XIV, Sec. 1445] |
| *Confidential Nature (Forms for registration and fingerprinting)* | 8 U.S.C., Chapter 12, Subchapter II, Part VII, Section 1304(b) | Department of Justice/ Department of State/ Department of Homeland Security<br>[Immigration and Nationality Act of June 27, 1952, Ch. 477, Title II, Ch. 7, Sec. 264, 66 Stat. 224] |
| *Confidential Nature of Claims* | 38 U.S.C., Part IV, Chapter 57, Subchapter I, Section 5701 (Renamed from Section 3301 by Public Law 102-40, Title IV, Sec. 402(c)(1), May 7, 1991, 105 Stat. 239) | Veterans Administration<br>[Title 38 "Veterans Benefits" (Social Security Act §§202 and 217), Pub. L. 85-857, Sept. 2, 1958, 72 Stat. 1236, Sec. 3301; amended by Public Law 87-671, Sec. 2, Sept. 19, 1962, 76 Stat. 557; Public Law 91-24, Sec. 11, June 11, 1969, 83 Stat. 34; Vietnam Era Veterans Readjustment Act of 1972, Public Law 92-540, Title IV, Sec. 412, Oct. 24, 1972, 86 Stat. 1093; Public Law 94-321, Sec. 1(a), June 29, 1976, 90 Stat. 713; Public Law 94-581, Title II, Sec. 210(b), Oct. 21, 1976, 90 Stat. 2863; Veterans Rehabilitation and Education Amendments of 1980, Public Law 96-466, Title VI, Sec. 606, Oct. 17, 1980, 94 Stat. 2212; Court of Veterans Appeals Judges Retirement Act, and Public Law 101-94, Title III, Sec. 302(a), Aug. 16, 1989, 103 Stat. 628; renumbered Sec. 5701 and amended by Public Law 102-40, Title IV, Sec. 402(b)(1), (d)(1), May 7, 1991, 105 Stat. 238, 239; and amended by Public Law 102-83, Sec. 2(c)(6), 4(a)(1), (2)(A)(xi), (3), (4), (b)(1), (2)(E), 5(c)(1), Aug. 6, 1991, 105 Stat. 402-406] |
| *Confidential Nature of Information Furnished Bureau* | 15 U.S.C., Chapter 5, Section 176a | Department of Commerce/ Bureau of Foreign and Domestic Commerce<br>[The Postal Act of 1938, Jan. 27, 1938, Ch. 11, Sec. 1, 52 Stat. 8] |

## Table 6: Legal Information Disclosure Prohibitions

| Subject/Title of Provision | United States Code Citation | Agency/Activity [Reference] |
|---|---|---|
| *Confidential Nature of Records (Visas)* | 8 U.S.C., Chapter 12, Subchapter II, Part III, Section 1202(f) | Department of State/ Depart-ment of Homeland Security<br>[Immigration and Nationality Act of June 27, 1952, Ch. 477, Title II, Ch. 7, Sec. 264, 66 Stat. 224] |
| *Confidential or Privileged Information in an Action Described in 28 U.S.C. Sec. 1581(c)* | Title IX, Rule 71, (c) | Department of Commerce/ International Trade Commission/ Judiciary<br>[Jurisdiction: Tariff Act of 1930] |
| *Confidential or Privileged Material* | 19 U.S.C., Chapter 4, Subchapter III, Part III, Section 1516a(b)(2)(B) | Department of Homeland Security/ Treasury Department/ Customs Service<br>[Tariff Act of 1930, June 17, 1930, Ch. 497, Title IV, Sec. 516A, as added to by the Trade Agreements Act of 1979, Public Law 96-39, Title X, Sec. 1001(a), July 26, 1979, 93 Stat. 300] |
| *Confidential Records and Information* | 7 U.S.C., Chapter 6, Subchapter II, Section 136e(d) | Environmental Protection Agency<br>[Federal Insecticide, Fungicide and Rodenticide Act, Public Law 95-396, Sec. 13, Sept. 30, 1978, 92 Stat. 829] |
| *Confidential Reports and Other Additional Requirements* | Title I, Section 107 | Departments and Agencies/Inspectors General |
| *Confidential Status of Application* | 7 U.S.C., Chapter 57, Subchapter II, Part E, Section 2426 | Department of Agriculture/ Plant Variety Protection Office<br>[Plant Variety Protection Act, Public Law 91-577, Title II, Sec. 56, Dec. 24, 1970, 84 Stat. 1549 amended by Public Law 96-574, Sec. 12, Dec. 22, 1980, 94 Stat. 3350] |
| *Confidential Status of Applications; Publication of Patent Applications* | 35 U.S.C., Part II, Chapter 11, Section 122 | Department of Commerce/ Patent Office<br>[1952 Patent Act, July 19, 1952, Ch. 950, 66 Stat. 801; amended by Public Law 93-596, Sec. 1, Jan. 2, 1975, 88 Stat. 1949, and the *Inventors' Rights Act of 1999,* Public Law 106-113, Div. B, Sec. 1000(a)(9) (Title IV, Sec. 4502(a)), Nov. 29, 1999, 113 Stat. 1536, 1501A-561] |

## Table 6: Legal Information Disclosure Prohibitions

| Subject/Title of Provision | United States Code Citation | Agency/Activity [Reference] |
|---|---|---|
| *Confidentiality* | 15 U.S.C., Chapter 2, Subchapter I,<br>Section 57b-2 | Department of Commerce/ Federal Trade Commission<br>[The Federal Trade Commission Act, Sept. 26, 1914, Ch. 311, Sec. 21, as added to by the Federal Trade Commission Improvements Act of 1979, Public Law 96-252, Sec. 14, May 28, 1980, 94 Stat. 385; and amended by the Federal Trade Commission Act Amendments of 1994, Public Law 103-312, Sec. 8, Aug. 26, 1994, 108 Stat. 1694] |
| *Confidentiality* | 20 U.S.C., Chapter 71, Section 9007 | Department of Education<br>[Safe and Drug-Free Schools and Communities Act of 1994, Public Law 103-382, Title IV, Sec. 408, Oct. 20, 1994, 108 Stat. 4034] |
| *Confidentiality and Informed Consent* | 42 U.S.C., Chapter 6A, Subchapter XXIV, Section 300ff-61 | Health and Human Services/Public Health Service/Medical<br>[Ryan White Comprehensive AIDS Resources Emergency Act of 1990, Public Law 101-381, Title III, Sec. 301(a), Aug. 18, 1990, 104 Stat. 609] |
| *Confidentiality of Abused Person's Address* | 42 U.S.C., Chapter 136, Subchapter III, Part B, Subpart 1, Section 13951 | US Postal Service<br>[Public Law 103-322, Title IV, Sec. 40281, Sept. 13, 1994, 108 Stat. 1938] |
| *Confidentiality of Certain Medical Records,* | 38 U.S.C., Part V,<br>Chapter 73, Subchapter III, Section 7332<br>(Renumbered by Public Law 102-40 from Section 44132) | Veterans Administration<br>[Public Law 94-581, Title I, Sec. 111(a)(1), Oct. 21, 1976, 90 Stat. 2849, Sec. 4132; amended by Public Law 100-322, Title I, Sec. 121, May 20, 1988, 102 Stat. 502; renumbered Sec. 7332 and amended by Public Law 102-40, Title IV, Sec. 401(a)(4)(A), 402(d)(1), 403(a)(1), (2), (4), (5), May 7, 1991, 105 Stat. 221, 239] |
| *Confidentiality of Financial Records* | 12 U.S.C., Chapter 35, Section 3403 | Financial Data<br>[Right to Financial Privacy Act of 1978, Public Law 95-630, Title XI, Sec. 1103, Nov. 10, 1978, 92 Stat. 3698; amended by Public Law 99-570, Title I, |
|  |  | Sec. 1353(a), Oct. 27, 1986, 100 Stat. 3207-21; and Public Law 100-690, Title VI, Sec. 6186(a), Nov. 18, 1988, 102 Stat. 4357] |

## Table 6: Legal Information Disclosure Prohibitions

| Subject/Title of Provision | United States Code Citation | Agency/Activity [Reference] |
|---|---|---|
| *Confidentiality of Information* | 7 U.S.C., Chapter 55, Section 2276 | Department of Agriculture<br>[Food Security Act of 1985, Public Law 99-198, Title XVII, Sec. 1770, Dec. 23, 1985, 99 Stat. 1657; Public Law 105-113, Sec. 4(a)(2), (b), Nov. 21, 1997, 111 Stat. 2276; Public Law 106-113, Div. B, Sec. 1000(a)(3) (Title III, Sec. 348), Nov. 29, 1999, 113 Stat. 1535, 1501A-207] |
| *Confidentiality of Information* | 18 U.S.C., Part II, Chapter 223, Section 3509(d)(1) | Criminal Procedure: Child Victims & Child Witnesses Rights<br>[Crime Control Act of 1990, Public Law 101-647, Title II, Sec. 225(a), Nov. 29, 1990, 104 Stat. 4798; amended by Public Law 103-322, Title XXXIII, Sec. 330010(6), (7), 330011(e), 330018(b), Sept. 13, 1994, 108 Stat. 2143, 2145, 2149] |
| *Confidentiality of Information* | 22 U.S.C., Chapter 75, Section 6744 | State Department<br>[Chemical Weapons Convention Implementation Act of 1998, Public Law 105-277, Div. I, Title IV, Sec. 404, Oct. 21, 1998, 112 Stat. 2681-882] |
| *Confidentiality of Medical Quality Assurance Records* | 38 U.S.C., Part IV,<br>Chapter 57, Subchapter I, Section 5705<br>(Renumbered by Public Law 102-40 from Section 3305) | Department of Veterans Affairs<br>[Veterans' Disability Compensation and Housing Benefits Amendments of 1980, Public Law 96-385, Title V, Sec. 505(a), Oct. 7, 1980, 94 Stat. 1535, Sec. 3305; amended by Veterans' Administration Health-Care Amendments of 1985, Public Law 99-166, title II, Sec. 201, Dec. 3, 1985, 99 Stat. 949; amended and renumbered by Department of Veterans Affairs Physicians' and Dentists' |
| | | Compensation and Labor-Relations Act of 1991, Public Law 102-40, Title IV, Sec. 402(b)(1), 403(b)(2), May 7, 1991, 105 Stat. 238, 239; amended by the Veterans Loans bill, Public Law 102-54, Sec. 14(d)(4), June 13, 1991, 105 Stat. 285 and the Department of Veterans Affairs Codification Act, Public Law 102-83, Sec. 4(a)(2)(F), (3), (4), (b)(1), (2)(E), Aug. 6, 1991, 105 Stat. 404, 405] |

## Table 6: Legal Information Disclosure Prohibitions

| Subject/Title of Provision | United States Code Citation | Agency/Activity [Reference] |
|---|---|---|
| *Confidentiality of Medical Quality Assurance Records: Qualified Immunity for Participants* | 10 U.S.C., Subtitle A, Part II, Chapter 55, Section 1102 | Department of Defense [National Defense Authorization Act for Fiscal Year 1987, Public Law 99-661, Div. A, Title VII, Sec. 705(a)((1)), Nov. 14, 1986, 100 Stat. 3902] |
| *Confidentiality of Records* | 42 U.S.C., Chapter 6A, Subchapter III-A, Part D, Section 290dd-2 | Public Health Service [ADAMHA Reorganization Act, Public Law 102-321] |
| *Counterintelligence Access to Telephone Toll and Transactional Records* | 18 U.S.C., Part I, Chapter 121, Section 2709 | Department of Justice/ Federal Bureau of Investigation/Communication Service Providers [Communications Assistance for Law Enforcement Act, Public Law 99-508, Title II, Sec. 201((a)), Oct. 21, 1986, 100 Stat. 1867] |
| *Critical Infrastructure Information* | 6 U.S.C., Chapter 1 | Department of Homeland Security [Critical Infrastructure Information Protection Act of 2002, Public Law 107-296, Title II, Subtitle B, Sec. 211-215] |
| *Crop Insurance - Purpose; Definitions; Protection of Information; Relation to Other Laws* | 7 U.S.C., Chapter 36, Section 1502 | Department of Agriculture [Agriculture Risk Protection Act of 2000, Public Law 106-224, Title I, Sec. 122, 141, June 20, 2000, 114 Stat. 377, 389] |
| *Cultural Property Advisory Committee* | 19 U.S.C., Chapter 14, Section 2605 | Treasury Department/ Department of Homeland Security [Convention on Cultural Property Implementation Act, Public Law 97-446, Title III, Sec. 306, Jan. 12, 1983, 96 Stat. 2356] |
| *Data Collection Authority of President* | 10 U.S.C., Subtitle A, Part IV, Chapter 148, Subchapter II, Section 2507 | Department of Defense/ National Defense Technology and Industrial Base Council [Defense Conversion, Reinvestment, and Transition Assistance Act of 1992, PublicLaw 102-484, Div. D, Title XLII, Sec. 4217, Oct. 23, 1992, 106 Stat. 2670; amended by Defense Conversion, Reinvestment and Transition Assistance Amendments of 1993, Public Law 103-160, Div. A, Title XI, Sec. 1182(b)(1), Nov. 30, 1993, 107 Stat. 1772] |

