Best Practices: Elements of a Federal Privacy Program

Version 1.0

Sponsored By:

Federal CIO Council
Privacy Committee

June 2010

Contents

Acknowledgements

Version 1.0 of *Best Practices: Elements of a Federal Privacy Program* was collaboratively developed by members of the Privacy Committee Best Practices Subcommittee of the Federal CIO Council ("Best Practices Working Group"), which consists of privacy experts from across the federal government. This collaboration significantly strengthened the document by identifying and incorporating best practices from a number of different federal entities.

The Best Practices Subcommittee is co-led by Jerry Hanley of the Department of Energy, Martha K. Landesberg of the Department of Homeland Security Privacy Office and Roanne Shaddox of the Federal Deposit Insurance Corporation. The Privacy Committee of the Federal CIO Council is co-chaired by Roger Baker of the Department of Veterans Affairs, Mary Ellen Callahan of the Department of Homeland Security, and Nancy Libin of the Department of Justice. The members of the Best Practices Working Group contributing to this document included:

Name	Organization
Claire Barrett	Transportation Security Administration
Chris Brannigan	United States Postal Service
Pamela Carcirieri	Social Security Administration
Debra Diener	Internal Revenue Service
Jerry Hanley	Department of Energy
Deborah Kendall	United States Postal Service
Martha K. Landesberg	Department of Homeland Security
Toby M. Levin	Department of Homeland Security
Steven Lott	Federal Deposit Insurance Corporation
Roanne Shaddox	Federal Deposit Insurance Corporation

The dedication and contributions of these individuals made the completion of this document possible. The Privacy Committee wishes to specially recognize Toby Levin for her leadership of this effort.

Roger Baker
Chief Information Officer
Department of Veterans Affairs

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security

Nancy Libin
Chief Privacy and
Civil Liberties Officer
Department of Justice

Purpose

This document serves as a best practices guide to help federal organizations implement and sustain privacy awareness and stewardship.[1] This document can be integrated into any government organizational level – department, component, office, or program – responsible or accountable for privacy. The seven elements described in this document provide the basis for a robust federal privacy program. A strong and multi-faceted privacy program will help ensure that organizations consider privacy protections and controls when first making business decisions involving the collection, use, sharing, retention, disclosure, and destruction of personally identifiable information (PII), whether in paper or electronic form.[2] These seven elements can also influence business decisions involving the use of new technologies or other interactions with the public, contractors, or employees that may not involve the collection and use of PII but may nonetheless raise privacy risks or concerns (e.g., the use of surveillance cameras, global positioning systems, or body imaging screening devices).

Elements of a Federal Privacy Program identifies the fundamental building blocks of a robust privacy program. The seven elements are:

- Element 1 – Leadership
- Element 2 – Privacy Risk Management and Compliance Documentation
- Element 3 – Information Security
- Element 4 – Incident Response
- Element 5 – Notice and Redress for Individuals
- Element 6 – Privacy Training and Awareness
- Element 7 – Accountability

Each element corresponds to recommended best practices that are illustrative of the actions necessary to establish a comprehensive federal privacy program. Each organization's specific mission, as well as its legal, regulatory, and operational obligations, requirements, and authorities, will affect the design and implementation of its privacy program. Organizations with national security or law enforcement authorities will take those interests, as well as privacy interests, into account in determining how to apply these elements. Law enforcement and

[1] Throughout the document, the term "organization" is used broadly to mean the department or agency or, in the alternative, the organization's privacy office, which is responsible for implementing the agency's privacy program. The term's specific meaning depends on the context within which it is being used.

[2] The Office of Management and Budget (OMB) Memorandum 07-16 (M-07-16) defines "personally identifiable information" as "information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."

intelligence programs and systems, particularly those that are classified, will require modifications of these elements in light of their legal and operational requirements. In addition, access to resources and funding streams will play a key role in determining the depth and breadth with which organizations are able to implement the recommendations included in this document.

Organization leadership can use this document to assist in designing an agency-wide privacy program and in determining the responsibilities of candidates for the position of Senior Agency Official for Privacy (SAOP) or Chief Privacy Officer (CPO) to lead the program.[3] This document will also be especially useful to the SAOP/CPO chosen to lead an organization's privacy program or for existing SAOPs/CPOs to identify where they can enhance their programs.[4] In addition, SAOPs/CPOs can use this document to assist in seeking funding to support their privacy initiatives. They can also use this document to support joint efforts with Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs) to adopt new or modify existing technologies to enhance overall privacy protections. SAOP/CPOs should make this document available to those individuals within their organizations who have historically played a role in privacy, including but not limited the FOIA Officer, Classification Security Officer (CSO), Chief Financial Officer (CFO), Information System Security Officer (ISSO), legal counsel, Paperwork Reduction Act (PRA) Liaison, Records Management Officer (RMO), Website Administrator, and other program officials, business owners, and system developers. Policy makers, organization enterprise architects, business owners, system developers, and others involved in policy and program development and implementation within an organization may use this document to build privacy considerations into business operations from the very beginning.

[3] For the purposes of this document, "SAOP/CPO" will be referenced throughout indicating the same role and job functions. In some organizations, one individual may be designated as both the SAOP and the CPO, while in other organizations, these roles may be held by separate individuals. Organizations that comply with both OMB M-05-08 *Designation of Senior Agency Officials for Privacy*, and Section 522 of the *Transportation, Treasury, Independent Agencies, and General Government Appropriations Act of 2005 (Pub. L. No. 108-447, div. H, Dec. 8, 2004, 118 Stat. 2801)*, may have both and an SAOP and a CPO. *See* Element 1: Leadership for more information on the role of the SAOP/CPO.

[4] In a number of circumstances, the document identifies specific roles and responsibilities for the SAOP/CPO, while leaving other roles and responsibilities to the organization to define, as organizations currently may have assigned some responsibilities to other offices.

