January 2005

ITL Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

INTEGRATING IT SECURITY INTO THE CAPITAL PLANNING AND INVESTMENT CONTROL PROCESS

By Joan S. Hash, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology

Introduction

To assist federal agencies with effectively integrating security into the capital planning and investment control (CPIC) process, NIST's Information Technology Laboratory has released Special Publication (SP) 800-65, *Integrating IT Security into the Capital Planning and Investment Control Process*. It provides tips and pointers in addition to a sample methodology, which can be used to address prioritization of security requirements in support of agency business units. The publication describes risk factors that should be considered in addressing security investments and links the current Office of Management and Budget (OMB) guidance in this area to the current Federal Information Security Management Act (FISMA), including the Plan of Action and Milestones (POA&M) process that all agencies are required to implement. This ITL Bulletin summarizes NIST SP 800-65.

Background

Traditionally, information technology (IT) security and capital planning and investment control (CPIC) processes have been performed independently by security and capital planning practitioners. However, the Federal Information Security Management Act (FISMA) of 2002 and other existing federal regulations charge agencies with integrating the two activities. In addition, with increased competition for limited federal budgets and resources, agencies must ensure that available funding is applied towards the agencies' highest-priority IT security investments. Applying funding towards high-priority security investments supports the objective of maintaining appropriate security controls, both at the enterprise-wide and system level, commensurate with levels of risk and data sensitivity. This special publication introduces common criteria against which agencies can prioritize security activities to ensure that corrective actions identified in the annual FISMA reporting process are incorporated into the capital planning process to deliver maximum security in a cost-effective manner.

The implementation of IT security and capital planning practices within the federal government is driven by a combination of legislation, rules and regulations, and agency-specific policies. FISMA requires agencies to integrate IT security into their capital planning and enterprise architecture processes, conduct annual IT security reviews of all programs and systems, and report the results of those reviews to OMB. Therefore, the implementation of FISMA legislation effectively integrates IT security and capital planning because agencies must document resource and funding plans for IT security. Furthermore, implementation of FISMA legislation ensures that agency resources are protected, ensures that risk is effectively managed, and requires agencies to incorporate IT security into the life cycle of their information systems. OMB's FISMA reporting guidance also suggests that agencies use NIST SP 800-26, *Security Self-Assessment Guide for Information Technology Systems*, to evaluate their security programs. The results of the self-assessment should be documented in the agency's annual FISMA report and logged in the agency's POA&M, along with POA&M inputs from other appropriate sources. The agency must then determine the costs and timeframes associated with mitigating the weaknesses identified in the POA&Ms. These costs are captured in

Continued on page 2

ITL Bulletins are published by the Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST). Each bulletin presents an in-depth discussion of a single topic of significant interest to the information systems community. **Bulletins are issued on an as-needed basis** and are available from ITL Publications, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8900, Gaithersburg, MD 20899-8900, telephone (301) 975-2832. To be placed on a mailing list to receive future bulletins, send your name, organization, and business address to this office. You will be placed on this mailing list only.

Bulletins issued since November 2003

- *Network Security Testing,* November 2003
- *Security Considerations in the Information System Development Life Cycle*, December 2003
- *Computer Security Incidents: Assessing, Managing, and Controlling the Risks*, January 2004
- *Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems*, March 2004
- *Selecting Information Technology Security Products*, April 2004
- *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004
- *Information Technology Security Services: How to Select, Implement, and Manage*, June 2004
- *Guide for Mapping Types of Information and Information Systems to Security Categories*, July 2004
- *Electronic Authentication: Guidance For Selecting Secure Techniques*, August 2004
- *Information Security Within The System Development Life Cycle*, September 2004
- *Securing Voice Over Internet Protocol (IP) Networks*, October 2004
- *Understanding the New NIST Standards and Guidelines Required by FISMA*, November 2004

the system or program's annual OMB Exhibit 300 and in the enterprise-wide Exhibit 53, which are the funding vehicles submitted to OMB to secure an operating budget.

Methodology

To address the capital planning and IT security requirements imposed on federal IT investments, NIST recommends a seven-step framework for integrating IT security into the capital planning process for enterprise-level IT security activities and individual system IT security activities:

- **Enterprise-level investments –** those security investments that are ubiquitous across the agency and will improve the overall agency's security posture (for example, an enterprise-wide firewall or intrusion detection system [IDS] acquisition or public key infrastructure [PKI]).
- **System-level investments –** those security investments designed to strengthen a discrete system's security posture (for example, strengthening password controls or testing a contingency plan for a particular system).