## Table 6: Legal Information Disclosure Prohibitions

| Subject/Title of Provision | United States Code Citation | Agency/Activity [Reference] |
|---|---|---|
| *Disclosure, Availability, and Use of Information* | 49 U.S.C., Subtitle II, Chapter 11, Subchapter II, Section 1114 | National Transportation Safety Board<br>[Public Law 103-272, Sec. 1(d), July 5, 1994, 108 Stat. 749; amended by National Transportation Safety Board Amendments of 1996, Public Law 104-291, title I, Sec. 102, 103, Oct. 11, 1996, 110 Stat. 3452] |
| *Disclosure of Confidential Information Generally* | 18 U.S.C., Part I, Chapter 93, Section 1905 | [Judiciary and Judicial Procedures Act, June 25, 1948, Ch. 645, 62 Stat. 791 as amended by Public Law 96-349, Sec. 7(b), Sept. 12, 1980, 94 Stat. 1158; Public Law 102-550, Title XIII, Sec. 1353, Oct. 28, 1992, 106 Stat. 3970; and Public Law 104-294, Title VI, Sec. 601(a)(8), Oct. 11, 1996, 110 Stat. 3498] |
| *Disclosure of Data* | 15 U.S.C., Chapter 53, Subchapter 1, Section 2613 | Environmental Protection Agency<br>[Toxic Substances Control Act, Public Law 94-469, Title I, Sec. 14, Oct. 11, 1976, 90 Stat. 2034; (Renumbered Title I,<br>Public Law 99-519, Sec. 3(c)(1), Oct. 22, 1986, 100 Stat. 2989)] |
| *Disclosure of Information* | 29 U.S.C., Chapter 22, Section 2008 | Polygraph<br>[Employee Polygraph Protection Act of 1988, Public Law 100-347, Sec. 9, June 27, 1988, 102 Stat. 652] |
| *Disclosure of Information by Commission* | 15 U.S.C., Chapter IID, Subchapter II,<br>Section 80b-10 | Securities and Exchange Commission<br>[The Investment Company Act of 1940, Aug. 22, 1940, Ch. 686, Title II, Sec. 210, 54 Stat. 854; Investment Advisers Act of 1940 Amendment, Public Law 86-750, Sec. 13, Sept. 13, 1960, 74 Stat. 887; and International Securities Enforcement Cooperation Act of 1990, Public Law 101-550, title II, Sec. 202(b)(2), Nov. 15, 1990, 104 Stat. 2715] |

## Table 6: Legal Information Disclosure Prohibitions

| Subject/Title of Provision | United States Code Citation | Agency/Activity [Reference] |
|---|---|---|
| *Disclosure of Information in Possession of Social Security Administration or Department of Health and Human Services* | 42 U.S.C. Chapter 7, Subchapter XI, Part A, Section 1306 | Social Security Administration/Department of Health and Human Services/Public Health Service<br>[Social Security Act of Aug. 14, 1935, Ch. 531, Title XI, Sec. 1106, as added Aug. 10, 1939, Ch. 666, Title VIII, Sec. 802, 53 Stat. 1398 amended Aug. 28, 1950, Ch. 809, Title IV, Sec. 403(d), 64 Stat. 559; Public Law 85-840, Title VII, Sec. 701, Aug. 28, 1958, 72 Stat. 1055;Public Law 89-97, Title I, Sec. 108(c), Title III, Sec. 340, July 30, 1965, 79 Stat. 339, 411; Public Law 90-248, Title I, Sec. 168, Title II, Sec. 241(c)(1), Jan. 2, 1968, 81 Stat. 875, 917; Public Law 92-603, Title II, Sec. 249C(a), Oct. 30, 1972, 86 Stat. 1428;<br>Public Law 93-647, Sec. 101(d), Jan. 4, 1975, 88 Stat. 2360; Public Law 97-35, Title XXII, Sec. 2207, Aug. 13, 1981, 95 Stat. 838; Public Law 98-369, Div. B, Title VI, Sec. 2663(j)(2)(D)(ii), (l), July 18, 1984, 98 Stat. 1170, 1171; Public Law 103-296, Title I, Sec. 108(b)(2)-(5), Title III, Sec. 311(a), 313(a), Aug. 15, 1994, 108 Stat. 1481, 1482, 1525, 1530] |
| *Disclosure of Wagering Tax Information* | 26 U.S.C., Subtitle D, Chapter 35, Subchapter C, Section 4424 | Treasury Department<br>[Public Law 93-499, Sec. 3(c)(1), Oct. 29, 1974, 88 Stat. 1550; amended by the Tax Reform Act of 1976, Public Law 94-455, Title XII, Sec. 1202(h)(6), Title XIX, Sec. 1906(b)(13)(A), Oct. 4, 1976, 90 Stat. 1688, 1834] |
| *Disclosures to FBI for Counterintelligence Purposes* | 15 U.S.C., Chapter 41, Subchapter III,<br>Section 1681u | [Fair Credit Reporting Act, Public Law 90-321, Title VI, Sec. 625, formerly Sec. 624, as added to by the Intelligence Authorization Act for Fiscal Year 1996, Public Law 104-93, Title VI, Sec. 601(a), Jan. 6, 1996, 109 Stat. 974; renumbered Sec. 625 and amended by the USA Patriot Act, Public Law 107-56, Title III, Sec. 358(g)(1)(A), Title V, Sec. 505(c), Oct. 26, 2001, 115 Stat. 327, 366] |

## Table 6: Legal Information Disclosure Prohibitions

| Subject/Title of Provision | United States Code Citation | Agency/Activity [Reference] |
|---|---|---|
| *Disclosure to Foreign Antitrust Authority of Antitrust Evidence* | 15 U.S.C., Chapter 88, Section 6201 | Department of Justice/Federal Trade Commission<br>[International Antitrust Enforcement Assistance Act of 1994, Pub. L. 103-438, Sec. 2, Nov. 2, 1994, 108 Stat. 4597] |
| *Disclosures to Government Agencies for Counterterrorism Purposes* | 15 U.S.C., Chapter 41,<br>Subchapter III,<br>Section 1681v | Department of Homeland Security/Counterterrorism<br>[Fair Credit Reporting Act, Public Law 90-321, Title VI, Sec. 626; as added to by the USA Patriot Act, Public Law 107-56, Title III, Sec. 358(g)(1)(B), Oct. 26, 2001, 115 Stat. 327] |
| *Disposition of Rights* | 35 U.S.C., Part II,<br>Chapter 18,<br>Section 202(c)(5) | Department of Commerce<br>Patent Rights<br>[Government Patent Policy Act of 1980, Public Law 96-517, Sec. 6(a), Dec. 12, 1980, 94 Stat. 3020; amended by the Trademark Clarification Act of 1984, Public Law 98-620, Title V, Sec. 501(6), Nov. 8, 1984, 98 Stat. 3364-3366] |
| *Dissemination of Unclassified Information* | 42 U.S.C., Chapter 23, Division A, Subchapter XI, Section 2168 | Department of Energy<br>[Atomic Energy Act of Aug. 1, 1946, Ch. 724, Title I, Sec. 148, as added to by Public Law 97-90, Title II, Sec. 210(a)(1), Dec. 4, 1981, 95 Stat. 1169 and amended by Public Law 97-415, Sec. 17, Jan. 4, 1983, 96 Stat. 2076; renumbered Title I, Public Law 102-486, Title IX, Sec. 902(a)(8), Oct. 24, 1992, 106 Stat. 2944] |
| *Employees of Nonappropriated Fund Instrumentalities: Reprisals* | 10 U.S.C., Subtitle A, Part II, Chapter 81, Section 1587(e) | Department of Defense<br>[Department of Defense Authorization Act, 1984, Public Law 98-94, Title XII, Sec. 1253(a)(1), Sept. 24, 1983, 97 Stat. 699; amended by the National Defense Authorization Act for Fiscal Year 1996, Public Law 104-106, Div. A, Title IX, Sec. 903(f)(3), Title X, Sec. 1040(a)-(d)(1), Feb. 10, 1996, 110 Stat. 402, 433] |
| *Equal Employment Opportunities Enforcement Provisions* | 42 U.S.C., Chapter 21, Subchapter 6, Section 2000e-5 | Equal Employment Opportunities Commission<br>[Civil Rights Act of 1964, Public Law 88-352, Title VII, Sec. 706, July 2, 1964, 78 Stat. 259] |

## Table 6: Legal Information Disclosure Prohibitions

| Subject/Title of Provision | United States Code Citation | Agency/Activity [Reference] |
|---|---|---|
| *Evidence, Procedure, and Certification for Payments* | 42 U.S.C., Chapter 7, Subchapter II, Section 405 | Social Security Numbers<br>[Social Security Act of Aug. 14, 1935, Ch. 531, Title II, Sec. 205, 49 Stat. 624 as amended (e.g., Public Law 93-445 Title III, Sec. 302(a), 303, Oct. 16, 1974, 88 Stat. 1358 and Public Law 101-624, Title XVII, Sec. 1735(a), (b), Title XXII, Sec. 2201(b), (c), Nov. 28, 1990, 104 Stat. 3791, 3792, 3951, 3952)] |
| *Family Educational and Privacy Rights* | 20 U.S.C., Chapter 31, Section 1232g | Department of Education, Students<br>[Elementary and Secondary Education Amendments of 1967, Public Law 90-247, Title IV, Sec. 444, formerly Sec. 438, as added to by Elementary and Secondary Education Amendments Act of 1974, Public Law 93-380, Title V, Sec. 513(a), Aug. 21, 1974, 88 Stat. 571; amended by Public Law 93-568, Sec. 2(a), Dec. 31, 1974, 88 Stat. 1858; Public Law 96-46, Sec. 4(c), Aug. 6, 1979, 93 Stat. 342; the Student Right-To-Know and Campus Security Act of 1990, Public Law 101-542, Title II, Sec. 203, Nov. 8, 1990, 104 Stat. 2385 Pub. L. 102-325, Title XV, Sec. 1555(a), July 23, 1992, 106 Stat. 840; renumbered Sec. 444 and amended by Public Law 103-382, Title II, Sec. 212(b)(1), 249, 261(h), Oct. 20, 1994, 108 Stat. 3913, 3924, 3928; amended by the Higher Education Amendments of 1998, Public Law 105-244, Title IX, Sec. 951, 952, Oct. 7, 1998, 112 Stat. 1835, 1836 and the Campus Sex Crimes Prevention Act, Public Law 106-386, Div. B, Title VI, Sec. 1601(d), Oct. 28, 2000, 114 Stat. 1538] |
|  |  |  |
| *Federal Parent Locator Service* | 42 U.S.C., Chapter 7, Subchapter IV, Part D, Section 653(b)(2) | Department of Health and Human Services<br>[Social Security Act of Aug. 14, 1935, Ch. 531, Title IV, Sec. 453, as added Public Law 93-647, Sec. 101(a), Jan. 4, 1975, 88 Stat. 2353 and amended by Public Law 105-33, Sec. 5534(a)(2)] |

## Table 6: Legal Information Disclosure Prohibitions

| Subject/Title of Provision | United States Code Citation | Agency/Activity [Reference] |
|---|---|---|
| *Fraud and Related Activity in Connection with Computers* | 18 U.S.C., Part D, Chapter 47, Section 1030(a)(3) | [Computer Fraud and Abuse Act of 1986, Public Law 99-474, Sec. 2, Oct. 16, 1986, 100 Stat. 1213; as amended by the National Information |
| | | Infrastructure Protection Act of 1996, Public Law 104-294, Title II, Sec. 201, Title VI, Sec. 604(b)(36), Oct. 11, 1996, 110 Stat. 3491, 3508] |
| *Fund for Rural America* | 7 U.S.C., Chapter 55, Section 2204f(c)(1)(D) | Department of Agriculture, Treasury Department<br>[Federal Agriculture Improvement and Reform Act of 1996, Public Law 104-127, Title VII, Sec. 793, Apr. 4, 1996, 110 Stat. 1152] |
| *General Provisions* | 7 U.S.C., Chapter 38, Subchapter II, Part E, Section 1636 | Department of Agriculture Livestock Reporting<br>[The Farmers' Home Administration Act of 1946, Aug. 14, 1946, Ch. 966, Title II, Sec. 251, as added to by the Agricultural Appropriations Act of 1999, Public Law 106-78, Title IX, Sec. 911(2), Oct. 22, 1999, 113 Stat. 1200] |
| *General Provisions Governing Discovery* | Title V, Depositions and Discovery, Rule 26 (a)(1)(E) and (c) | International Trade Courts<br>[Rules and Forms of the U.S. Court of International Trade, Title V, Rule 26] |
| *General Provisions Respecting Control of Devices Intended for Human Use* | 21 U.S.C., Chapter 9, Subchapter V, Part A, Section 360j | Department of *Health and Human Services*<br>[Fair Labor Standards Act, June 25, 1938, Ch. 675, Sec. 520, as added to by the Medical Device Regulation Act, Public Law 94-295, Sec. 2, May 28, 1976, 90 Stat. 565] |
| *General Rules Regarding Provision of Assistance* | 7 U.S.C., Chapter 88, Subchapter VI, Section 5906(d) | Department of Agriculture/ Alternative Agricultural Research and Commercialization Corporation<br>[Food, Agriculture, Conservation, and Trade Act of 1990, Public Law 101-624, Title XVI, Sec. 1662, Nov. 28, 1990, 104 Stat. 3764] |
| *Identifying Numbers* | 26 U.S.C., Subtitle F, Chapter 61 Subchapter B, Section | Department of Agriculture<br>Internal Revenue Service |