Introduction: Privacy Stewardship and Governance

Protecting privacy is a core consideration for every federal organization, and it is best achieved when it is an integral part of the organization's business operations. Privacy must be considered as part of the upfront assessment of policy and programmatic decision-making as well as business operations, application development, and related activities; it should not be an afterthought. Privacy stewardship and governance are keys to a successful privacy program and can reduce the risk that government programs erode privacy protections and ultimately lose the public's trust.

Privacy is a broad and complex concept that arises in a variety of contexts: information privacy (rules that govern collection, handling, and use of PII), bodily privacy (protection against invasion of a person's physical being), territorial privacy (limitations on the ability to intrude into another person's environment), and communications privacy (protection of mail, telephone, and email).[5] Federal laws and regulations tend to focus primarily on information privacy issues, particularly as federal organizations increasingly use technology to collect, process, and store PII on employees and members of the public. However, information privacy is only one of many privacy issues that federal organizations must manage.

The need for federal organizations to protect PII and safeguard privacy has not fundamentally changed since the passage of the Privacy Act of 1974, as amended (Privacy Act).[6] Administrations continue to recognize that individuals[7] are entitled to a transparent and open government[8] and to the protections set forth in the Privacy Act. These protections include: notice; protection against unauthorized disclosures; the right of individuals to review their records and to find out if these records have been disclosed; the right to request corrections or amendments; assurances that the information collected or maintained is accurate, relevant, timely, and complete; and accountability for violations of personal privacy.[9]

What has changed since 1974, however, are the information environments in which federal organizations must operate. Organizations have undergone a technology revolution, expanding the ability of government to access, organize, and search data in documents, emails, web pages, and computer databases. Connected and converged systems have created unprecedented reach

[5] International Association of Privacy Professionals, *Information Privacy: Official Reference for the Certified Information Privacy Professional*, "Classes of Privacy," at 2.
[6] 5 U.S.C. § 552a.
[7] As defined in the Privacy Act, the term individual means "a citizen of the United States or an alien lawfully admitted for permanent residence." Some federal organizations have extended the administrative protections of the Privacy Act to visitors to the United States.
[8] *Transparency and Open Government Memorandum for the Heads of Executive Departments and Agencies*, 74 Fed. Reg. 4,685 (Jan. 26, 2009), *available at* http://edocket.access.gpo.gov/2009/pdf/E9-1777.pdf and OMB Memorandum No. M-10-06, *Open Government Directive* (2009), *available at* http://www.whitehouse.gov/omb/assets/memoranda_2010/m10-06.pdf.
[9] 5 U.S.C. § 552a. Certain exceptions may apply where records are legally exempt.

into warehouses of information. The expanded use of web-based, social media technologies is also challenging existing information and communication paradigms for individuals, government, and business.

These advances have also created an even greater challenge for information management and privacy. To meet these challenges, support for privacy should start at the top and resonate throughout an organization. The SAOP/CPO serves as the privacy steward for the organization. To be effective, the SAOP/CPO should have support from the head of the organization and the authority necessary to implement privacy policy for the organization and be involved in key decisions, projects, and operations in their early stages of development. Moreover, an organization's SAOP/CPO should be a member of senior leadership and have adequate funding and staff to establish a robust privacy program.[10] This structure provides the basis for the SAOP/CPO to provide privacy governance and stewardship of the public's information.

This document provides a roadmap for establishing effective management and oversight of an organization's privacy program and for establishing a strategic privacy planning framework. A privacy program's stated mission, principles, and individual policies must be aimed at materially reducing privacy risks, while also fulfilling legal and regulatory requirements. Appendix II provides a compilation of federal privacy-related legal and regulatory requirements. Many other statutes covering particular types of information, e.g., tax, grand jury, and health information, also may contribute to the legal foundation protecting privacy of individuals in the U.S.

The two primary federal privacy laws – the Privacy Act and the E-Government Act of 2002 (E-Government Act)[11] – have embedded within them the Fair Information Practice Principles (FIPPs), a comprehensive framework for privacy policy and implementation. The FIPPs were initially articulated in a 1973 Department of Health, Education and Welfare advisory committee report entitled *Records, Computers and the Rights of Citizens*.[12] These principles are also mirrored in the laws and policies of many U.S. states, as well as many foreign nations and international organizations.[13] The FIPPs provide a framework for organizing and addressing privacy requirements and capabilities and are the basis for the Privacy Control Families outlined

[10] Indeed, Section 803 of the Implementing Recommendations of the 9/11 Commission Act *requires* that "[t]he Attorney General, the Secretary of Defense, the Secretary of State, the Secretary of the Treasury, the Secretary of Health and Human Services, the Secretary of Homeland Security, the Director of National Intelligence, the Director of the Central Intelligence Agency, and the head of any other department, agency, or element of the executive branch designated by the Privacy and Civil Liberties Oversight Board to designate no less than one (1) senior officer to serve as the principle advisor to assist the head of such department, agency, or element and other officials…in appropriately considering privacy…when such officials are proposing, developing, or implementing laws, regulations, policies, procedures, or guidelines related to efforts to protect the Nation against terrorism." 42 U.S.C § 2000ee-1(a). Section 803 further requires that these privacy officers report directly to their agency heads. 42 U.S.C § 2000ee-1(c).

[11] Pub. L. No. 107-347, 116 Stat. 2899.

[12] http://aspe.os.dhhs.gov/datacncl/1973privacy/tocprefacemembers.htm.

[13] *See generally* Organization for Economic Cooperation and Development (OECD), *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, *available at* http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

in the Federal Enterprise Architecture-Security and Privacy Profile (FEA-SPP).[14] (See excerpted Privacy Control Families below.) The elements outlined in this document build upon the FIPPs and FEA-SPP privacy control families and provide the operational context for their implementation. A new version of the FEA-SPP, which includes the following Privacy Control Families, is currently under final review by federal organizations. The Privacy Control Families are also discussed in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-122, *Guide to Protecting the Confidentiality of PII* (April 2010).