The framework assists federal agencies in integrating IT security into the capital planning process by providing a systematic approach to selecting, managing, and evaluating IT security investments. The methodology relies on existing data inputs so it can be readily implemented at federal agencies. Inputs for the methodology include:

Who we are

The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST) of the Technology Administration, U.S. Department of Commerce. We develop tests and measurement methods, reference data, proof-of-concept implementations, and technical analyses that help to advance the development and use of new information technology. We seek to overcome barriers to the efficient use of information technology, and to make systems more interoperable, easily usable, scalable, and secure than they are today. Our website is http://www.itl.nist.gov/.

- **Enterprise-Level Information**
  - Stakeholder rankings of enterprise-wide initiatives
  - Enterprise-wide initiative IT security status
  - Cost of implementing remaining appropriate security controls for enterprise-wide initiatives
- **System-Level Information**
  - System categorization (see NIST Federal Information Processing Standard 199, *Standard for Security Categorization of Federal Information and Information Systems)*
  - Security compliance
  - Corrective action cost

The seven-step methodology, shown in *Figure 1* can help agencies identify high-priority corrective actions for immediate funding. The seven steps include:

1. **Identify the Baseline:** use information security metrics or other available data to baseline the current security posture.
2. **Identify Prioritization Requirements:** evaluate security posture against legislative and Chief Information Officer (CIO)-articulated requirements and agency mission.
3. **Conduct Enterprise-Level Prioritization:** prioritize potential enterprise-level IT security investments against mission and financial impact of implementing appropriate security controls.
4. **Conduct System-Level Prioritization:** prioritize potential system-level corrective actions against system category and corrective action impact.
5. **Develop Supporting Materials:** for enterprise-level investments, develop concept paper, business case analysis, and Exhibit 300. For system-level investments, adjust Exhibit 300 to request additional funding to mitigate prioritized weaknesses.
6. **Implement Investment Review Board (IRB) and Portfolio Management:** prioritize agency-wide business cases against requirements and CIO priorities and determine investment portfolio.

FIGURE 1
Integrating IT Security and Capital Planning

7. **Submit Exhibit 300s, Exhibit 53, and Conduct Program Management:** ensure approved 300s become part of the agency's Exhibit 53; ensure investments are managed through their life cycle (using Earned Value Management for Development/Modernization/Enhancement investments and operational assessments for steady state investments) and through the General Accounting Office (GAO) Information Technology Investment Management (ITIM) maturity framework.

The process presented is intended to serve as a model methodology. Agencies should work within their investment planning environments to adapt and incorporate the pieces of this process into their own unique processes to develop workable approaches for CPIC. If incorporated into an agency's processes, the methodology can help ensure that IT security is appropriately planned for and funded throughout the investment's life cycle, thus strengthening the agency's overall security posture.

This systematic approach can help agencies:

- Identify relevant OMB and other guidance that applies to governing federal government IT security investment decisions;

- Explain how current security requirements relate and support the IT CPIC process;
- Understand the IT investment management process phases—Select, Control, and Evaluate—as they relate to security investments;
- Identify CPIC-related roles and responsibilities required to manage IT security investments;
- Explain the best practices IT security management process and why it is important for making sound IT security investment decisions;
- Understand how to develop security requirements and appropriate supporting documentation for IT acquisition;
- Identify steps and materials required to complete a sound business case in support of investment requests; and
- Understand implementation issues associated with incorporating IT security into the CPIC process.

Figure 2 illustrates the relationship between legislation, regulation, and guidance that exists for IT security and capital planning for the federal government.

FISMA provides overarching requirements for securing federal resources and ensuring that security is incorporated into all phases of the investment life cycle. FISMA codifies specific responsibilities of federal agency officials, addresses protection of agency information resources, calls for agency officials to manage risk to an appropriate level, and requires agencies to incorporate security into the life cycle of information systems. FISMA requires agencies to complete an annual program review that includes conducting self-assessments for all agency systems and conducting a FISMA independent evaluation. Results from these activities are compiled into a comprehensive FISMA report, which is submitted to OMB along with the budget year financial documentation. The corrective actions that agencies identify to mitigate weaknesses found in the FISMA report are documented and tracked in the POA&M.