## Table 6: Legal Information Disclosure Prohibitions

| Subject/Title of Provision | United States Code Citation | Agency/Activity [Reference] |
|---|---|---|
| | 6109 | [The Internal Revenue Code Amendment of 1961, Public Law 87-397, Sec. 1(a), Oct. 5, 1961, 75 Stat. 828; amended by the Social Security Independence and Program Improvements Act of 1994, Public Law 103-296, Title III, Sec. 316(b), Aug. 15, 1994, 108 Stat. 1532; and the Minimum Wage Increase Act of 1996, Public Law 104-188, Title I, Sec. 1615(a)(2)(A), 1704(t)(42), Aug. 20, 1996, 110 Stat. 1853, 1889] |
| *Information* | 30 U.S.C., Chapter 29, Section 1733 | Department of the Interior [Federal Oil and Gas Royalty Management Act of 1982, Public Law 97-451, Title II, Sec. 203, Jan. 12, 1983, 96 Stat. 2458] |
| *Information Collection* | 16 U.S.C., Chapter 38, Subchapter V,<br>Section 1881a | Department of Commerce Fisheries<br>[Interim Fisheries Zone Extension and Management Act, Public Law 94-265, Title IV, Sec. 402, as added to by the Fisheries Financing Act of1996, Public Law 104-297, Title II, Sec. 203, Oct. 11, 1996, 110 Stat. 3607] |
| *Inspector General for Agency* | 50 U.S.C., Chapter 15, Section 403q(e)(3)(A) | Central Intelligence Agency [Central Intelligence Agency Act of 1949, June 20, 1949, Ch. 227, Sec. 17, as added to by Pub. L. 102-496, Title VI, Sec. 601, Oct. 24, 1992, 106 Stat. 3187; and amended by the Intelligence Authorization Act for Fiscal Year 1993, Public Law 104-93, Title IV, Sec. 403, Jan. 6, 1996, 109 Stat. 969] |
| *Interagency Data Sharing* | 12 U.S.C., Chapter 16, Section 1828b | Treasury Department [Gramm-Leach-Bliley Act, Public Law 106-102, Title I, Sec. 132, Nov. 12, 1999, 113 Stat. 1382] |
| *Interception and Disclosure of* | 18 U.S.C., Part I, Chapter | Wire Taps |

## Table 6: Legal Information Disclosure Prohibitions

| Subject/Title of Provision | United States Code Citation | Agency/Activity [Reference] |
|---|---|---|
| *Wire, Oral, or Electronic Communications Prohibited* | 119, Section 2511 | [Omnibus Crime Control and Safe Streets Act of 1968, Public Law 90-351, Title III, Sec. 802, June 19, 1968, 82 Stat. 213 amended by District of Columbia Court Reform and Criminal Procedure Act of 1970, Public Law 91-358, Title II, Sec. 211(a), July 29, 1970, 84 Stat. 654; Foreign Intelligence Surveillance Act of 1978,Public Law 95-511, Title II, Sec. 201(a)-(c), Oct. 25, 1978, 92 Stat. 1796, 1797; Cable Communications Policy Act of 1984, Public Law 98-549, Sec. 6(b)(2), Oct. 30, 1984, 98 Stat. 2804; Electronic Communications Privacy Act of 1986, Public Law 99-508, Title I, Sec. 101(b), (c)(1), (5), (6), (d), (f)((1)), 102, Oct. 21, 1986, 100 Stat. 1849, 1851-1853; Violent Crime Control Law Enforcement Act of 1994, Public Law 103-322, Title XXXII, Sec. 320901, Title XXXIII, Sec. 330016(1)(G), Sept. 13, 1994, 108 Stat. 2123, 2147; Communications Assistance for Law Enforcement Act,<br>Public Law 103-414, Title II, Sec. 202(b), 204, 205, Oct. 25, 1994, 108 Stat. 4290, 4291; Public Law 104-294, Title VI, Sec. 604(b)(42), Oct. 11, 1996, 110 Stat. 3509; and the USA Patriot Act, Public Law 107-56, Title II, Sec. 204, 217(2), Oct. 26, 2001, 115 Stat. 281, 291] |
| *Inspector General* | 22 U.S.C., Chapter 52,<br>Subchapter II,<br>Section 3929(f) | State Department<br>[Foreign Service Act of 1980, Public Law 96-465, Title I, Sec. 209, Oct. 17, 1980, 94 Stat. 2080] |
| *Investigations* | 42 U.S.C., Chapter 21,<br>Subchapter VI,<br>Section 2000e-8 | Equal Employment Opportunity Commission<br>[Public Law 88-352, Title VII, Sec. 709, July 2, 1964, 78 Stat. 262 and Public Law 92-261, Sec. 6, Mar. 24, 1972, 86 Stat. 107] |

## Table 6: Legal Information Disclosure Prohibitions

| Subject/Title of Provision | United States Code Citation | Agency/Activity [Reference] |
|---|---|---|
| *Jurisdiction* | 28 U.S.C., Part III,<br>Chapter 44, Section 652(d) | Courts<br>[Judicial Improvements and Access to Justice Act, Public Law 100-702, Title IX, Sec. 901(a), Nov. 19, 1988, 102 Stat. 4659; amended by the Alternative Dispute Resolution Act of 1998, Public Law 105-315, Sec. 4, Oct. 30, 1998, 112 Stat. 2994] |
| *Limitations on access to financial records* | 38 U.S.C., Part IV,<br>Chapter 53, Section 5319 | Department of Veterans Affairs<br>[Veterans' Benefits Act of 1992, Public Law 102-568, Title VI, Sec. 603(b)(1), Oct. 29, 1992, 106 Stat. 4342] |
| *Maps, Charts, and Geodetic Data: Public Availability;*<br>*Exceptions* | 10 U.S.C., Subtitle A,<br>Part I, Chapter 22, Subchapter II, Section 455 | Department of Defense<br>[Intelligence Authorization Act, Fiscal Year 1991, Public Law 102-88, Title V, Sec. 502(a)(1), Aug. 14, 1991, 105 Stat. 435, Sec. 2796; amended by the National Imagery and Mapping Agency Act of 1996, Public Law 104-201, Div. A, Title XI, Sec. 1112(b), Sept. 23, 1996, 110 Stat. 2682; and the National Defense Authorization Act for Fiscal Year 1998, Public Law 105-85, Div. A, Title IX, Sec. 933(a), (b)(1), Nov. 18, 1997, 111 Stat. 1866] |
| *Miscellaneous Provisions* | 12 U.S.C., Chapter 7A, Section 1141j | Farm Credit Administration/Treasury Department<br>[Agricultural Marketing Act, June 15, 1929, Ch. 24, Sec. 15, 46 Stat. 18] |
| *National Program of Cancer Registries* | 42 U.S.C., Chapter 6A, Subchapter II, Part M, Section 280e | Department of Health and Human Services/Public Health Service<br>[Public Health Service Act of July 1, 1944, Ch. 373, Title III, Sec. 399B, formerly Sec. 399H, as added Public Law 102-515, Sec. 3, Oct. 24, 1992, 106 Stat. 3372 renumbered Sec. 399B and amended by Public Law 106-310, Div. A, Title V, Sec. 502(2)(A), (B), Oct. 17, 2000, 114 Stat. 1115] |

## Table 6: Legal Information Disclosure Prohibitions

| Subject/Title of Provision | United States Code Citation | Agency/Activity [Reference] |
|---|---|---|
| *Noncombatant Assistance to United Nations* | 22 U.S.C., Chapter 7, Section 287d-1(d) | State Department<br>[United Nations Participation Act of 1945, Dec. 20, 1945, ch. 583, Sec. 7, as added Oct. 10, 1949, Ch. 660, Sec. 5, 63 Stat. 735] |
| *Notice of Defendant's Intention to Disclose Classified Information* | 18 U.S.C., Unlawful Possession or Receipt of Fire Arms, Section 1201 to 1203, Interstate Agreement on Detainers, Sec. 5 | Courts<br>[Classified Information Criminal Trial Procedures Act, Public Law 96-456, Sec. 5, Oct. 15, 1980, 94 Stat. 2026] |
| *Obligation to Make Royalty Payments* | 17 U.S.C., Chapter 10, Subchapter C,<br>Section 1003(c)(2) | Department of Commerce<br>[Audio Home Recording Act of 1992, Public Law 102-563, Sec. 2, Oct. 28, 1992, 106 Stat. 4240] |
| *Obligations With Respect to Disclosures of Personal Information* | 15 U.S.C., Chapter 94, Subchapter I, Section 6802 | Financial<br>[Gramm-Leach-Bliley Act a.k.a. Financial Modernization Act of 1999, Public Law 106-102, Title V, Sec. 502, Nov. 12, 1999, 113 Stat. 1437] |
| *Patents and Technical Information* | 22 U.S.C., Chapter 32, Subchapter III, Part I, Section 2356 | Department of State<br>Department of Defense<br>[Foreign Assistance Act of 1961, Public Law 87-195, Pt. III, Sec. 606, Sept. 4, 1961, 75 Stat. 440] |
| *Paul D. Coverdell Drug-Free Workplace Program* | 15 U.S.C., Chapter 14A, Section 654(c) | Medical Information<br>[Small Business Act, Public Law 85-536, Sec. 2(27), as added to by the Small Business Administration Reauthorization and Amendments Act of 1990, Public Law 101-574, Title III, Sec. 310, Nov. 15, 1990, 104 Stat. 2831] |
| *Payment of Cost of Testing for Sexually Transmitted Diseases* | 42 U.S.C., Chapter 136, Subchapter III, Part E, Section 14011 | Law Enforcement<br>[Violence Against Women Act of 1994, Public Law 103-322, Title IV, Sec. 40503, Sept. 13, 1994, 108 Stat. 1946 and Public Law 104-294, Title VI, Sec. 604(b)(1), Oct. 11, 1996, 110 Stat. 3506] |

## Table 6: Legal Information Disclosure Prohibitions

| Subject/Title of Provision | United States Code Citation | Agency/Activity [Reference] |
|---|---|---|
| *Penalties for Disclosure of Information* | 8 U.S.C., Chapter 12, Subchapter II, Part IX, Section 1367 | Department of Justice<br>[Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Public Law 104-208, Div. C, Title III, Sec. 308(g)(8)(D), 384, Sept. 30, 1996, 110 Stat. 3009-624, 3009-652; as amended by Public Law 105-33, Title V, Sec. 5572(b), Aug. 5, 1997, 111 Stat. 641; and Public Law 106-386, Div. B, Title V, Sec. 1513(d), Oct. 28, 2000, 114 Stat. 1536] |
| *Permissive Provisions* | 7 U.S.C., Chapter 79, Section 4810 | Department of Agriculture<br>[Food Security Act of 1985, Public Law 99-198, Title XVI, Sec. 1621, Dec. 23, 1985, 99 Stat. 1617] |
| *Permissive Terms and Conditions in Orders* | 7 U.S.C., Chapter 60, Section 2706 | Department of Agriculture/ Egg Board<br>[Egg Research and Consumer Information Act, Public Law 93-428, Sec. 7, Oct. 1, 1974, 88 Stat. 1173] |
| *Petroleum Product Information* | 33 U.S.C., Chapter 12, Subchapter I,<br>Section 555a(d) | Army Corps of Engineers/ Department of Defense<br>[Water Resources Development Act of 1986, Public Law 99-662, Title IX, Sec. 919, Nov. 17, 1986, 100 Stat. 4192] |
| *Physical Protection of Special Nuclear Material: Limitation on Dissemination of Unclassified Information* | 10 U.S.C., Subtitle A, Part I, Chapter 3, Section 128 | Department of Energy<br>[Department of Energy National Security and Military Applications of Nuclear Energy Authorization Act of 1988, Public Law 100-180, Div. A, Title XI, Sec. 1123(a), Dec. 4, 1987, 101 Stat. 1149 as amended by the National Defense Authorization Act<br>for Fiscal Year 1991, Public Law, Div. A, Title XIII, Sec. 1311(1), Nov. 5, 1990, 104 Stat. 1669] |
| *Privacy* | 15 U.S.C., Chapter 94 | Privacy<br>[Gramm-Leach-Bliley Act a.k.a. Financial Modernization Act of 1999, Public Law 106-102, Nov. 12, 1999] |
| *Privacy* | 5 U.S.C., Part I, Chapter 5, Subchapter II, Section 552a (*Administrative Procedure*) | Privacy<br>[Privacy Act of 1974, Public Law 93-579, Dec. 31, 1974] |