The FEA-SPP Privacy Control Families

- Transparency: Providing notice to the individual regarding the collection, use, dissemination, and maintenance of PII.
- Individual Participation and Redress: Involving the individual in the process of using PII and seeking individual consent for the collection, use, dissemination, and maintenance of PII. Providing mechanisms for appropriate access, correction, and redress regarding the use of PII.
- Purpose Specification: Specifically articulating the authority that permits the collection of PII and specifically articulating the purpose or purposes for which the PII is intended to be used.
- Data Minimization and Retention: Only collecting PII that is directly relevant and necessary to accomplish the specified purpose(s). Only retaining PII for as long as is necessary to fulfill the specified purpose(s) and in accordance with the National Archives and Records Administration (NARA) approved record retention schedule.
- Use Limitation: Using PII solely for the purpose(s) specified in the public notice. Sharing information should be for a purpose compatible with the purpose for which the information was collected.
- Data Quality and Integrity: Ensuring, to the greatest extent possible, that PII is accurate, relevant, timely, and complete for the purposes for which it is to be used, as identified in the public notice.
- Security: Protecting PII (in all media) through appropriate administrative, technical, and physical security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.
- Accountability and Auditing: Providing accountability for compliance with all applicable privacy protection requirements, including all identified authorities and established policies and procedures that govern the collection, use, dissemination, and maintenance of PII. Auditing for the actual use of PII to demonstrate compliance with established privacy controls.

[14] The FEA represents the U.S. federal government's framework for information technology investment analysis, management, and use. The FEA is comprised of five, inter-related reference models and three profiles (Geospatial Profile, Records Management Profile, and FEA-Security and Privacy Profile), which are intended to promote common, consistent enterprise architecture practices that improve government performance. *See* www.whitehouse.gov/omb/e-gov/fea.

Element 1 –Leadership

The success of an organization's privacy program is dependent upon its leadership – the selection of a senior official with privacy expertise as the SAOP/CPO and direct support from the organization head are critical. Tangible and visible actions by the organization head attest to the importance of a vibrant privacy program. Support from the organization head may include: making it clear to subordinate officials that privacy issues are integral to the organization's accomplishing its mission; communicating the importance of privacy to the organization's staff; participating in selected privacy programs and initiatives; and providing adequate funding to support a robust privacy program. The SAOP/CPO must be an integral member of the organization's senior management team so that she or he has both the authority and vantage point from which to develop, implement, and lead the privacy program.

Every organization should have an SAOP/CPO who reports to the head of the organization and has direct privacy management and oversight responsibilities.[15] Each organization will need to evaluate its particular situation to determine the appropriate management structure for privacy. Relevant authorities include those specifically delineated by the Office of Management and Budget (OMB),[16] as well as those which are inherent in the SAOP's/CPO's position as a member of the senior management team, i.e., advising the organization head and other senior officials on the manner in which privacy considerations and requirements can be integrated into the organization's business operations.[17]

[15] In some organizations, one individual may be designated as both the SAOP and the CPO, while in other organizations, these roles are held by separate individuals. Organizations that comply with both OMB M-05-08 *Designation of Senior Agency Officials for Privacy*, and Section 522 of the *Omnibus Spending Bill for Transportation, Treasury, Independent Agencies, and General Government Appropriations Act of 2005*, may have both an SAOP and a CPO.

[16] In accordance with OMB M-05-08, "The senior agency official will have overall responsibility and accountability for ensuring the agency's implementation of information privacy protections, including the agency's full compliance with federal laws, regulations, and policies relating to information privacy . . . have a central role in overseeing, coordinating, and facilitating the agency's compliance efforts. This role shall include reviewing the agency's information privacy procedures to ensure that they are comprehensive and up-to-date and, where additional or revised procedures may be called for, working with the relevant agency offices in the consideration, adoption, and implementation of such procedures. Finally, the senior agency official shall ensure the agency's employees and contractors receive appropriate training and education programs regarding the information privacy laws, regulations, policies, and procedures governing the agency's handling of personal information . . . the senior agency official must also have a central policy-making role in the agency's development and evaluation of legislative, regulatory and other policy proposals which implicate information privacy issues, including those relating to the agency's collection, use, sharing, and disclosure of personal information. In evaluating these proposals, agencies must consider their potential impact on information privacy and take this impact into account in evaluating alternatives and making decisions."

[17] It is a common practice in the federal environment to designate an SAOP/CPO who also has other responsibilities. Where possible, organizations should appoint an SAOP/CPO whose sole function is administering privacy and who is a member of the senior leadership of the organization.

Only with appropriate leadership and resources can an organization's privacy program fully meet the growing number of legal, regulatory, policy, technology, and operational challenges posed by an organization's increasing demand for the collection and use of PII.

The following are representative examples of the range of SAOP/CPO responsibilities:

- Overall responsibility and accountability for ensuring the organization's implementation of information privacy protections, including the organization's full compliance with federal laws, regulations, and policies relating to privacy protection.
- Exercising a central role in overseeing, coordinating, and facilitating the organization's privacy compliance efforts. This role includes reviewing the organization's privacy procedures to ensure that they are comprehensive and current. Where additional or revised procedures are identified, the SAOP/CPO consults and collaborates with the appropriate organization offices in developing, adopting, and implementing these procedures.
- Ensuring the organization's employees and contractors receive appropriate training and education regarding their privacy protection responsibilities. These programs inform employees about the underlying privacy laws, regulations, policies, and procedures governing the organization's handling of PII, documents, and records.
- Playing a central policy-making role in the organization's development and evaluation of legislative, regulatory, and related policy proposals implicating privacy issues. Such issues include the organization's collection, use, sharing, retention, disclosure, and destruction of PII.

The SAOP/CPO must engage in close collaboration internally with key offices to ensure that the privacy program's mission is fully integrated into the organization's efforts to protect and secure PII. This requires close coordination with the CIO, CISO, legal counsel, records management, and other organization officials who have historically had a privacy related role.