FISMA reporting includes providing a status of security weaknesses in key

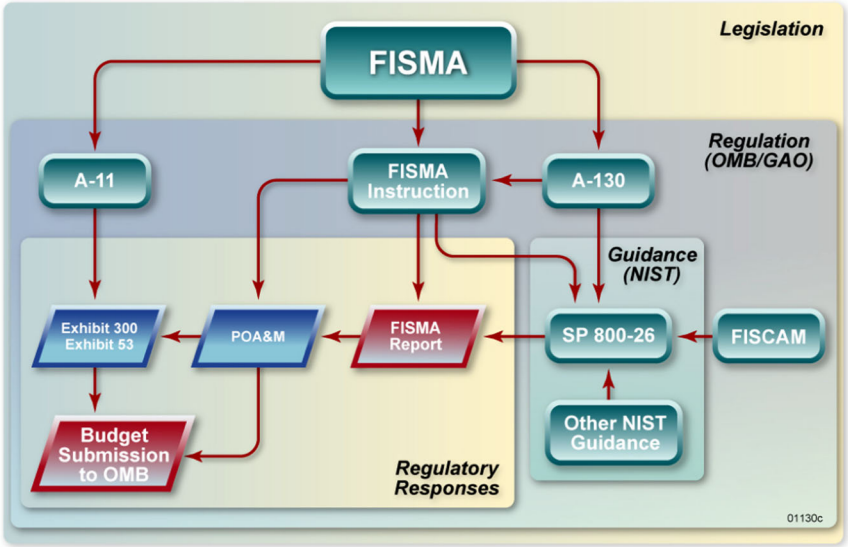

FIGURE 2
Federal IT Security and Capital Planning Legislation, Regulations, and Guidance

areas of a security program. As required by FISMA, OMB provides specific guidance annually. FISMA reporting guidance specifies reporting formats and identifies required actions associated with the quarterly and annual reporting.

The POA&M process provides a direct link to the capital planning process. The POA&M information includes the costs of corrective actions that have to be captured in the Exhibit 300 and rolled into the Exhibit 53, which provides an overview of an agency's IT portfolio. The Exhibit 53 includes a rollup of all Exhibit 300s and additional IT expenses from across the agency. All IT investments are identified by mission area and include their budget year and life-cycle cost, as well as the percentage of their costs that are devoted to IT security. All costs are totaled across the agency to provide an overall picture of the agency's IT portfolio.

Costs associated with each POA&M item are required to map to annual budget requests in the Exhibit 300s and the Exhibit 53. These costs are captured as a component of the *percentage of IT security*, or the percentage of the total investment for the budget year associated with IT security in the Exhibit 300, and are then aggregated in the Exhibit 53. Typically, these costs include direct costs of providing IT security for the specific IT investments. Examples include the following:

- Risk assessment
  - Security planning and policy
  - Certification and accreditation (C&A)
  - Specific security controls
  - Authentication or cryptographic applications
  - Education, awareness, and training
  - System reviews/evaluations (including system security test and evaluation [ST&E])
  - Oversight or compliance inspections
  - Development or maintenance of agency reports to OMB and corrective action plans as they pertain to the specific investment
  - Contingency planning and testing
  - Physical and environmental controls for hardware and software
  - Auditing and monitoring
  - Computer security investigations and forensics
  - Reviews, inspections, audits, and other evaluations performed on contractor facilities and operations
  - Privacy impact assessments.

- Products, procedures, and personnel that have an incidental or integral component and/or a quantifiable benefit for the specific IT investment. Examples include the following:
  a. Configuration or change management control
  a. Personnel security
  a. Physical security
  a. Operations security
  a. Privacy training
  a. Program/system evaluations whose primary purpose is other than security
  a. System administrator functions
  a. System upgrades with new features that obviate the need for other stand-alone security controls.
- Allocated security control costs for networks that provide some or all necessary security controls for associated applications. Examples include the following:
  - Firewalls
  - IDSs
  - Forensic capabilities
  - Authentication capabilities (e.g., PKI)
  - Additional 'add-on' security considerations.

ITL Bulletins Via E-Mail
We now offer the option of delivering your ITL Bulletins in ASCII format directly to your e-mail address. To subscribe to this service, send an e-mail message from your business e-mail account to listproc@nist.gov with the message **subscribe itl-bulletin**, and your name, e.g., John Doe. For instructions on using listproc, send a message to listproc@nist.gov with the message **HELP**. To have the bulletin sent to an e-mail address other than the From address, contact the ITL editor at 301-975-2832 or elizabeth.lennon@nist.gov.