## Table 6: Legal Information Disclosure Prohibitions

| Subject/Title of Provision | United States Code Citation | Agency/Activity [Reference] |
|---|---|---|
| *Prohibition on Release and Use of Certain Personal Information from State Motor Vehicle Records* | 18 U.S.C., Part I, Chapter 123, Section 2721 | States<br>[Driver's Privacy Protection Act of 1994, Public Law 103-322, Title XXX, Sec. 300002(a), Sept. 13, 1994, 108 Stat. 2099 amended by Public Law 106-69, Title III, Sec. 350(c), (d), Oct. 9, 1999, 113 Stat. 1025; and Public Law 106-346, Sec. 101(a) (Title III, Sec. 309(c)-(e)), Oct. 23, 2000, 114 Stat. 1356, 1356A-24] |
| *Program Requirements* | 42 U.S.C., Chapter 13, Section 1758 | Department of Agriculture/ Public Health Service<br>[Better Nutrition and Health for Children Act of 1994, Public Law 103-448, Sec. 108] |
| *Prohibition Against Disclosure of Information* | 42 U.S.C., Chapter 7, Subchapter XI, Part B, Section 1320c-9 | Department of Health and Human Services/ Public Health Service/ Social Security Administration<br>[Social Security Act of Aug. 14, 1935, Ch. 531, Title XI, Sec. 1160, as added to by Public Law 97-248, Title I, Sec. 143, Sept. 3, 1982, 96 Stat. 391 and amended by Public Law 99-509, Title IX, Sec. 9353(d)(1), Oct. 21, 1986, 100 Stat. 2047; Public Law 100-203, Title IV, Sec. 4039(h)(6), Dec. 22, 1987, as added to by Public Law 100-360, Title IV, Sec. 411(e)(3), July 1, 1988, 102 Stat. 776; Public Law 101-508, Title IV, Sec. 4205(d)(1)(B), (e)(1), Nov. 5, 1990, 104 Stat. 1388-113, 1388-114; Public Law 103-432, Title I, Sec. 156(b)(2)(B), (4), Oct. 31, 1994, 108 Stat. 4441] |
| *Prohibition of Advance Disclosure of Funding Decisions* | 42 U.S.C., Chapter 44, Section 3537a | Department of Housing and Urban Development<br>[Department of Housing and Urban Development Act, Public Law 89-174, Sec. 12, as added to by Pub. L. 101-235, Title I, Sec. 103, Dec. 15, 1989, 103 Stat. 1995] |
| *Prohibition Against Disclosure of Information or Knowledge* | 22 U.S.C., Chapter 7, Section 287t | International Monetary Fund<br>[Participation in UNESCO, July 30, 1946, Ch. 700, Sec. 8, 60 Stat. 714] |

## Table 6: Legal Information Disclosure Prohibitions

| Subject/Title of Provision | United States Code Citation | Agency/Activity [Reference] |
|---|---|---|
| *Prohibition of Public Disclosure of Proprietary Information* | 12 U.S.C., Chapter 46, Section 4546 | Treasury Department<br>[Federal Housing Enterprises Financial Safety and<br>Soundness Act of 1992, Public Law 102-550, Title XIII, Sec. 1326, Oct. 28, 1992, 106 Stat. 3955] |
| *Protection of Trade Secrets and Other Information* | 7 U.S.C., Chapter 6, Subchapter II,<br>Section 136h | Department of Agriculture/ Environmental Protection Agency [Federal Insecticide, Fungicide, and Rodenticide Act, June 25, 1947, Ch. 125, Sec. 10, as added to by Public Law 92-516, Sec. 2, Oct. 21, 1972, 86 Stat. 989; amended by the Federal Pesticide Act of 1995, Public Law 95-396, Sec. 15, Sept. 30, 1978, 92 Stat. 829; Public Law 98-620, Title IV, Sec. 402(4) (B), Nov. 8, 1984, 98 Stat. 3357; Public Law 100-532, Title VIII, Sec 801(f), Oct. 25, 1988, 102 Stat. 2682; and Public Law 102-237, Title X, Sec. 1006(b)(1), (2), (3)(J), Dec. 13, 1991, 105 Stat. 1895, 1896]. |
| *Provision of Certain Counseling Services* | 42 U.S.C., Chapter 6A, Subchapter XXIV,<br>Section 300ff-62 | Department of Health and Human Services/Public Health Service [Ryan White Comprehensive AIDS Resources Emergency Act of 1990, Public Law 101-381, Title III, Sec. 301(a), Aug. 18, 1990, 104 Stat. 610] |
| *Provisions* | 22 U.S.C., Chapter 58, Subchapter III,<br>Section 4833 | State Department<br>[Omnibus Diplomatic Security and Antiterrorism Act of 1986, Public Law 99-399, Title III, Sec. 303, Aug. 27, 1986, 100 Stat. 859] |
| *Provisions Relating to Disclosures of Violations of Law, Gross Mismanagement, and Certain Other Matters* | 5 U.S.C., Part II,<br>Chapter 12, Subchapter II,<br>Section 1213(h) | Office of Personnel Management<br>[Whistleblower Protection Act of 1989, Public Law 101-12, Sec. 3(a)(13), Apr. 10, 1989, 103 Stat. 21; as amended by the General Accounting Office Act of 1996, Public Law 104-316, Title I, Sec. 103(a), Oct. 19, 1996, 110 Stat. 3828] |
| *Public Access to Information* | 33 U.S.C., Chapter 29, Section 1513 | Department of Transportation/ Department of Homeland Security [Public Law 93-627, Sec. 14, Jan. 3, 1975, 88 Stat. 2139] |

## Table 6: Legal Information Disclosure Prohibitions

| Subject/Title of Provision | United States Code Citation | Agency/Activity [Reference] |
|---|---|---|
| *Public Disclosure* | 7 U.S.C., Chapter 1, Section 12 | Commodity Futures Trading Commission<br>[Grain Futures Act of Sept. 21, 1922, Ch. 369, Sec. 8, 42 Stat. 1003; amended by the Commodity Exchange Act of June 15, 1936, Ch. 545, Sec. 2, 49 Stat. 1491; Public Law 90-258, Sec. 19(a), Feb. 19, 1968, 82 Stat. 32; Commodity Futures Trading Commission Act, Public Law 93-463, Title I, Sec. 103(a), (e), Oct. 23, 1974, 88 Stat. 1392; Public Law 95-405, Sec. 16, Sept. 30, 1978, 92 Stat. 873; Futures Trading Act of 1982, Public Law 97-444, Title II, Sec. 222, Jan. 11, 1983, 96 Stat. 2309; Futures Trading Practices Act of 1992, Public Law 102-546, Title II, Sec. 205, Title III, Sec. 304, 305, Title IV, Sec. 402(7), Oct. 28, 1992, 106 Stat. 3600, 3623, 3624; and Public Law 106-554, Sec. 1(a)(5) (Title I, Sec. 123(a)(18), Title II, Sec. 253(a)), Dec. 21, 2000, 114 Stat. 2763, 2763A-410, 2763A-449] |
| *Public Disclosure of Final Orders and Agreements (Government Sponsored Enterprises)* | 12 U.S.C., Chapter 46, Sections 4522, 4586 and 4639 | Treasury Department<br>[Federal Housing Enterprises Financial Safety and Soundness Act of 1992, Public Law 102-550, Title XIII, Sec. 1326, Oct. 28, 1992, 106 Stat. 3955] |
| *Public Disclosure of Information* | 15 U.S.C., Chapter 47, Section 2055 | Consumer Product Safety Commission<br>[Consumer Product Safety Act, Public Law 92-573, Sec. 6, Oct. 27, 1972, 86 Stat. 1212; amended by Public Law 97-35, Title XII, Sec. 1204, Aug. 13, 1981, 95 Stat. 713; the Orphan Drug Act of 1997, Public Law 97-414, Sec. 9(j)(1), Jan. 4, 1983, 96 Stat. 2064; and the Consumer Product Safety Improvement Act of 1990, Public Law 101-608, title I, Sec. 106, 112(c), Nov. 16, 1990, 104 Stat. 3111, 3116] |

## Table 6: Legal Information Disclosure Prohibitions

| Subject/Title of Provision | United States Code Citation | Agency/Activity [Reference] |
|---|---|---|
| *Recommendations by Promotion Boards* | 10 U.S.C., Subtitle E, Part III, Chapter 1403, Section 14108 | Department of Defense [Reserve Officer Personnel Management Act of 1994, Pub. L. 103-337, div. A, title XVI, Sec. 1611, Oct. 5, 1994, 108 Stat. 2928] |
| *Recordkeeping, Inspections, Monitoring, and Entry* | 42 U.S.C., Chapter 85, Subchapter I, Part A, Section 7414(c) | Environmental Protection Agency [Clean Air Act of July 14, 1955, Ch. 360, Title I, Sec. 114, as added to by Public Law 91-604, Sec. 4(a), Dec. 31, 1970, 84 Stat. 1687] |
| *Records and Reports; Inspections* | 33 U.S.C., Chapter 26, Subchapter III, Section 1318(b) | Water Pollution [River and Harbor Act of 1948, June 30, 1948, Ch. 758, Title III, Sec. 308, as added to by the Water Pollution Control Act of 1972, Public Law 92-500, Sec. 2, Oct. 18, 1972, 86 Stat. 858; amended by the Water Quality Act of 1987, Public Law 100-4, Title III, Sec. 310, Title IV, Sec. 406(d)(1), Feb. 4, 1987, 101 Stat. 41, 73] |

## Table 6: Legal Information Disclosure Prohibitions

| Subject/Title of Provision | United States Code Citation | Agency/Activity [Reference] |
|---|---|---|
| *Records Maintained on Individuals* | 5 U.S.C., Part I, Chapter 5, Subchapter II, Section 552a | Privacy Act<br>[Privacy Act of 1974, Public Law 93-579, Dec. 31, 1974; amended by Public Law 94-183, Sec. 2(2), Dec. 31, 1975, 89 Stat. 1057; Debt Collection Act of 1982, Public Law 97-365, Sec. 2, Oct. 25, 1982, 96 Stat. 1749; Congressional Reports Elimination Act of 1982, Public Law 97-375, Title II, Sec. 201(a), (b), Dec. 21, 1982, 96 Stat. 1821; Public Law 97-452, Sec. 2(a)(1), Jan. 12, 1983, 96 Stat. 2478; Central Intelligence Agency Information Act, Public Law 98-477, Sec. 2(c), Oct. 15, 1984, 98 Stat. 2211; National Archives and Records Administration Act of 1984, Public Law 98-497, Title I, Sec. 107(g), Oct. 19, 1984, 98 Stat. 2292; Computer Matching and Privacy Protection Act of 1988, Public Law 100-503, Sec. 2-6(a), 7, 8, Oct. 18, 1988, 102 Stat. 2507-2514; Omnibus Budget Reconciliation Act of 1990, Public Law 101-508, Title VII, Sec. 7201(b)(1), Nov. 5, 1990, 104 Stat. 1388-334; Omnibus Budget Reconciliation Act of 1993, Public Law 103-66, Title XIII, Sec. 13581(c), Aug. 10, 1993, 107 Stat. 611; Personal Responsibility and Work Opportunity Recon-ciliation Act of 1996, Public Law 104-193, Title I, Sec. 110(w), Aug. 22, 1996, 110 Stat. 2175; Social Security-Medicare and Medicaid Coverage Data Bank Repeal, Public Law 104-226, Sec. 1(b) (3), Oct. 2, 1996, 110 Stat. 3033; General Accounting Office Act of 1996, Public Law 104-316, Title I, Sec. 115(g)(2)(B), Oct. 19, 1996, 110 Stat. 3835; Taxpayer Re-lief Act of 1997, Public Law 105-34, Title X, Sec. 1026(b) (2), Aug. 5, 1997, 111 Stat. 925; Federal Reports Elimination Act, Public Law 105-362, Title XIII, Sec. 1301(d), Nov. 10, 1998, 112 Stat. 3293; Tax Relief Extension Act of 1999, Public Law 106-170, Title IV, Sec. 402(a)(2), Dec. 17, 1999, 113 Stat. 1908.] |