In addition, interagency SAOP/CPO collaboration helps all participating programs to mature at an accelerated rate, while minimizing organization expenditures. Organizations can work together to identify—

- Best practices and common activities;
- Innovative solutions to common problems; and
- Overlapping management areas where memoranda of understanding, system of records notices, computer matching agreements, and interagency security agreements can be leveraged across organizations to improve operations and coordination among organizations.

Some organizations may also engage in international data sharing activities that require the SAOP/CPO to work closely with international partners to ensure that such efforts are performed in conformance with relevant U.S. and international data protection laws.

To promote transparency and accountability in privacy operations, the organization can consider establishing internal and external privacy advisory committees. External advisory committees will be governed by the requirements of the Federal Advisory Committee Act (FACA).[18] External committees can serve to assist the SAOP/CPO in addressing the ramifications of new programs, initiatives, systems, and technologies on the privacy rights of individuals.

To have an effective privacy program, the SAOP/CPO must have the requisite authority, resources, and support to implement policies and programs aimed at protecting privacy and PII that the organization collects, uses, disseminates, and maintains.

[18] 5 U.S.C. App. (1972).

Element 2 – Privacy Risk Management and Compliance Documentation

Introduction

The SAOP's/CPO's duties should include evaluating new technologies, programs, online activities, contracts, regulations, and legislation for potential privacy impacts, and advising other members of senior leadership on implementation of corresponding privacy protections. The SAOP/CPO uses the FIPPs/FEA-SPP framework to identify and mitigate privacy risks in programs and systems. The SAOP/CPO uses compliance documentation tools – (e.g., risk assessments, Privacy Impact Assessments (PIAs), and Privacy Act System of Records Notices (SORNs)) – to identify and reduce the privacy impact of the organization's activities, and to notify the public about any privacy impacts and steps taken to mitigate them. In addition, the SAOP/CPO should meet regularly with the organization's CIO, CISO, business owners, privacy personnel, and other organization officials who have historically had privacy related roles, as appropriate, to discuss new initiatives and how privacy can be addressed from the beginning of program design and throughout the System Development Life Cycle (SDLC).[19]

Identification and Compliance Oversight

The SAOP/CPO should leverage available resources in order to identify programs that must go through the privacy compliance process. Resources may include the Federal Information Security Management Act (FISMA)[20] Certification and Accreditation (C&A) process[21] or the OMB 300 budget process.[22] Working with the CIO and Chief Financial Officer (CFO), the SAOP/CPO can play an integral role by serving as a subject matter expert for reviews of new programs and IT systems to identify privacy compliance issues.

Compliance Documentation

The PIA and SORN are typically the key tools through which organizations identify holdings of PII, assess privacy risks, and implement privacy protections in their systems and programs. As part of the privacy compliance process, the SAOP/CPO works with program managers, system owners, and IT security personnel to ensure that sound privacy practices and controls are integrated into the organization's operations and activities that impact privacy. Some organizations have published official guidance regarding the requirements and content for

[19] SDLC is a model used by an organization in developing an information system. Many SDLC models exist. A general SDLC model includes the following five phases: (1) initiation, (2) acquisition/development, (3) implementation/assessment, (4) operations/maintenance, and (5) sunset (disposition). For more information on the SDLC see NIST Guidance available at: http://csrc.nist.gov/groups/SMA/sdlc/index.html.
[20] 44 U.S.C. §§ 3541-49.
[21] Certification is the comprehensive analysis of information technology systems' technical and non-technical security controls. Accreditation or "authorized processing" is the official management authorization for the operation of a system or application and is based on the certification process as well as other management considerations. NIST Computer Security Division, Computer Security Resource Center Frequently Asked Questions, *available at:* http://csrc.nist.gov/groups/SMA/fasp/faqs.html.
[22] *See* OMB Circular A-11, Section 300, *Planning, Budgeting, Acquisition, and Management of Capital Assets*, *available at* http://www.whitehouse.gov/OMB/circulars/a11/current_year/s300.pdf.

compliance documentation such as privacy risk assessments, PIAs, SORNs, Privacy Act (e)(3) Statements,[23] and computer matching agreements to assist those responsible for completing privacy compliance documentation.

Assessing Systems and Programs for Privacy Risks

The SAOP/CPO should develop and implement systems or tools for assessing the privacy impacts of all new and existing systems and programs.[24] The first step is to perform a privacy risk assessment to determine: (1) whether an activity involves PII or otherwise may impact privacy; (2) whether a PIA is required; and (3) whether an existing system of records notice covers a particular information collection, or if a new one is required. The privacy risk assessment is also the means by which the organization ensures that privacy is considered in systems undergoing C&A, and for assisting in determining the security categorization of a system based on the potential impact to the organization or individuals should there be a breach of security.[25]

The risk assessment process can also be used to formally document other program decisions that affect privacy. For example, the organization can use its PIA process to document and track a program or IT system that collects Social Security numbers (SSNs) from the public. The SAOP/CPO can work with the program manager or system owner to complete the privacy risk assessment. The results of the privacy risk assessment determine whether a PIA or SORN is required. The NIST Risk Management Framework[26] provides a systematic approach for assessing and evaluating risk and should be included as part of the SAOP's/CPO's methodology for identifying risk and implementing appropriate mitigation strategies.

PIAs

Section 208 of the E-Government Act requires federal agencies to conduct PIAs for any new or substantially changed technology that collects, maintains, or disseminates PII.[27] PIAs help

---

[23] *See* discussion below at 12.

[24] For example, the Department of Homeland Security has developed the "Privacy Threshold Analysis" (PTA) and the Department of Justice has developed an "Initial Privacy Assessment" (IPA) to assist them in determining the privacy impact of an activity, system, or program and whether a PIA or SORN is required. Other organizations have discretion to design their own assessment tools to assist with this initial privacy risk determination.

