ITL BULLETIN FOR APRIL 2010

GUIDE TO PROTECTING PERSONALLY IDENTIFIABLE INFORMATION

Shirley Radack, Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Federal organizations maintain significant amounts of information about individuals and have a special responsibility to protect that information from loss and misuse. Security incidents involving personally identifiable information can result in considerable harm, embarrassment, and inconvenience to the individual and may lead to identity theft or other fraudulent use of the information. Organizations can experience a loss of public trust, legal liability, or remediation costs.

Personally identifiable information (PII) is any information about an individual that is maintained by an agency, including information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information (based on General Accountability Office and Office of Management and Budget definitions).

Concerns about the security of PII have been raised over the past few years as some federal agencies have reported the loss or theft of equipment containing personal information or unauthorized access to information on agency systems.

Federal Requirements to Protect Information and Information Systems

The Privacy Act of 1974 and the E-Government Act of 2002 establish federal agency responsibilities to protect personal information, and to ensure its security. Under the Federal Information Security Management Act (FISMA) of 2002, federal agencies must develop, document, and implement programs to protect their information and information systems. This policy applies to the systems that support the operations and assets of the agency, and includes those systems provided or managed by another agency, contractor, or other source. FISMA calls for agencies to apply a risk-based policy to achieve cost-effective results for the security of their information and information systems.

Standards and guidelines developed by the Information Technology Laboratory of the National Institute of Standards and Technology (NIST) assist agencies in carrying out effective information security programs based on the management of risk. Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems,* specifies that federal organizations

categorize their information and information systems based on the potential impact on the organization should adverse events occur which could jeopardize the information and information systems needed by the organization to accomplish its mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals.

FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems,* helps organizations use the categorization results obtained under FIPS 199 to designate their information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability. For each information system, agencies then select an appropriate set of security controls from NIST Special Publication (SP) 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations,* to satisfy their minimum security requirements.

NIST has developed the Risk Management Framework (RMF) to guide agencies through a structured process to identify the risks to the information systems, assess the risks, and take steps to reduce risks to an acceptable level. NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach,* explains the basic concepts to be applied to the management of security risks to information systems. It covers planning and building information security capabilities into information systems throughout the system life cycle; implementing up-to-date management, operational, and technical security controls; and maintaining awareness of the security condition of information systems through improved monitoring.

The Office of Management and Budget (OMB) has issued guidance concerning agency responsibilities to protect information, including actions that agencies should take to protect personally identifiable information from unauthorized use, access, disclosure, or sharing. In addition, OMB has issued requirements for reporting security breaches and the loss or unauthorized access of personally identifiable information, and has directed agencies to develop policies for notifying those affected by such breaches.

NIST Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*

NIST recently issued SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),* to assist federal agencies in carrying out their responsibilities to protect PII in information systems. Written by Erika McCallister, Tim Grance, and Karen Scarfone of NIST, the publication discusses how to identify PII and protect the confidentiality of PII as part of the organization's information security procedures. The guide also explains the importance of protecting the privacy of the individuals whose personal information is kept by the organization, as required by federal laws and in accordance with Fair Information Practices.

A section of the guide outlines the factors to be considered when determining the impact level for the security objective of confidentiality of the PII. The guide explains the need

to determine the PII confidentiality impact level, taking into account additional requirements for protecting personal information.

Other topics covered in the guide include the operational safeguards, privacy-specific safeguards, and security controls that should be applied as part of the organization's risk-based approach for protecting the confidentiality of PII; the development of policies and procedures for protecting PII; the establishment of training and awareness programs for staff members; and the development of policies and procedures for handling security incidents involving PII.

The appendices to the guide provide detailed information on scenarios for PII identification and handling; frequently asked questions (FAQs); terms and definitions for PII; Fair Information Practices; a glossary; explanation of acronyms and abbreviations; and a reference list of additional resources for protecting PII.

NIST SP 800-122 is available from NIST's Web page http://csrc.nist.gov/publications/PubsSPs.html.

NIST's Recommendations to Organizations for Protecting PII

NIST recommends that organizations take the following steps to protect their PII:

Identify all PII residing in the organizational environment.

All PII should be identified on all systems, including databases, shared network drives, backup tapes, and sites maintained by contractors. Examples of PII include, but are not limited to:

- Name, such as full name, maiden name, mother's maiden name, or alias;
- Personal identification number, such as social security number (SSN), passport number, driver's license number, taxpayer identification number, or financial account or credit card number;
- Address information, such as street address or email address;
- Personal characteristics, including photographic image, especially a face image or other identifying characteristic; fingerprints; handwriting; or other biometric data, such as retina scan, voice signature, and facial geometry; and
- Information about an individual that is linked or linkable to one of the above categories, such as date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, and financial information.

Minimize the use, collection, and retention of PII to what is strictly necessary to accomplish their business purpose and mission.

The likelihood of harm caused by a breach involving PII is greatly reduced if an organization minimizes the amount of PII that it uses, collects, and stores. For example, an organization should only request PII in a new form if the PII is absolutely necessary. Also, an organization should regularly review its holdings of previously collected PII to determine whether the PII is still relevant and necessary for meeting the organization's business purpose and mission. Disposal of PII should be conducted in accordance with National Archives and Records Administration (NARA) and specific agency requirements.

OMB (see Memorandum M-07-16 in the More Information section below) specifically requires agencies to:

- Review current holdings of PII and ensure they are accurate, relevant, timely, and complete;
- Reduce PII holdings to the minimum necessary for proper performance of agency functions;
- Develop a schedule for periodic review of PII holdings; and
- Establish a plan to eliminate the unnecessary collection and use of social security numbers (SSNs).