## Table 6: Legal Information Disclosure Prohibitions

| Subject/Title of Provision | United States Code Citation | Agency/Activity [Reference] |
|---|---|---|
| *Regulation of Unfair and Deceptive Acts and Practices in Connection with Collection and Use of Personal Information from and About Children on the Internet* | 15 U.S.C., Chapter 91, Section 6502(b)(2)(C)(ii) | Internet<br>[Children's Online Privacy Protection Act (15 U.S.C. §6501-6506), Public Law 105-277, Div. C, Title XIII, Sec. 1303, Oct. 21, 1998, 112 Stat. 2681-730] |
| *Reporting of Suspicious Transactions* | 31 U.S.C., Subtitle IV, Chapter 53, Subchapter II, Section 5318(g)(2) | Financial<br>[Money Laundering Suppression Act of 1994, Public Law 103-325, Section 413(b)(1), Sept. 23, 1994, 108 Stat. 2245, 2252, 2254] |
| *Reporting Requirements; Disclosure of Information* | 16 U.S.C., Chapter 16C, Section 973j | Department of Commerce<br>[South Pacific Tuna Act of 1988, Public Law 100-330, Sec. 12, June 7, 1988, 102 Stat. 599] |
| *Reports of Information Regarding Safety and Soundness of Depository Institutions* | 12 U.S.C., Chapter 16, Section 1831m-1(a)(2)(B) | Financial<br>[Annunzio-Wylie Anti-Money Laundering Act of 1992, Public Law 102-550, Title XV, Sec. 1542, Oct. 28, 1992, 106 Stat. 4067] |
| *Reports; Recordkeeping; Investigations* | 29 U.S.C., Chapter 30, Subchapter V,<br>Section 2935(a)(4)(B)(i) | Department of Labor<br>[Twenty-First Century Workforce Commission Act,<br>Public Law 105-220, Title I, Sec. 185, Aug. 7, 1998, 112 Stat. 1046] |
| *Requests by Authorized Investigative Agencies* | 50 U.S.C., Chapter 15, Section 436 (b) and (e) | Intelligence Community<br>[National Security Act of 1947, July 26, 1947, Ch. 343, Title VIII, Sec. 802, as added to by the Counterintelligence<br>and Security Enhancements Act of 1994, Public Law 103-359, Title VIII, Sec. 802(a), Oct. 14, 1994, 108 Stat. 3436] |
| *Required Terms in Orders* | 7 U.S.C., Chapter 101, Subchapter V,<br>Section 7484 | Department of Agriculture/ Popcorn Board<br>[Agriculture Improvement and Reform Act of 1996, Public Law 104-127, Title V, Sec. 575, Apr. 4, 1996, 110 Stat. 1077] |
| *Required Terms of Order; Agreements Under Order; Records* | 7 U.S.C., Chapter 76, Subchapter II,<br>Section 4534 | Department of Agriculture/ National Dairy Research Endowment Institute<br>[Dairy Production Stabilization Act of 1983, Public Law 98-180, Title I, Sec. 133, as added to by the Food Security Act of 1985, Public Law 99-198, Title I, Sec. 121, Dec. 23, 1985, 99 Stat. 1369] |

## Table 6: Legal Information Disclosure Prohibitions

| Subject/Title of Provision | United States Code Citation | Agency/Activity [Reference] |
|---|---|---|
| *Research on Transplantation of Fetal Tissue* | 42 U.S.C., Chapter 6A, Subchapter III, Part H, Section 289g-1(d)(2) | Department of Health and Human Services/National Institutes of Health<br>[Public Health Service Act of July 1, 1944, Ch. 373, Title IV, Sec. 498A, as added to by Public Law 103-43, Title I, Sec. 111, June 10, 1993, 107 Stat. 129] |
| *Restriction of Access by Minors to Materials Commercially Distributed by Means of World Wide Web that are Harmful to Minors* | 47 U.S.C., Chapter 5, Subchapter II, Part I, Section 231 | [Communications Act of 1934, June 19, 1934, Ch. 652, Title II, Sec. 231, as added to by the Children's Online Privacy Protection Act of 1998, Public Law 105-277, Div. C, Title XIV, Sec. 1403, Oct. 21, 1998, 112 Stat. 2681-736] |
| *Restrictions on Disclosing and Obtaining Contractor Bid or Proposal Information or Source Selection Information* | 41 U.S.C., Chapter 7, Section 423 | [Office of Federal Procurement Policy Act, Public Law 93-400, Sec. 27, as added to by Office of Federal Procurement Policy Act Amendments of 1988, Public Law 100-679, Sec. 6(a), Nov. 17, 1988, 102 Stat. 4063 and amended by the National Defense Authorization Act for Fiscal Years 1990 and 1991, Public Law 101-189, Div. A, Title VIII, Sec. 814(a)-(d)(1), Nov. 29, 1989, 103 Stat. 1495-1498; National Defense Authorization Act for Fiscal Year 1991, Public Law 101-510, Div. A, Title XIV, Sec. 1484(l)(6), Nov. 5, 1990, 104 Stat. 1720; Persian Gulf Conflict Supplemental Authorization and Personnel Benefits Act of 1991, Public Law 102-25, Title VII, Sec. 705(i), Apr. 6, 1991, 105 Stat. 121; Federal Acquisition Streamlining Act of 1994, Public Law 103-355, Title VIII, Sec. 8301(e), Oct. 13, 1994, 108 Stat. 3397; and the Federal Acquisition Reform Act of 1996, Public Law 104-106, Div. D, Title XLIII, Sec. 4304(a), Feb. 10, 1996, 110 Stat. 659] |
| *Right to Financial Privacy* | 12 U.S.C., Chapter 35 | [Right to Financial Privacy Act of 1978, Public Law 95-630, Nov. 10, 1978] |

## Table 6: Legal Information Disclosure Prohibitions

| Subject/Title of Provision | United States Code Citation | Agency/Activity [Reference] |
|---|---|---|
| *Rules and Regulations* | 22 U.S.C., Chapter 46, Section 3104(c) | State Department<br>[International Investment Survey Act, Public Law 94-472, Sec. 5, Oct. 11, 1976, 90 Stat. 2062; amended by the Foreign Direct Investment and International Financial Data Improvements Act of 1990, Public Law 101-533, Sec. 6(d), (e), 7(a), Nov. 7, 1990, 104 Stat. 2349] |
| *Safeguards Information,* | 42 U.S.C, Chapter 23, Division A, Subchapter XI, Section 2167 | Department of Energy<br>[Atomic Energy Act of Aug. 1, 1946, Ch. 724, Title I, Sec. 147, as added to by Public Law 96-295, Title II, Sec. 207(a)(1), June 30, 1980, 94 Stat. 788; renumbered Title I, Public Law 102-486, Title IX, Sec. 902(a)(8), Oct. 24, 1992, 106 Stat. 2944] |
| *Safety Performance History of New Drivers; Limitation on Liability* | 49 U.S.C., Subtitle I, Chapter 5, Subchapter I, Section 508(b) | Motor Carrier<br>[Transportation Equity Act for the 21st Century, Public Law 105-178, Title IV, Sec. 4014(a)(1), June 9, 1998, 112 Stat. 409] |
| *Secrecy* | Federal Rules of Criminal Procedure, Rule 6(e) | Grand Juries |
| *Security and Law Enforcement in Property Under the Jurisdiction of the Department of Veterans Affairs* | 38 U.S.C., Chapter 9 | Department of Veterans Affairs<br>[Department of Veterans Affairs Codification Act, Public Law 102-83, Sec. 2(a), Aug. 6, 1991, 105 Stat. 397] |
| *Security and Research and Development Activities* | 49 U.S.C., Subtitle VII, Part A, Subpart i,<br>Chapter 401,<br>Section 40119(b)(1) | Federal Aviation Administration<br>[Public Law 103-272, Sec. 1(e), July 5, 1994, 108 Stat. 1117] |
| *Special Provisions Concerning the Department of Justice* | 5 U.S.C., Appendix 2, Federal Advisory Committee Act, Section 8E | Department of Justice<br>[Federal Advisory Committee Act, Public Law 92-463, Oct. 6, 1972, 86 Stat. 770; as amended by the Government in the Sunshine Act, Public Law 94-409, Sec. 5(c), Sep. 13, 1976, 90 Stat. 1247; Public Law 96-523, Sec. 2, Dec. 12, 1980, 94 Stat. 3040; and the Congressional Reports Elimination Act of 1982, Public Law 97-375, Title II, Sec. 201(c), Dec. 21, 1982, 96 Stat. 1822] |

## Table 6: Legal Information Disclosure Prohibitions

| Subject/Title of Provision | United States Code Citation | Agency/Activity [Reference] |
|---|---|---|
| *Special Provisions Concerning the Department of the Treasury* | 5 U.S.C., Federal Advisory Committee Act,<br>Section 8D | Treasury Department<br>[Federal Advisory Committee Act, Public Law 92-463, Oct. 6, 1972, 86 Stat. 770; as amended by the Government in the Sunshine Act, Public Law 94-409, Sec. 5(c), Sep. 13, 1976, 90 Stat. 1247; Public Law 96-523, Sec. 2, Dec. 12, 1980, 94 Stat. 3040; and the Congressional Reports Elimination Act of 1982, Public Law 97-375, Title II, Sec. 201(c), Dec. 21, 1982, 96 Stat. 1822] |
| *Submission of Purchase Intentions by Cigarette Manufacturers* | 7 U.S.C., Chapter 35, General Provisions, Section 1314g(c) | Department of Agriculture<br>[Agricultural Adjustment Act of 1938, Feb. 16, 1938, Ch. 30, Title III, Sec. 320A, as added to by Public Law 99-272, Title I, Sec. 1103(d), Apr. 7, 1986, 100 Stat. 88] |
| *Transition Period* | 45 U.S.C., Chapter 21, Section 1204 (b) | Department of Transportation<br>Railroads<br>[Alaska Railroad Transfer Act of 1982, Public Law 97-468, Title VI, Sec. 605(b), Jan. 14, 1983, 96 Stat. 2562, 2563] |

## Table 6: Legal Information Disclosure Prohibitions

| Subject/Title of Provision | United States Code Citation | Agency/Activity [Reference] |
|---|---|---|
| *Unauthorized Disclosure of Information* | 26 U.S.C., Subtitle F, Chapter 75, Subchapter A, Part I, Section 7213 | Treasury Department/IRS [Internal Revenue Code, Public Law 83-591, Aug. 16, 1954, Ch. 736, 68A Stat. 855; Technical Amendments Act of 1958, Public Law 85-866, Title I, Sec. 90(c), Sept. 2, 1958, 72 Stat. 1666; Social Security Amendments of 1960, Public Law 86-778, Title I, Sec. 103(s), Sept. 13, 1960, 74 Stat. 940; Tax Reform Act of 1976, Public Law 94-455, Title XII, Sec. 1202(d), (h)(3), Oct. 4, 1976, 90 Stat. 1686, 1688; Revenue Act of 1978, Public Law 95-600, Title VII, Sec. 701 (bb)(1)(C), (6), Nov. 6, 1978, 92 Stat. 2922, 2923; Food Stamp Act Amendments of 1980, Public Law 96-249, Title I, Sec. 127(a)(2)(D), May 26, 1980, 94 Stat. 366; Public Law 96-265, Title IV, Sec. 408(a)(2)(D), June 9, 1980, 94 Stat. 468, as amended; Omnibus Reconciliation Act of 1980, Public Law 96-499, Title III, Sec. 302(b), Dec. 5, 1980, 94 Stat. 2604; Social Security Act Titles IV, XVI and XVIII Amendment,<br>Pub. L. 96-611, Sec. 11(a)(4)(A), Dec. 28, 1980, 94 Stat. 3574; Tax Equity and Fiscal Responsibility Act of 1982, Pub. L. 97-248, Title III, Sec. 356(b)(2), Sept. 3, 1982, 96 Stat. 645; Debt Collection Act of 1982, Public Law 97-365, Sec. 8(c)(2), Oct. 25, 1982, 96 Stat. 1754; Deficit Reduction Act of 1984, Public Law 98-369, Div. A, Title IV, Sec. 453(b)(4), Div. B, Title VI, Sec. 2653(b)(4), July 18, 1984, 98 Stat. 820, 1156; Child Support Enforcement Amendments of 1984, Public Law 98-378, Sec. 21(f)(5), Aug. 16, 1984, 98 Stat. 1326; Family Support Act of 1988, Public Law 100-485, Title VII, Sec. 701(b)(2)(C), Oct. 13, 1988, 102 Stat. 2426; Technical and Miscellaneous Revenue Act of 1988, Public Law 100-647, Title VIII, Sec. 8008(c)(2)(B), Nov. 10, 1988, 102 Stat. 3787; Omnibus Budget Reconciliation Act of 1989, Public Law 101-239, Title VI, Sec. 6202(a)(1)(C), Dec. 19, 1989, 103 Stat. 2228; Omnibus Budget Reconciliation Act of 1990, Public Law 101-508, Title V, Sec. |