[25] The FIPS 199 impact level – low, moderate, or high, is based on the sensitivity of the information maintained in the system. Systems that collect or maintain PII are designated at least "moderate" for security purposes. *See* FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems.*

[26] *See* NIST Special Publication 800-37 *Guide for Applying the NIST Risk Management Framework to Federal Information Systems, available at* http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final-errata.pdf.

[27] The E-Government Act also requires a PIA prior to initiating, consistent with the Paperwork Reduction Act, a new collection of PII from ten or more individuals in the public. Additionally, the DHS Chief Privacy Officer has statutory authority under section 222 of the Homeland Security Act to conduct PIAs for rulemakings and departmental programs generally, and to ensure that technologies employed at DHS sustain, and do not erode, privacy protections. Section 522 of the Consolidated Appropriations Act of 2005, Division H, Transportation/Treasury also extends the PIA requirement to the rulemaking process. Finally, Congress may require PIAs for specific programs.

ensure that privacy considerations and protections are incorporated into an organization's activities. The PIA is intended to serve as a decision-making tool and should be used in a project's design phase and updated as needed to address significant changes in the project. The PIA assesses how PII is collected, used, disseminated, and maintained and describes the actions taken to mitigate any identified privacy risks. This is the opportunity to incorporate the legal requirements and FIPPs into specific systems or activities.

When a PIA is required, the program manager or system owner works closely with the SAOP/CPO to complete the PIA utilizing any guidance or instructions prepared by the SAOP/CPO. The SAOP/CPO should oversee guidance development for privacy compliance documentation in order to ensure consistent and complete documentation. PIA Guidance should provide a detailed analysis for conducting PIAs and include templates to ensure consistency and accuracy.[28]

SORNs

The SAOP/CPO should oversee the organization's SORN process. The Privacy Act requires federal agencies to issue SORNs for every system of records under their control that collects PII and from which a person's records are retrieved by an identifier. A SORN is a legal document used to promote transparency and provide notice to the public regarding rights and procedures for individuals to access and correct PII maintained by an agency.

To help facilitate the SORN process, the SAOP/CPO should oversee the development and publication of SORN templates and guidance.[29] Each program or IT system should be responsible for identifying the system(s) of records for which it is responsible and completing the SORN process. The SAOP/CPO should work with the program managers or IT system owner to determine if the new system can be covered by an existing SORN or if a new SORN needs to be drafted. The SAOP/CPO should work closely with the project manager and legal counsel to draft new SORNs or update existing SORNs. Legal counsel should perform a final review of each SORN before final approval by the SAOP/CPO.

- Publishing SORNs

The SAOP/CPO should oversee the publishing of all SORNs. SORNs must first be sent to OMB and to Congress for a ten-day comment period and are then published in the *Federal Register* for 30 days to give the public notice and time to comment. A SORN must be published in the *Federal Register* for 30 calendar days prior to the system becoming operational. If comments are filed, the SAOP/CPO should review them with the program manager and legal counsel prior

[28] For example, see DHS' Privacy Impact Assessments Official Guidance at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_guidance_may2007.pdf and DOJ's Privacy Impact Assessment Official Guidance at http://www.justice.gov/opcl/pia_manual.pdf.
[29] For example, see DHS System of Records Notices Official Guidance a*vailable a:t* http://www.dhs.gov/xlibrary/assets/privacy/privacy_guidance_sorn.pdf and Systems of Records Template ,*available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_sorn_template.pdf*.

to publishing the final rule. An updated SORN may be republished along with the final rule to address the comments.[30]

- SORN Review

SORNs must be reviewed at least every two years following publication in the *Federal Register*. OMB requires each SORN to be reviewed every two years to ensure that it accurately describes the system of records. Biennial SORN reviews should be overseen by the SAOP/CPO and include each system of records for which the organization has promulgated exemption rules pursuant to the Privacy Act, to determine whether those exemptions are still needed.[31] Biennial SORN reviews examine the routine uses[32] or categories of approved sharing of information associated with each system of records to ensure that the recipient's use of such records continues to be compatible with the purpose for which the information was collected.[33] Only SORNs requiring changes or updates are re-published.[34]

- Retiring a System of Records

An organization should notify the public whenever a Privacy Act System of Records is retired. A System of Records (whether in electronic or paper form) should be removed from an organization's inventory when it is no longer needed, thereby streamlining management of the organization's systems generally.

The SAOP/CPO should work with the system manager to determine if a System of Records should be retired and to draft a *Notice of Removal of a Privacy Act System of Records* (a "retirement notice"). The retirement notice summarizes what information system is being retired and why, followed by a brief description of what the system was originally designed to collect. The retirement notice should be reviewed and approved by legal counsel and the SAOP/CPO. The notice must also be reviewed by OMB before being published in the *Federal Register*.

[30] The Privacy Act allows organizations to exempt certain records from the access and amendment provisions of the Act. 5 U.S.C. § 522a(j) and § 522a(k). If an organization claims exemptions from the Act's requirements, the organization must issue a Notice of Proposed Rulemaking (NPRM) in the Federal Register for 30 days. A final rule is then published after providing the public with an opportunity to comment on the NPRM.
[31] *See* 5 U.S.C. § 522a(j) and § 522a(k) for a listing of general and specific exemption rules.
[32] The term "routine use" refers to the Privacy Act requirement that records can only be shared outside the agency for a purpose which is compatible with the purpose for which the record was collected. SORNs identify the routine uses for the public.
[33] Organizations may choose to make one annual comprehensive publication consolidating minor changes to SORNs. This requirement is in addition to the requirement to report to OMB and Congress significant changes to systems of records and to publish those changes in the *Federal Register*.
[34] For additional information on the SORN review process, see Appendix I to OMB A-130, *Federal Agency Responsibilities for Maintaining Records about Individuals, available at* www.omb.gov.