Categorize all PII by the PII confidentiality impact level.

All PII should be evaluated to determine the PII confidentiality impact level. This assessment helps the organization apply appropriate safeguards for PII. The PII confidentiality impact level (low, moderate, or high) indicates the potential harm that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed, and may be different from the confidentiality impact levels that are determined by the application of FIPS 199. When the PII confidentiality impact level is determined, it is used to supplement the provisional confidentiality impact level, which was determined using the FIPS 199 processes. Organizations should decide which factors they will use to determine the PII confidentiality impact level, and should create and implement appropriate policy, procedures, and controls.

Examples of factors to be considered include:

- **How easily PII can be used to identify specific individuals**. For example, an SSN uniquely and directly identifies an individual, but a telephone area code identifies a set of people.

• **How many individuals can be identified from the PII**. Breaches of 25 records and 25 million records may have different impacts. The PII confidentiality impact level may be raised but should not be lowered based on this factor.

• **Evaluation of the sensitivity of each individual PII data field**. For example, an individual's SSN or financial account number is generally more sensitive than an individual's phone number or ZIP code. Organizations should also evaluate the sensitivity of the PII data fields when the data from different fields is combined.

• **Evaluation of the context of use of the PII.** The context of use is the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated. The context of use may result in the same PII data elements being assigned to different PII confidentiality impact levels based on their use. For example, an organization may have two lists that contain the same PII data fields, such as name, address, and phone number. The first list may be composed of people who subscribe to a general-interest newsletter produced by the organization, and the second list may be composed of people who work undercover in law enforcement. If the confidentiality of the lists is breached, the potential impacts to the affected individuals and to the organization are significantly different for each list.

• **Obligations to protect confidentiality.** Organizations should consider their specific obligations to protect PII when determining the PII confidentiality impact level. Obligations to protect PII are specified in laws, regulations, and other mandates, including the Privacy Act and OMB guidance. Federal agencies, such as the Census Bureau and the Internal Revenue Service (IRS), are subject to specific legal requirements to protect certain types of PII.

• **Access to and location of PII.** Organizations may choose to take into consideration the nature of authorized access to and the location of PII. When PII is accessed more often or by more people and systems, or the PII is regularly transmitted or transported off-site, then there are more opportunities for the confidentiality of the PII to be compromised.

Apply the appropriate safeguards for PII based on the PII confidentiality impact level.

Organizations should apply appropriate safeguards to protect the confidentiality of PII based on the PII confidentiality impact level. Safeguards may differ based on the confidentiality impact level. PII, such as the public phone directory, does not have to be protected for confidentiality when the organization has permission or authority to release such information publicly. NIST recommends using operational safeguards, privacy-specific safeguards, and security controls, such as:

• **Developing comprehensive policies and procedures** for protecting the confidentiality of PII.

• **Requiring that all individuals receive appropriate training** before being granted access to systems containing PII to reduce the possibility that PII will be accessed, used, or disclosed inappropriately.

• **De-identifying records** by removing enough PII so that the remaining information does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual. De-identified records can be used when full records are not necessary, such as for examinations of correlations and trends.

• **Controlling access to PII** through access control policies and access enforcement mechanisms, such as access control lists.

• **Prohibiting or strictly limiting access to PII from portable and mobile devices**, such as laptops, cell phones, and personal digital assistants (PDAs), which are generally higher-risk than non-portable devices, such as desktop computers at the organization's facilities.

• **Protecting the confidentiality of transmitted PII**. This can be implemented by encrypting the communications or by encrypting the information before it is transmitted.

• **Monitoring events** that affect the confidentiality of PII, such as inappropriate access to PII.

Develop an incident response plan to handle breaches involving PII.

Breaches involving PII are hazardous to both individuals and organizations. Harm to individuals and organizations can be contained and minimized through the development of effective incident response plans for breaches involving PII. Organizations should develop plans that include elements such as determining when and how individuals should be notified, how a breach should be reported, and whether to provide remedial services, such as credit monitoring, to affected individuals.

Encourage close coordination among chief privacy officers, senior agency officials for privacy, chief information officers, chief information security officers, and legal counsel when addressing issues related to PII.

To protect the confidentiality of PII effectively, organizations need a comprehensive understanding of their information systems, information security, privacy, and legal requirements. Decisions regarding the applicability of a particular law, regulation, or other mandate should be made in consultation with the organization's legal counsel and privacy officer since the laws, regulations, and other mandates are often complex and may change over time. Also, new technical security controls may be needed to implement and enforce new security policies that are adopted. Close coordination of the organization's technical and legal experts helps to prevent incidents that could result in

the compromise and misuse of PII by ensuring proper interpretation and implementation of requirements.

More Information on Protecting Personally Identifiable Information

Information about the following NIST publications that help organizations protect personally identifiable information and about other publications that address information security issues is available from NIST's Computer Security Resource Center at http://csrc.nist.gov/.

Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*
FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*
NIST Special Publication (SP) 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*
NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*
NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*
NIST SP 800-60, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories,* (Volumes 1 and 2)
NIST SP 800-61 Revision 1, *Computer Security Incident Handling Guide*
NIST SP 800-64, Revision 2, *Security Considerations in the System Development Life Cycle*

Information about OMB directives to federal agencies, including the following, is available from the OMB Web page http://www.whitehouse.gov/omb/memoranda/.

OMB Memorandum M-06-15, *Protecting Personally Identifiable Information*
OMB Memorandum M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*
OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*

The General Accountability Office (GAO) has issued several reports concerning the threats to and protection of PII, including the following report available from the GAO Web page http://www.gao.gov/.

GAO Report 08-343, *Protecting Personally Identifiable Information*

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.