## Table 6: Legal Information Disclosure Prohibitions

| Subject/Title of Provision | United States Code Citation | Agency/Activity [Reference] |
|---|---|---|
| *Unlawful Disclosure of Information* | 49 U.S.C., Subtitle IV,<br>Part C, Chapter 161, Section 16103 | Department of Transportation<br>Pipeline Carriers<br>[ICC Termination Act of 1995, Public Law 104-88, Title I, Sec. 106(a), Dec. 29, 1995, 109 Stat. 931] |
| *Unlawful Possession or Receipt of Firearms, Federal Rules of Criminal Procedure, The Grand Jury* | 18 U.S.C., Sections 1201-1203, Sec. 16, I, Rule 6 | Courts<br>[Advisory Committee on Rules: 1944; Advisory Committee on Rules Amendment Feb. 28, 1966; Advisory Committee on Rules Amendment Apr. 24, 1972; Advisory Committee on Rules Amendments Apr. 26 and July 8, 1976 (amended by Public Law 95-78, Sec. 2(a), July 30, 1977, 91 Stat. 319); Advisory Committee on Rules Amendment Apr. 30, 1979; Advisory Committee on Rules Amendment Apr. 28, 1983; amended by Public Law 98-473, Title II, Sec. 215(f), Oct. 12, 1984, 98 Stat. 2016; Advisory Committee on Rules Amendment Apr. 29, 1985; USA Patriot Act, Pubic Law 107-56, Title II, Sec. 203(a), Oct. 26, 2001, 115 Stat. 278] |
| *Verification of Compliance* | 22 U.S.C., Chapter 35,<br>Subchapter III,<br>Section 2577d | State Department<br>[Arms Control and Disarmament Act, Public Law 87-297, Title III, Sec. 306, formerly Sec. 37, as added to by Arms Control and Disarmament Act Amendments, Public Law 95-108, Sec. 4, Aug. 17, 1977, 91 Stat. 871; amended by Arms Control and Nonproliferation Act of 1994, Public Law 103-236, Title VII, Sec. 712, Apr. 30, 1994, 108 Stat. 495 renumbered Sec. 306 and amended by Public Law 105-277, Div. G, Subdiv. A, title XII, Sec. 1223(11), (21), Oct. 21, 1998, 112 Stat. 2681-770, 2681-772] |

## Table 6: Legal Information Disclosure Prohibitions

| Subject/Title of Provision | United States Code Citation | Agency/Activity [Reference] |
|---|---|---|
| *Voluntary Disclosure of Customer Communications or Records* | 18 U.S.C., Part I, Chapter121, Section 2702 | [Electronic Communications Privacy Act of 1986, Public Law 99-508, Title II, Sec. 201((a)), Oct. 21, 1986, 100 Stat. 1860; amended by Public Law 100-690, Title VII, Sec. 7037, Nov. 18, 1988, 102 Stat. 4399; Protection of Children From Sexual Predators Act of 1998, Public Law 105-314, Title VI, Sec. 604(b), Oct. 30, 1998, 112 Stat. 2984; and the USA Patriot Act, Public Law 107-56, title II, Sec. 212(a)(1), Oct. 26, 2001, 115 Stat. 284] |
| *Written Evaluations* | 12 U.S.C., Chapter 30, Section 2906 | Treasury Department/ Comptroller of the Currency/ Federal Reserve System/ Federal Deposit Insurance Corporation [Housing and Community Development Act, Public Law 95-128, Title VIII, Sec. 807, as added to by the Financial Institutions Reform, Recovery, and Enforcement Act of 1989, Public Law 101-73, Title XII, Sec. 1212(b), Aug. 9, 1989, 103 Stat. 527 and amended by the Foreign Bank Supervision Enhancement Act of 1991, Public Law 102-242, Title II, Sec. 222, Dec. 19, 1991, 105 Stat. 2306] |
| *Wrongful Disclosure of Information* | 13 U.S.C., Chapter 7, Subchapter I, Section 214 | Census Bureau<br>Census Information<br>[Census Act, Aug. 31, 1954, Ch. 1158, 68 Stat. 1023;<br>Public Law 94-521, Sec. 12(a), Oct. 17, 1976, 90 Stat. 2464; and the Census Address List Improvement Act of 1994, Public Law 103-430, Sec. 2(c), Oct. 31, 1994, 108 Stat. 4394] |
| *Wrongful Disclosure of Individually Identifiable Health Information* | 42 U.S.C., Chapter 7, Subchapter XI, Section 1320d-6 | [Social Security Act of Aug. 14, 1935, Ch. 531, Title XI, Sec. 1177, as added to by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, Title II, Sec. 262(a), Aug. 21, 1996, 110 Stat. 2029] |

**Table 6: Legal Information Disclosure Prohibitions**

| Subject/Title of Provision | United States Code Citation | Agency/Activity [Reference] |
|---|---|---|
| *Wrongful Disclosure of Video Tape Rental or Sale Records* | 18 U.S.C., Part 1, Chapter 121, Section 2710 | [Video Privacy Protection Act of 1988, Public Law 100-618, Sec. 2(a)(2), Nov. 5, 1988, 102 Stat. 3195] |

## E.2 Executive Mandates

### E.2.1 Office of Management and Budget Memoranda and Guidelines

(a) Appendix III to OMB Circular No. A-130 of February 1996
Subject: Security of Federal Automated Information Resources
[See text at http://csrc.nist.gov/secplcy/a130app3.txt.]

(b) OMB Memorandum of November 3, 1997
MEMORANDUM FOR THE CHIEF INFORMATION SECURITY OFFICERS
Subject: Privacy Act Responsibilities for Implementing the Personal Responsibility and Work Opportunity Reconciliation Act of 1996
[See text at http://www.whitehouse.gov/omb/inforeg/infopoltech.html.]

(c) OMB M-99-05 of January 7, 1999
MEMORANDUM FOR HEADS OF DEPARTMENTS AND AGENCIES
Subject: Instructions on complying with President's Memorandum of May 14, 1998, "Privacy and Personal Information in Federal Records"
[See text at http://www.whitehouse.gov/omb/memoranda/m99-05.html.]

(d) OMB M-99-18 of June 2, 1999
MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES
Subject: Privacy Policies on Federal Web Sites
[See text at http://csrc.nist.gov/policies/privacypol.pdf.]

> Federal agencies must protect an individual's right to privacy when they collect personal information. This is required by the Privacy Act, 5 U.S.C. 552a, and OMB Circular No. A-130, "Management of Federal Information Resources," 61 Fed. Reg. 6428 (Feb. 20, 1996), and supported by the *Principles for Providing and Using Personal Information* published by the Information Infrastructure Task Force on June 6, 1995. Posting a privacy policy helps ensure that individuals have notice and choice about, and thus confidence in, how their personal information is handled when they use the Internet.

(e) OMB M-99-20 of June 23, 1999
MEMORANDUM FOR THE HEADS OF DEPARTMENTS AND AGENCIES
Subject: Security of Federal Automated Information Resources
[See text at http://www.whitehouse.gov/omb/memoranda/m99-20.html.]

(f) OMB M-00-13 of June 22, 2000
MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES
Subject: Privacy Policies and Data Collection on Federal Web Sites
[See text at http://www.whitehouse.gov/omb/memoranda/m00-13.html.]

(g) OMB M-00-15 of September 25, 2000
MEMORANDUM FOR THE HEADS OF DEPARTMENTS AND AGENCIES
Subject: OMB Guidance on Implementing the Electronic Signatures in Global and National Commerce Act
[Text at http://www.whitehouse.gov/omb/memoranda/m00-15.html affects integrity impact determinations.]

(h) OMB M-01-05 of December 20, 2000
MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES
Subject: Guidance on Inter-agency Sharing of Personal Data – Protecting Personal Privacy
[Text at http://www.whitehouse.gov/omb/memoranda/m01-05.html.]

(i) OMB M-01-08 of January 16, 2001
MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES
Subject: Guidance on Implementing the Government Information Security Reform Act
[Text at http://csrc.nist.gov/policies/actmemo-guid.pdf.]

(j) OMB Memorandum of October 15, 2001
MEMORANDUM TO CHIEF INFORMATION OFFICERS AND PROGRAM
Subject: Guidance on the Release of Security Act Reports
[See text at http://csrc.nist.gov/policies/memo-ciopo.txt.]

(k) OMB Guideline of February 22, 2002
Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated By Federal Agencies (*Federal Register*, Notices, Vol. 67, No. 36, 8452)
[See text at http://www.whitehouse.gov/omb/fedreg/reproducible2.pdf.]

(l) OMB M-03-18 of August 1, 2003
MEMORANDUM TO ALL DEPARTMENT AND AGENCY HEADS
Subject: Implementation Guidance for the E-Government Act of 2002
[See especially text referring to information security and to privacy at http://www.whitehouse.gov/omb/memoranda/m03-18.pdf]

(m) OMB M-03-19 of August 6, 2003
MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES
Subject: Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting

[See text at http://www.whitehouse.gov/omb/memoranda/m03-19.pdf]

(n) OMB M-03-22 of September 26, 2003
MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES
Subject: OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002
[See text at http://www.whitehouse.gov/omb/memoranda/m03-22.html]

(o) OMB M-04-04 of December 16, 2003
MEMORANDUM TO THE HEADS OF ALL DEPARTMENTS AND AGENCIES
Subject: E-Authentication Guidance for Federal Agencies
[Text at http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf may affect integrity impact determination.]

(p) OMB CIRCULAR NO. A-130, Revised, (Transmittal Memorandum No. 4) of April 14, 2004
MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES
Subject: Management of Federal Information Resources
[See http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html. Note especially the privacy requirements in Appendix I.]

(q) OMB M-04-15 of June 17, 2004
MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES
Subject: Development of Homeland Security Presidential Directive (HSPD) – 7 Critical Infrastructure Protection Plans to Protect Federal Critical Infrastructures and Key Resources
[See text at http://www.whitehouse.gov/omb/memoranda/fy2004/m04-15.pdf]

(r) OMB M-04-25 of August 23, 2004
MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES
Subject: FY 2004 Reporting Instructions for the Federal Information Security Management Act
[See text at http://www.whitehouse.gov/omb/memoranda/fy2004/m04-25.pdf]

(s) OMB M-05-15 of June 13, 2005
MEMORANDUM FOR THE HEADS OF DEPARTMENTS AND AGENCIES
Subject: FY 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management
[See text at http://www.whitehouse.gov/omb/memoranda/fy2005/m05-15.pdf]

(t) OMB M-05-24 of August 5, 2005
MEMORANDUM FOR THE HEADS OF ALL DEPARTMENTS AND AGENCIES
Subject: Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors
[See text at http://www.whitehouse.gov/omb/memoranda/fy2005/m05-24.pdf]

(u) OMB M-06-02 of December 16, 2005

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES
Subject: Improving Public Access to and Dissemination of Government Information and Using the Federal Enterprise Architecture Data Reference Model
[See text at http://www.whitehouse.gov/omb/memoranda/fy2006/m06-02.pdf]

(v) OMB M-06-04 of December 30, 2005
MEMORANDUM FOR HEADS OF DEPARTMENT AND AGENCIES
Subject: Implementation of the President's Executive Order "Improving Agency Disclosure of Information"
[See text at http://www.whitehouse.gov/omb/memoranda/fy2006/m06-04.pdf]

(w) OMB M-06-12 of April 13, 2006
MEMORANDUM FOR HEADS OF DEPARTMENT AND AGENCIES
Subject: Follow-up Memorandum on "Implementation of the President's Executive Order 'Improving Agency Disclosure of Information'"
[See text at http://www.whitehouse.gov/omb/memoranda/fy2006/m06-12.pdf

(x) OMB M-06-15 of May 22, 2006
MEMORANDUM FOR THE HEADS OF DEPARTMENTS AND AGENCIES
Subject: Safeguarding Personally Identifiable Information
[See text at http://www.whitehouse.gov/omb/memoranda/fy2006/m06-15.pdf]

(y) OMB M-06-16 of June 23, 2006
MEMORANDUM FOR THE HEADS OF DEPARTMENTS AND AGENCIES
Subject: Protection of Sensitive Agency Information
[See text at http://www.whitehouse.gov/omb/memoranda/fy2006/m06-16.pdf]

(z) OMB M-06-19 of July 12, 2006
MEMORANDUM FOR CHIEF INFORMATION OFFICERS
Subject: Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments
[See text at http://www.whitehouse.gov/omb/memoranda/fy2006/m06-19.pdf]

(aa) OMB M-06-20 of July 17, 2006
MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES
Subject: FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management
[See text at http://www.whitehouse.gov/omb/memoranda/fy2006/m06-20.pdf

(bb) OMB M-06-25 of August 22, 2006
MEMORANDUM FOR CHIEF INFORMATION OFFICERS
Subject: FY 2006 E-Government Act Reporting Instructions
[See text at http://www.whitehouse.gov/omb/memoranda/fy2006/m06-25pdf]

(cc) OMB Recommendation of September 20, 2006

MEMORANDUM FOR HEADS OF DEPARTMENTS AND AGENCIES
Subject: Recommendations for Identity Theft Related Data Breach Notification
[See text at
http://www.whitehouse.gov/omb/memoranda/fy2006/task_force_theft_memo.pdf]

(dd) OMB M-07-16 of May 22, 2007
MEMORANDUM FOR THE HEADS OF EXECUT IVE DEPARTMENTS AND AGENCIES
Subject: Safeguarding Against and Responding to the Breach of Personally Identifiable Information
[See text at: http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf]

(ee) OMB M-07-19 of July 25, 2007
MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES
Subject: FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management
[See text at http://www.whitehouse.gov/omb/memoranda/fy2007/m07-19.pdf]

### E.2.2 Presidential Directives and Executive Orders

(a) Executive Order 10450 of April 27, 1953
SECURITY REQUIREMENTS FOR GOVERNMENT EMPLOYEES
[EO 10450, Apr. 27, 1953, 18 F.R. 2489, as amended by Ex. Ord. No. 10491, Oct. 15, 1953, 18 F.R. 6583; Ex. Ord. No. 10531, May 27, 1954, 19 F.R. 3069; Ex. Ord. No. 10548, Aug. 3, 1954, 19 F.R. 4871; Ex. Ord. No. 10550, Aug. 6, 1954, 19 F.R. 4981; Ex. Ord. No. 11605, July 2, 1971, 36 F.R. 12831; Ex. Ord. No. 11785, June 4, 1974, 39 F.R. 20053; Ex. Ord. No. 12107, Dec. 28, 1978, 44 F.R. 1055]
[See http://www.dss.mil/nf/adr/10450/eo10450F.htm.]