Privacy Act (e)(3) Statements

Another responsibility of the SAOP/CPO in many organizations is to oversee the issuing of Privacy Act Statement guidance[35] that provides instructions to personnel on developing Privacy Act Statements required by subsection (e)(3) of the Privacy Act.[36] Privacy Act Statements, or "(e)(3)" Statements, are required on most forms (paper and electronic) that the organization uses to collect PII from members of the public, when the information will be entered into a System of Records. These statements inform individuals at the time their information is collected what the legal authority for and purpose of the collection is, and how the organization will use this information. Privacy Act Statements also notify individuals if providing the information requested is mandatory or voluntary, and the consequences of failing to provide the information.

Computer Matching Agreements

The SAOP/CPO should also oversee the review and approval of the organization's computer matching agreements[37] prior to submission to the organization's Data Integrity Board[38] for the Board's statutory review and approval.[39] The SAOP/CPO should ensure that computer matching agreements include procedures governing the recipient agency's use of information and procedures regarding notification to individuals, information verification, record retention, and records security.

Compliance is the heart of any privacy program. An effective privacy program requires the SAOP/CPO to evaluate potential privacy risks associated with organizational activities and oversee compliance efforts to mitigate those risks while maintaining transparency, mission support, and effective business operations.

[35] For an example of Privacy Act Statement guidance see http://www.dhs.gov/xlibrary/assets/privacy/privacy_guidance_e3.pdf.
[36] *See* 5 U.S.C. § 552a(e)(3).
[37] The Computer Matching and Privacy Protection Act of 1988 (5 U.S.C. § 552a(a)(8)) amended the Privacy Act to require matching agreements before a department can match its data with another federal or state government, either as a recipient or the source of the data. A "matching program" is any computerized comparison of two or more automated systems of records, or a system of records with non-federal records, for the purposes of establishing or verifying the eligibility of, or continuing compliance with statutory and regulatory requirements by, applications for, recipients or beneficiaries of, participants in, or providers of services with respect to, cash or in-kind assistance or payments under federal benefit programs, or recouping payments or delinquent debts under such federal benefit programs, or two or more automated federal personnel or payroll systems of records or a system of federal personnel or payroll records with non-federal records.
[38] The SAOP/CPO should serve as the Chairperson of the organization's Data Integrity Board (DIB), which is responsible for approving and overseeing the organization's use of computer-matching programs. *See* 5 U.S.C. § 552a(u) for more information on Data Integrity Boards.
[39] OMB Circular A-130, Appendix I requires that organization's annually review each ongoing matching program in which the organization participates in order to ensure that the requirements of the Privacy Act, OMB guidance, and any organization regulations, operating instructions, or guidelines have been met.

Element 3 – Information Security

Introduction

Robust privacy and security programs are essential to the protection of PII collected, used, shared, retained, disclosed, and destroyed by the organization. Privacy and security programs are dependent on each other and have complementary objectives. A close partnership between the organization's SAOP/CPO and the organization's CISO is critical to the success of these programs. The SAOP/CPO must keep the CISO informed of current statutory and regulatory privacy protection requirements for PII and provide the CISO with privacy program metrics and related information required to meet the organization's FISMA privacy reporting requirements.[40]

SAOP/CPO Security Responsibilities

In addition to coordinating with the organization's information security leadership, the SAOP/CPO is responsible for providing guidance to the organization for reducing the collection or retention of PII, thereby supporting the CISO's work to enhance information security. Data minimization, one of the FIPPs -- limiting data collection and/or retention to only that information which is necessary and relevant to the mission -- can substantially mitigate the risk of information being compromised, inadvertently exposed, or stolen. If the organization does not need the data, then it should not be collected. In this instance, a "less is more" approach will actually add to information security -- the less information collected the less information is at risk. Records containing PII must be maintained in accordance with NARA and agency approved retention, disposition, and destruction schedules to further support the goals of privacy and security.

The Privacy Act expressly requires that PII be secured. Once an organization approves a policy decision to collect and use PII for a specific authorized purpose, the SAOP/CPO is responsible for implementing comprehensive privacy policies and procedures to ensure the confidentiality, integrity, and availability of that data. The SAOP/CPO is responsible for establishing requirements, including the use of appropriate technologies, for privacy-related data management.

PII Security Controls Required by Statute

The Privacy Act and the E-Government Act give federal organizations responsibilities for protecting PII, including ensuring its security, but other statutes may establish additional requirements for specific organizations or categories of PII, such as health information.[41]

---

[40] Each year, OMB issues a memorandum directing federal agencies to submit information in response to specific privacy questions. The questions may vary year to year. The most recent memorandum is OMB M-09-29, *FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, *available at* http://www.cio.gov/Documents/FY2009_Reporting_FISMA_Privacy_Management.pdf.

[41] E.g. the Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191, 110 Stat. 1936.

FISMA requires organizations to develop, document, and implement organization-wide programs to provide robust security for their information and information systems.[42] The SAOP/CPO plays a key role, in conjunction with the CIO, CISO, the Chief Security Officer, and other officials having privacy related responsibilities, as appropriate, in identifying risks to PII and taking steps to mitigate those risks.

PII Security Controls Required by OMB

OMB issued a series of privacy guidance memoranda in 2006 and 2007 that establish formal organization responsibilities for information security and provide technical guidance, focusing in particular on the Privacy Act and E-Government Act requirements associated with PII.[43] SAOPs/CPOs are specifically responsible for working closely with the CISO, program owners, and information system developers, as necessary, to identify systems containing PII and to ensure that appropriate protections are implemented and monitored. In addition, as discussed in Element 4 below, OMB has taken the lead in providing incident response guidance and promoting use of data loss prevention (DLP) technologies to reduce the risk of data loss.

Security Tied to Information Sensitivity

Although privacy laws and OMB guidance set minimum requirements for protecting PII, some categories of PII may require additional protections, based upon their sensitivity. When appropriate, the SAOP/CPO may determine that, for purposes of privacy risk mitigation, certain personal information maintained by an organization that in itself is not expressly covered by privacy statutes or regulation may still require equivalent security.