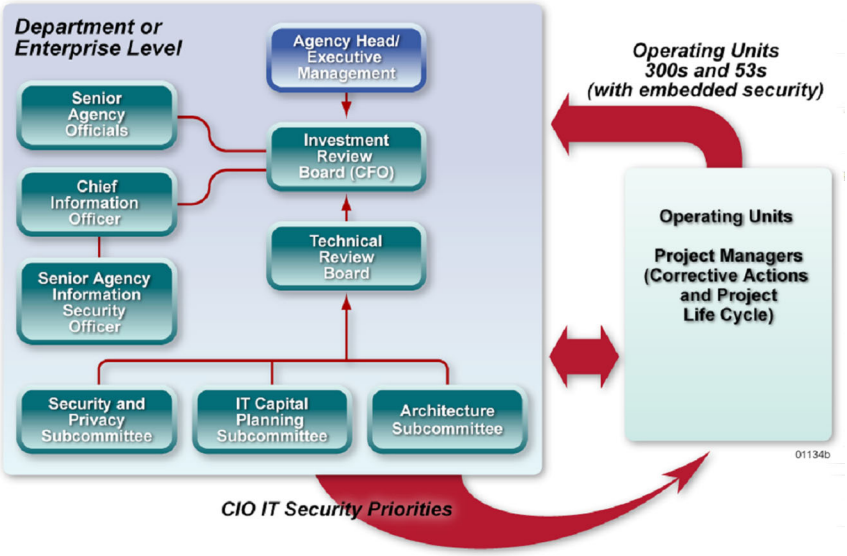

FIGURE 3
Notional IT Management Hierarchy

Ongoing security costs (operations and maintenance costs) are combined with the specific remediation costs and are submitted to OMB in the Exhibit 300s and Exhibit 53 for the budget year.

Select, Control, Evaluate Process

In concert with the OMB capital planning and NIST security requirements, agencies use GAO's best practices, three-phased investment life-cycle model for federal IT investments, **Select, Control, and Evaluate,** to ensure that investment management practices, including security, are disciplined and thorough throughout each phase of the investment life cycle.

The **Select** phase refers to activities associated with assessing and prioritizing current and proposed IT projects based on mission needs and improvement priorities and then creating a portfolio of IT projects to address the needs and priorities. Typical Select phase activities include screening new projects; analyzing and ranking all projects based on benefit, cost, and risk criteria; selecting a portfolio of projects; and establishing project review schedules.

The **Control** phase refers to activities designated to monitor the investment during its operational phase to determine if the investment is within the cost and schedule milestones established at the beginning of the investment life cycle. Typical processes involved in the Control phase include using a set of performance measures to monitor the developmental progress for each IT project to enable early problem identification and resolution.

The **Evaluate** phase refers to determining the efficacy of the investment, answering the question, "Did the investment achieve the desired results and performance goals identified during the Select phase?"

IT Management Hierarchy

Integrating IT security into the capital planning process requires input and collaboration across agencies and functions. *Figure 3* depicts a hierarchical approach to capital planning in which investment decisions are made at both the enterprise and operating unit levels.

While specific practices for investment management vary greatly at the operating unit level because of varying sizes and missions of the operating units, the process generally mirrors the process at the departmental level. The CIO formulates and articulates IT security priorities to the organization to be considered within the context of all agency investments. Priorities may be based on agency mission, executive

branch guidance such as the President's Management Agenda, OMB guidance, or other external/internal priorities. Examples of security priorities include certifying and accrediting all systems or implementing PKI throughout the enterprise. (It is important to note that OMB/Executive Branch guidance or laws should be ranked highest among these priorities.)

Once operating units finalize their IT portfolios and budget requests for the budget year, they forward their requests to the agency-level decision makers. At the agency level, several committees evaluate IT portfolios from the operating units as referenced in *Figure 3*, culminating in a review by the IRB. The IRB then decides on an agency-level IT portfolio and forwards recommendations to the agency head for review.

Once the agency-level IT portfolio is approved by the agency head, the necessary Exhibit 300s and Exhibit 53 are forwarded to OMB to obtain funding.

Conclusion

NIST Special Publication 800-65 describes in detail the underpinning methodology which can be easily applied to address security requirement integration and prioritization into an agency's capital planning and investment planning process using well-understood concepts related to the current FISMA framework and existing NIST standards and guidance. The publication is available at http://csrc.nist.gov/publications/nistpubs/index.html.

Disclaimer
Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
100 Bureau Drive, Stop 8900
Gaithersburg, MD 20899-8900

PRSRT STD
POSTAGE & FEES PAID
NIST
PERMIT NUMBER G195

Official Business
Penalty for Private Use $300

Address Service Requested