> Section 8 (a) The investigations conducted pursuant to this order shall be designed to develop information as to whether the employment or retention in employment in the Federal service of the person being investigated is clearly consistent with the interests of the national security. Such information shall relate, but shall not be limited, to the following:
>
> > (6) Intentional unauthorized disclosure to any person of security information, or of other information disclosure of which is prohibited by law, or willful violation or disregard of security regulations.

(b) Executive Order 12046 of March 27, 1978
RELATING TO THE TRANSFER OF TELECOMMUNICATIONS FUNCTIONS
[See http://www.archives.gov/federal_register/codification/executive_order/12046.html.]

> 2-405. The Secretary of Commerce shall provide for the coordination of the telecommunications activities of the Executive Branch, and shall assist in the formulation of policies and standards for those activities, including but not limited to considerations of interoperability, privacy, security, spectrum use and emergency readiness.

(c) Executive Order 12656 of November 18, 1988

ASSIGMMENT OF EMERGENCY PREPAREDNESS RESPONSIBILITIES

[See http://www.archives.gov/federal_register/codification/executive_order/12656.html. Amended by: EO 13074, February 9, 1998; EO 13228, October 8, 2001; EO 13286, February 28, 2003]

Sec. 201. *General.* The head of each Federal department and agency, as appropriate, shall:

(12) Ensure a capability to provide, during a national security emergency, information concerning Acts of Congress, presidential proclamations, Executive orders, regulations, and notices of other actions to the Archivist of the United States, for publication in the Federal Register, or to each agency designated to maintain the Federal Register in an emergency.

Sec. 701. *Lead Responsibilities.* In addition to the applicable responsibilities covered in Parts 1 and 2, the Secretary of Energy shall:

(1) Conduct national security emergency preparedness planning, including capabilities development, and administer operational programs for all energy, resources, including:

(a) Providing information, in cooperation with Federal, State, and energy industry officials, on energy supply and demand conditions and on the requirements for and the availability of materials and services critical to energy supply systems.

Sec. 1101. *Lead Responsibilities.* In addition to the applicable responsibilities covered in Parts 1 and 2, the Attorney General of the United States shall:

(6) Provide information and assistance to the Federal Judicial branch and the Federal Legislative branch concerning law enforcement, continuity of government, and the exercise of legal authority during national security emergencies.

Sec. 1802. *Support Responsibility.* The Administrator of General Services shall develop plans to assist Federal departments and agencies in operation and maintenance of essential automated information processing facilities during national security emergencies.

(d) Executive Order 12812 of July 22, 1992

DECLASSIFICATION AND RELEASE OF MATERIALS PERTAINING TO PRISONERS OF WAR AND MISSING IN ACTION

[See http://www.dtic.mil/dpmo/foia/eo12812.htm.]

Sec. 2. All executive departments and agencies shall make publicly available documents, files, and other materials declassified pursuant to section 1, except for those the disclosure of which would constitute a clearly unwarranted invasion of personal privacy of returnees, family members of POWs and MIAs, or other persons, or would impair the deliberative processes of the executive branch.

(e) Presidential Decision Directive PDD/NSC-12 of August 5, 1993

Subject: Security Awareness and Reporting of Foreign Contacts
[See http://www.usaid.gov/policy/ads/500/pdd-nsc-12.pdf.]

Presidential Decision Directive/NSC-12 requires that government employees report all contacts with individuals of any nationality, either within or outside the scope of the employee's official activities, in which:

- Illegal or unauthorized access is sought to classified or otherwise sensitive information.
- The employee is concerned that he/she may be the target of actual or attempted exploitation by a foreign entity.

Government employees must immediately report any discussion in which someone asks them to provide sensitive information which they are not authorized to receive. If in doubt, the agency Security Office has or knows personnel that are available to assess information and determine if a potential counterintelligence threat exists.

(f) Executive Order 12951 of February 24, 1995
RELEASE OF IMAGERY ACQUIRED BY SPACE-BASED NATIONAL INTELLIGENCE RECONNAISSANCE SYSTEMS
[See http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=1995_register&docid=fr28fe95-133.pdf.]

Section 1. Public Release of Historical Intelligence
Imagery. Imagery acquired by the space-based national intelligence reconnaissance systems known as the Corona, Argon, and Lanyard missions shall, within 18 months of the date of this order, be declassified and transferred to the National Archives and Records Administration with a copy sent to the United States Geological Survey of the Department of the Interior consistent with procedures approved by the Director of Central Intelligence and the Archivist of the United States. Upon transfer, such imagery shall be deemed declassified and shall be made available to the public.

Section. 3. General Provisions. (a) This order prescribes a comprehensive and exclusive system for the public release of imagery acquired by space-based national intelligence reconnaissance systems. This order is the exclusive Executive order governing the public release of imagery for purposes of section 552(b)(1) of the Freedom of Information Act.

(g) Executive Order 12958 of April 17, 1995
CLASSIFIED NATIONAL SECURITY INFORMATION
[See http://www.whitehouse.gov/news/releases/2003/03/20030325-11.html.]

Section 3.7. Processing Requests and Reviews. In response to a request for information under the Freedom of Information Act, the Privacy Act of 1974, or the mandatory review provisions of this order, or pursuant to the automatic declassification or systematic review provisions of this order:

(a) An agency may refuse to confirm or deny the existence or nonexistence of requested information whenever the fact of its existence or nonexistence is itself classified under this order.

(b) When an agency receives any request for documents in its custody that contain information that was originally classified by another agency, or comes across such documents in the process of the automatic declassification or systematic review provisions of this order, it shall refer copies of any request and the pertinent documents to the originating agency for processing, and may, after consultation with the originating agency, inform any requester of the referral unless such association is itself classified under this order. In cases in which the originating agency determines in writing that a response under paragraph (a), above, is required, the referring agency shall respond to the requester in accordance with that paragraph.

(h) Executive Order 12968 of August 4, 1995
ACCESS TO CLASSIFIED INFORMATION
[See http://www.dss.mil/seclib/eo12968.htm.]

Section 5.2. Review Proceedings for Denials or Revocations of Eligibility for Access.
(a) Applicants and employees who are determined to not meet the standards for access to classified information established in section 3.1 of this order shall be:

(1) provided as comprehensive and detailed a written explanation of the basis for that conclusion as the national security interests of the United States and other applicable law permit; provided within 30 days, upon request and to the extent the documents would be provided if requested under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act (3 U.S.C. 552a), as applicable, any documents, records, and reports upon which a denial or revocation is based.

(i) Presidential Decision Directive PDD 63 of May 22, 1998
Subject: The Clinton Administration’s Policy on Critical Infrastructure Protection
[See text in http://csrc.nist.gov/policies/paper598.pdf.]

(j) Presidential Decision Directive PDD/NSC 66 of September 16, 1998
Subject: Encryption Policy
[See text in http://fas.org/irp/offdocs.]

(k) MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES of March 3, 2000
Subject: Action by Federal Agencies to Safeguard Against Internet Attacks
[See http://csrc.nist.gov/policies/Wh3300Memo.txt.]

(l) Executive Order 13228 of October 8, 2001
ESTABLISHING THE OFFICE OF HOMELAND SECURITY AND THE HOMELAND SECURITY COUNCIL
[See http://www.whitehouse.gov/news/releases/2001/10/20011008-2.html.]

(e) Protection. The Office shall coordinate efforts to protect the United States and its critical infrastructure from the consequences of terrorist attacks. In performing this function, the Office shall work with Federal, State, and local agencies, and private entities, as appropriate, to: …

(ii) coordinate efforts to protect critical public and privately owned information systems within the United States from terrorist attack;

(f) Response and Recovery. The Office shall coordinate efforts to respond to and promote recovery from terrorist threats or attacks within the United States. In performing this function, the Office shall work with Federal, State, and local agencies, and private entities, as appropriate, to: …

(ii) coordinate efforts to ensure rapid restoration of public and private critical information systems after disruption by a terrorist threat or attack;

(m) Executive Order 13231 of October 16, 2001
CRITICAL INFRASTRUCTURE PROTECTION IN THE INFORMATION AGE
[See http://csrc.nist.gov/policies/cip-infoage.html.]

(n) Executive Order 13233 of November 1, 2001
FURTHER IMPLEMENTATION OF THE PRESIDENTIAL RECORDS ACT
[See http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=2001_register&docid=fr05no01-104.pdf.]

(o) Military Order of November 13, 2001
DETENTION, TREATMENT, AND TRIAL OF CERTAIN NON-CITIZENS IN THE WAR AGAINST TERRORISM
[See http://www.whitehouse.gov/news/releases/2001/11/20011113-27.html.]

Section 4. Authority of the Secretary of Defense Regarding Trials of Individuals Subject to this Order.

(c) Orders and regulations issued under subsection (b) of this section shall include, but not be limited to, rules for the conduct of the proceedings of military commissions, including pretrial, trial, and post-trial procedures, modes of proof, issuance of process, and qualifications of attorneys, which shall at a minimum provide for--

(4) in a manner consistent with the protection of information classified or classifiable under Executive Order 12958 of April 17, 1995, as amended, or any successor Executive Order, protected by statute or rule from unauthorized disclosure, or otherwise protected by law, (A) the handling of, admission into

evidence of, and access to materials and information, and (B) the conduct, closure of, and access to proceedings;

(p) Executive Order 13284 of January 23, 2003
AMENDMENT OF EXECUTIVE ORDERS, AND OTHER ACTIONS, IN CONNECTION WITH THE ESTABLISHMENT OF THE DEPARTMENT OF HOMELAND SECURITY
[See http://www.state.gov/documents/organization/22978.doc.]

Section 19. Functions of Certain Officials in the Department of Homeland Security.

The Secretary of Homeland Security, the Deputy Secretary of Homeland Security, the Under Secretary for Information Analysis and Infrastructure Protection, Department of Homeland Security, and the Assistant Secretary for Information Analysis, Department of Homeland Security, each shall be considered a "Senior Official of the Intelligence Community" for purposes of Executive Order 12333, and all other relevant authorities, and shall:

(a) recognize and give effect to all current clearances for access to classified information held by those who become employees of the Department of Homeland Security by operation of law pursuant to the Homeland Security Act of 2002 or by Presidential appointment;
(b) recognize and give effect to all current clearances for access to classified information held by those in the private sector with whom employees of the Department of Homeland Security may seek to interact in the discharge of their homeland security-related responsibilities;
(c) make all clearance and access determinations pursuant to Executive Order 12968 of August 2, 1995, or any successor Executive Order, as to employees of, and applicants for employment in, the Department of Homeland Security who do not then hold a current clearance for access to classified information; and
(d) ensure all clearance and access determinations for those in the private sector with whom employees of the Department of Homeland Security may seek to interact in the discharge of their homeland security- related responsibilities are made in accordance with Executive Order 12829 of January 6, 1993.

(q) Executive Order 13286 of February 28, 2003
AMENDMENT OF EXECUTIVE ORDERS, AND OTHER ACTIONS, IN CONNECTION WITH THE TRANSFER OF CERTAIN FUNCTIONS TO THE SECRETARY OF HOMELAND SECURITY
[See http://www.whitehouse.gov/news/releases/2003/02/20030228-8.html.]

Section 7. Executive Order 13231 of October 16, 2001 ("Critical Infrastructure Protection in the Information Age"), as amended: see Executive Order for text.

Section 1.4. Classification Categories. Information shall not be considered for classification unless it concerns:
(a) military plans, weapons systems, or operations;

(b) foreign government information;
(c) intelligence activities (including special activities), intelligence sources or methods, or cryptology;
(d) foreign relations or foreign activities of the United States, including confidential sources;
(e) scientific, technological, or economic matters relating to the national security, which includes defense against transnational terrorism;
(f) United States Government programs for safeguarding nuclear materials or facilities;
(g) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism; or
(h) weapons of mass destruction.