For example, a law enforcement organization database that includes covered employee PII such as names, SSNs, birth dates, and emergency contact numbers might also include less sensitive information, e.g., office locations and phone numbers, or other information that if exposed and combined with the more sensitive PII could produce an increased privacy risk. In such cases, an SAOP/CPO may determine that this risk can be effectively mitigated only by providing all categories of PII with the same level of security. Some PII is inherently sensitive, e.g., account information, SSNs, and health information that has not been de-identified. Other PII is sensitive based on its context, including what other information it is linked to it. For example, a list of names may not be particularly sensitive; however, when it is a list of federal air marshals or a list of employees with poor performance evaluations, the list can be very sensitive. NIST Special Publication (SP) 800-122, *Guide for Protecting the Confidentiality of Personally Identifiable*

[42] 44 U.S.C. § 3541–49.
[43] OMB guidance includes but is not limited to: OMB M-06-15, *Safeguarding Personally Identifiable Information;* OMB M-06-16, *Protection of Sensitive Agency Information*; OMB M-06-19, *Reporting Incidents Involving Personally Identifiable Information*; and OMB M-07-16, *Safeguarding against and Responding to the Breach of Personally Identifiable Information*.

Information (PII), which was released in April 2010, provides guidance on protecting PII based on information sensitivity.[44]

Weaknesses Identified in Organization Security Controls for Protecting PII

In June 2009, the Government Accountability Office (GAO) reported that "persistent weaknesses appear in five major categories of federal information system controls: (1) access controls, which ensure that only authorized individuals can read, alter, or delete data; (2) configuration management controls, which provide assurance that only authorized software programs are implemented; (3) segregation of duties, which reduces the risk that one individual can independently perform inappropriate actions without detection; (4) continuity of operations planning, which provides for the prevention of significant disruptions of computer-dependent operations; and (5) an organization-wide information security program, which provides the framework for ensuring that risks are understood and that effective controls are selected and properly implemented."[45] As a result, according to GAO, "federal systems and sensitive information are at increased risk of unauthorized access and disclosure, modification, or destruction, as well as inadvertent or deliberate disruption of system operations and services… and federal organizations continue to experience numerous security incidents that could leave sensitive PII in federal records vulnerable to identity theft."[46] It is the responsibility of the SAOP/CPO to coordinate their organization's privacy information and communication program with the organization's security program (GAO item 5 and Element 3) to ensure a consistent privacy/security message across the organization's management, functions, and employees.

SDLC Planning

It is vital that organizations incorporate security and privacy risk mitigation in the earliest project and lifecycle planning stages, providing project managers with the opportunity to build security and privacy directly into processes and tools. Integrated security and privacy controls are more effective, easier to maintain, and typically have lower lifecycle costs. The SAOP/CPO is responsible for identifying various ways to embed privacy into these SDLC[47] processes. For example, PIAs can provide an opportunity to review implementation of SDLC security practices and assess their adequacy for specific projects and programs.[48]

- **Technology Solutions for Protecting PII**

  The SAOP/CPO can provide expertise in support of the CISO's efforts to use privacy enhancing technologies to mitigate information security risks. For example, organizations should review and implement, to the maximum extent practicable, automated solutions, such as encryption and data loss prevention (DLP) technologies that

[44] *Available at:* http://crsc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf
[45] GAO-09-759T *Identity Theft: Governments Have Acted to Protect Personally Identifiable Information, but Vulnerabilities Remain.*
[46] *Id* at 11.
[47] See Element 2 for additional information on the SDLC process.
[48] Organizations may decide to use other privacy documentation to integrate into the SDLC process.

prevent inadvertent exposure of PII in storage or transmission.[49] Encryption technologies that meet NIST requirements have been used for years to protect PII maintained by federal organizations in data bases or on mobile devices and when transferring data across the Internet. Implementation of this technology, however, may not be complete across an organization.

- **Security Controls**

  Federal organizations covered by FISMA are required to implement, test, and monitor specific management, operations, and technical controls. NIST SP 800-53A, *Recommended Security Controls for Federal Information Systems*, establishes common criteria for assessing the effectiveness of security controls in federal information systems. Organizations use the recommended assessment procedures from NIST SP 800-53A to develop their own assessment procedures.[50] The SAOP/CPO can provide non-technical support to the CISO in implementing security controls in order to protect systems that contain PII.

  Organizations report annually on specific privacy and security activities in their annual FISMA reports to OMB.[51] The SAOP/CPO reports jointly with the CIO in response to a set of questions that may vary each year, based on what OMB determines to be the priority activities for reporting.[52]

Ensuring the security of PII is a top priority of the SAOP/CPO, as failure to do so not only can cause individual harm to those whose information is compromised or lost, but also can cause the organization to suffer significant loss of reputation and loss of public trust. Increasingly, SAOPs/CPOs and their staff work closely with security-related offices to ensure that information security is made a priority at every level.

Security is an essential and fundamental element for a successful privacy program. Security is not limited to the organization's IT security function; it is a primary responsibility of all organization employees with access to PII, in electronic or hard copy format.

Events have shown repeatedly that a single employee can inadvertently defeat well-funded and FISMA-compliant security technologies. The SAOP/CPO, in coordination with the CISO, is responsible for ensuring this message is continuously reinforced in all security-related privacy messaging and training delivered throughout the organization.

---

[49] DLP is also commonly referred to as Data Leakage Protection. Both terms signify the same underlying principles. DLP systems are automated software systems that provide multiple means of scanning IT infrastructure to identify risks to information. For example, DLP systems can scan incoming and outgoing enterprise email traffic for unauthorized or unencrypted transmission of PII.

[50] *See* http://csrc.nist.gov/groups/SMA/fisma/assessment.html.

[51] The most recent memorandum is OMB M-10-15, *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, *available at* http://www.whitehouse.gov/omb/assets/memoranda_2010/m10-15.pdf.