(r) EXECUTIVE ORDER 13292 of March 25, 2003
FURTHER AMENDMENT TO EXECUTIVE ORDER 12958, AS AMENDED, CLASSIFIED NATIONAL SECURITY INFORMATION
[See http://foia.state.gov/eo12958/EO13292.asp.]

Section 1.7. Classification Prohibitions and Limitations.

(a) In no case shall information be classified in order to:
(1) conceal violations of law, inefficiency, or administrative error;
(2) prevent embarrassment to a person, organization, or agency;
(3) restrain competition; or
(4) prevent or delay the release of information that does not require protection in the interest of the national security.

(b) Basic scientific research information not clearly related to the national security shall not be classified.

(c) Information may be reclassified after declassification and release to the public under proper authority only in accordance with the following conditions:
(1) the reclassification action is taken under the personal authority of the agency head or deputy agency head, who determines in writing that the reclassification of the information is necessary in the interest of the national security;
(2) the information may be reasonably recovered; and
(3) the reclassification action is reported promptly to the Director of the Information Security Oversight Office.

(d) Information that has not previously been disclosed to the public under proper authority may be classified or reclassified after an agency has received a request for it under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act of 1974 (5 U.S.C. 552a), or the mandatory review provisions of section 3.5 of this order only if such classification meets the requirements of this order and is accomplished on a document-by-document basis with the personal participation or under the direction of the agency head, the deputy agency head, or the senior agency official designated under section 5.4 of this order.

(e) Compilations of items of information that are individually unclassified may be classified if the compiled information reveals an additional association or relationship that: (1) meets the standards for classification under this order; and (2) is not otherwise revealed in the individual items of information. As used in this order, "compilation" means an aggregation of pre-existing unclassified items of information.

Section 1.8. Classification Challenges.

(a) Authorized holders of information who, in good faith, believe that its classification status is improper are encouraged and expected to challenge the classification status of the information in accordance with agency procedures established under paragraph (b) of this section.

(b) In accordance with implementing directives issued pursuant to this order, an agency head or senior agency official shall establish procedures under which authorized holders of information are encouraged and expected to challenge the classification of information that they believe is improperly classified or unclassified. These procedures shall ensure that:

(1) individuals are not subject to retribution for bringing such actions;
(2) an opportunity is provided for review by an impartial official or panel; and
(3) individuals are advised of their right to appeal agency decisions to the Interagency Security Classification Appeals Panel (Panel) established by section 5.3 of this order.

(s) Executive Order 13311 of July 29, 2003
HOMELAND SECURITY INFORMATION SHARING
[See http://a257.g.akamaitech.net/7/257/2422/14mar20010800/edocket.access.gpo.gov/2003/pdf/03-19675.pdf.]

Section 1. Assignment of Functions.

(a) The functions of the President under section 892 of the Act are assigned to the Secretary of Homeland Security (the "Secretary"), except the functions of the President under subsections 892(a)(2) and 892(b)(7).

(f) A determination, under the procedures issued by the Secretary in the performance of the function of the President under section 892(a)(1) of the Act, as to whether, or to what extent, an individual who falls within the category of "State and local personnel" as defined in sections 892(f)(3) and (f)(4) of the Act shall have access to information classified pursuant to Executive Order 12958 of April 17, 1995, as amended, is a discretionary determination and shall be conclusive and not subject to review or appeal.

(t) Homeland Security Presidential Directive/HSPD-6 of September 16, 2003
Subject: Integration and Use of Screening Information
[See http://www.whitehouse.gov/news/releases/2003/09/20030916-5.html.]

> (2) The heads of executive departments and agencies shall, to the extent permitted by law, provide to the Terrorist Threat Integration Center (TTIC) on an ongoing basis all appropriate Terrorist Information in their possession, custody, or control. The Attorney General, in coordination with the Secretary of State, the Secretary of Homeland Security, and the Director of Central Intelligence shall implement appropriate procedures and safeguards with respect to all such information about United States persons. The TTIC will provide the organization referenced in paragraph (1) with access to all appropriate information or intelligence in the TTIC's custody, possession, or control that the organization requires to perform its functions.

(u) Homeland Security Presidential Directive / HSPD-7 of December 17, 2003
Subject: Critical Infrastructure Identification, Prioritization, and Protection
[See http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html.]

> (10) Federal departments and agencies will appropriately protect information associated with carrying out this directive, including handling voluntarily provided information and information that would facilitate terrorist targeting of critical infrastructure and key resources consistent with the Homeland Security Act of 2002 and other applicable legal authorities.
>
> (22) (f) The Office of Management and Budget (OMB) shall oversee the implementation of government-wide policies, principles, standards, and guidelines for Federal government computer security programs. The Director of OMB will ensure the operation of a central Federal information security incident center consistent with the requirements of the Federal Information Security Management Act of 2002.
>
> (24) All Federal department and agency heads are responsible for the identification, prioritization, assessment, remediation, and protection of their respective internal critical infrastructure and key resources. Consistent with the Federal Information Security Management Act of 2002, agencies will identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information.

### E.2.3 Other EOP Guidance

(a) MEMORANDUM FOR THE HEADS OF DEPARTMENTS AND AGENCIES of February 22, 2000
Subject: Security of Federal Information Systems
[See http://csrc.nist.gov/policies/cos-memo.html.]

(b) MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES of March 19, 2002
Subject: Action to Safeguard Information Regarding Weapons of Mass Destruction and Other Sensitive Documents Related to Homeland Security
[See http://csrc.nist.gov/policies/guidance-homelandsec.html.]

(c) MEMORANDUM FOR DEPARTMENTS AND AGENCIES of March 19, 2002
Subject: Safeguarding Information Regarding Weapons of Mass Destruction and Other Sensitive Records Related to Homeland Security
[See http://csrc.nist.gov/policies/guidance-homelandsec.html.]

> III. Sensitive But Unclassified Information
>
> In addition to information that could reasonably be expected to assist in the development or use of weapons of mass destruction, which should be classified or reclassified as described in Parts I and II above, departments and agencies maintain and control sensitive information related to America's homeland security that might not meet one or more of the standards for classification set forth in Part 1 of Executive Order 12958. The need to protect such sensitive information from inappropriate disclosure should be carefully considered, on a case-by-case basis, together with the benefits that result from the open and efficient exchange of scientific, technical, and like information.
>
> All departments and agencies should ensure that in taking necessary and appropriate actions to safeguard sensitive but unclassified information related to America's homeland security, they process any Freedom of Information Act request for records containing such information in accordance with the Attorney General's FOIA Memorandum of October 12, 2001, by giving full and careful consideration to all applicable FOIA exemptions. See FOIA Post, "New Attorney General FOIA Memorandum Issued" (posted 10/15/01) (found at http://www.usdoj.gov/oip/foiapost/2001foiapost19.htm), which discusses and provides electronic links to further guidance on the authority available under Exemption 2 of the FOIA, 5 U.S.C. § 552(b)(2), for the protection of sensitive critical infrastructure information. In the case of information that is voluntarily submitted to the Government from the private sector, such information may readily fall within the protection of Exemption 4 of the FOIA, 5 U.S.C. § 552(b)(4).

## E.3 OMB and Case Law Interpretations

The disclosure prohibitions, as stated in law are often imprecise. As a result, Office of Management and Budget and case law interpretations are sometimes necessary to clarify the prohibitions. In some cases, the analyst may need to identify such clarifications and interpretations.

One law imposing disclosure prohibitions that has received particular attention across the Federal government deserves special attention. The Privacy Act of 1974, 5 U.S.C. § 552a (2000), which has been in effect since September 27, 1975, can generally be characterized as an omnibus "code of fair information practices" that attempts to regulate the collection, maintenance, use, and dissemination of personal information by federal executive branch agencies. However, the Act's imprecise language, limited legislative history, and somewhat outdated regulatory guidelines have rendered it a difficult statute to decipher and apply. Moreover, even after more than twenty-five years of administrative and judicial analysis, numerous Privacy Act issues remain unresolved or unexplored. Adding to these interpretational difficulties is the fact that many Privacy Act cases are unpublished district court decisions.

A primary element of the Privacy Act of 1974 is the “no disclosure without consent” rule: *No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains [subject to 12 exceptions]." 5 U.S.C. § 552a(b).*

Note that a "disclosure" can be by any means of communication - written, oral, electronic, or mechanical. [See OMB Guidelines, 40 Fed. Reg. 28,948, 28,953 (1975).]
Details of the Privacy Act of 1974, together with OMB and judicial interpretations can be found on the Department of Justice web site, http://www.usdoj.gov/04foia/04_7_1.html.

Subsection (v) of the Privacy Act requires the Office of Management and Budget (OMB) to: (1) "prescribe guidelines and regulations for the use of agencies in implementing" the Act; and (2) "provide continuing assistance to and oversight of the implementation" of the Act by agencies. 5 U.S.C. § 552a(v). The vast majority of OMB's Privacy Act Guidelines (OMB Guidelines) are published at 40 Fed. Reg. 28,948-78 (1975). However, these original guidelines have been supplemented in particular subject areas over the years. 40 Fed. Reg. 56,741-43 (1975) (system of records definition, routine use and intra-agency disclosures, consent and congressional inquiries, accounting of disclosures, amendment appeals, rights of parents and legal guardians, relationship to Freedom of Information Act (FOIA)); 48 Fed. Reg. 15,556-60 (1983) (relationship to Debt Collection Act); 52 Fed. Reg. 12,990-93 (1987) ("call detail" programs); 54 Fed. Reg. 25818-29 (1989) (computer matching); 56 Fed. Reg. 18,599-601 (proposed Apr. 23, 1991) (computer matching); 61 Fed. Reg. 6428, 6435-39 (1996) ("Federal Agency Responsibilities for Maintaining Records About Individuals").

As a general rule, the OMB Guidelines are entitled to the deference usually accorded the interpretations of the agency that has been charged with the administration of a statute. *Quinn v. Stone*, 978 F.2d 126, 133 (3d Cir. 1992); *Baker v. Dep't of the Navy*, 814 F.2d 1381, 1383 (9th Cir. 1987); *Perry v. FBI*, 759 F.2d 1271, 1276 n.7 (7th Cir. 1985) (citing *Bartel v. FAA*, 725 F.2d 1403, 1408 n.9 (D.C. Cir. 1984); *Albright v. United States*, 631 F.2d 915, 919 n.5 (D.C. Cir. 1980)), *rev'd en banc on other grounds*, 781 F.2d 1294 (7th Cir. 1986); *Smiertka v. United States Dep't of the Treasury*, 604 F.2d 698, 703 n.12 (D.C. Cir. 1979); *Rogers v. United States Dep't of Labor*, 607 F. Supp. 697, 700 n.2 (N.D. Cal. 1985); *Sanchez v. United States*, 3 Gov't Disclosure Serv. (P-H) ¶ 83,116, at 83,709 (S.D. Tex. Sept. 10, 1982); *Golliher v. United States Postal Serv.*, 3 Gov't Disclosure Serv. (P-H) ¶ 83,114, at 83,703 (N.D. Ohio June 10, 1982); *Greene v. VA*, No. C-76-461-S, slip op. at 6-7 (M.D.N.C. July 3, 1978); *Daniels v. FCC*, No. 77-5011, slip op. at 8-9 (D.S.D. Mar. 15, 1978); see also *Martin v. Office of Special Counsel*, 819 F.2d 1181, 1188 (D.C. Cir. 1987) (OMB interpretation is "worthy of our attention and solicitude"). However, a few courts have rejected particular aspects of the OMB Guidelines as inconsistent with the statute. *Kassel v. VA*, No. 87-217-S, slip op. at 24-25 (D.N.H. Mar. 30, 1992) (subsection (e)(3)); *Saunders v. Schweiker*, 508 F. Supp. 305, 309 (W.D.N.Y. 1981) (same); *Metadure Corp. v. United States*, 490 F. Supp. 1368, 1373-74 (S.D.N.Y. 1980) (subsection (a)(2)); *Fla. Med. Ass'n v. HEW*, 479 F. Supp. 1291, 1307-11 (M.D. Fla. 1979) (same); *Zeller v. United States*, 467 F. Supp. 487, 497-99 (E.D.N.Y. 1979) (same).

Additionally, OMB has issued guidance regarding implementation of the privacy provisions of the E-Government Act of 2002 (See Section 208 of Public Law 107-347, 44 U.S.C. Chapter 36). Section 208 of the E-Government Act of 2002 requires that OMB issue guidance to agencies on implementing the privacy provisions of the E-Government Act. M-03-22, the September 26, 2003 Memorandum for Heads of Executive Departments and Agencies, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, complies with this requirement (see http://www.whitehouse.gov/omb/memoranda/m03-22.html). M-03-22 also provides a general outline of regulatory requirements pursuant to the Children's Online Privacy Protection Act ("COPPA") and a summary of modifications to existing guidance. A complete list of OMB privacy guidance currently in effect is available at OMB's website.