[52] *See* Element 7-Accountability below for more information on reporting requirements.

The SAOP/CPO is responsible for helping to identify and mitigate privacy risks related to the security of PII. Meeting this responsibility requires close coordination with an organization's technical security functions and implementation of a creative communication, training/education, and awareness program that reinforces both the technical information security message and the individual employee's responsibility for protecting privacy and all PII entrusted to the organization.

Element 4 – Incident Response

Introduction

By statute, organizations are responsible for providing information security protections and complying with security standards and guidelines.[53] OMB has stated in its implementing guidance that "[s]afeguarding [PII] in the possession of the government and preventing its breach are essential to ensure the government retains the trust of the American public."[54] Maintaining the public's trust greatly depends on an organization's procedures for detecting, reporting, and responding to privacy incidents involving the suspected or confirmed breach of PII.[55] OMB M-07-16 requires organizations to develop and maintain a privacy incident response policy and notification plan. Even with the implementation and monitoring of privacy and security controls, however, it is impossible to prevent all risks associated with government operations; and it is inevitable that federal organizations will experience privacy incidents. Being prepared to respond to and mitigate these risks before substantial damage is done is critical to the success of a privacy program.

Documentation

Planning and preparing for privacy incidents requires development of reporting and notification procedures for all levels of responders: senior leadership; managers of programs experiencing a breach; SAOP/CPO; CIO; CISO; legal counsel; Office of the Inspector General (OIG); Communications Office; Legislative Affairs Office; the Management Office (including budget and procurement functions); and the information security incident center (help desk). An effective privacy incident response plan also requires educating all employees and contractors on when and how to report privacy incidents.[56]

A privacy incident response plan must, of course, take the potential for security breaches into account. Several NIST publications provide essential guidance for developing security-related aspects of a privacy incident response plan. *Minimum Security Requirements for Federal Information and Information Systems* (FIPS 200), *Standards for Security Categorization of Federal Information and Information Systems* (FIPS 199) and NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations,* provide a framework for categorizing information and information systems, and provide baseline security requirements and security controls for incident handling and reporting. The procedures organizations must use to implement FISMA requirements are found in two primary documents:

[53] *See* FISMA requirements at 44 U.S.C. § 3544(a).
[54] OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*.
[55] In this document, the term "privacy incident" includes, but is not limited to "breaches," as defined in OMB M-07-16.
[56] Employees include all personnel, including any employee, contractor, company, consultant, partner, detailee, or government agency that is performing a federal function on behalf of an agency.

NIST Special Publication 800-61, *Computer Security Incident Handling Guide*;[57] and the Concept of Operations for the United States Computer Emergency Readiness Team (US-CERT), the federal security incident-handling center located within the Department of Homeland Security.[58]

Mechanism for Tracking Privacy Incidents

Organizations should have in place a manual or automated system for tracking privacy incidents to ensure that all are detected, reported, and responded to consistent with the criteria set forth in OMB M-07-16. This guidance identifies the factors to consider and what steps an organization must take to mitigate potential harms. There are seven recommended stages of incident handling: (1) Reporting; (2) Escalation; (3) Investigation; (4) Notification; (5) Mediation; (6) Closure; and (7) Annual Program Review. An organization's structure for incident handling should be designed to restrict the number of reporting tiers to the minimum necessary, while ensuring that officials responsible for safeguarding PII are fully informed of when incidents occur or could occur. The reporting standards and timelines must be followed in order for organizations to mitigate the risk of harm to their systems and to the individuals whose PII has been affected. In order to fulfill tracking and reporting mandates and protect the information and the organization, privacy incident reporting should be given a high priority.

Contingency Planning

Organizations may consider, as part of their privacy incident response plans, using the General Services Administration's (GSA) blanket purchase agreements (BPA) to expedite notification and credit monitoring (or similar services) as needed to protect individuals and the organization, and minimize the impact of privacy incidents. Using a BPA can reduce administrative costs to the government and enable a prompt response to an incident.

OMB M-07-16 requires federal organizations to develop, implement, and publish their policies and procedures for responding to privacy incidents involving PII. Often the organization SAOP/CPO will have the lead responsibility for coordinating investigations and responses.

Breach Notification Policy

As part of its incident response plan, each organization should develop a breach notification policy and plan that incorporates the six factors identified in OMB M-07-16 as critical to considering whether to provide external notification of a breach:

- Whether breach notification to impacted individuals is required;
- Timeliness of the notification;

[57] See *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology* (http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf).
[58] The responsibilities of US-CERT are outlined in 44 U.S.C. § 3546. Its complete set of operating procedures may be found on the US-CERT website *at* www.us-cert.gov/federal/reportingRequirements.html.

- Source of the notification;
- Contents of the notification;
- Means of providing the notification; and,
- Who should receive notification -- public outreach in response to a breach.[59]

To implement the breach notification policy and plan, each organization should establish a breach response team. The team should include the manager of the program affected by the breach, the SAOP/ CPO, the CIO, the Communications Officer, Legislative Affairs Officer, legal counsel, and the management officer responsible for budget and procurement functions. Roles and responsibilities should clearly delineate the responsibilities of personnel, program managers, security managers, and senior leadership for:

- Reporting suspected or confirmed incidents involving PII;
- Convening the breach response team to determine the appropriate course of action in the event of a privacy incident; and
- Notifying US-CERT[60] and, as necessary, affected individuals, appropriate organization staff offices, the Inspector General, Congress, law enforcement, and the press. Organizations must report all suspected and confirmed incidents involving PII to US-CERT within one hour.

To determine whether notification is required, the organization should first assess the likely risk of harm caused by the breach and then assess the level of risk. Organizations should exercise care in evaluating the benefit of notifying the public of low impact incidents. OMB M-07-16 provides guidance on the five factors that should be considered: (1) the nature of the data elements breached; (2) the number of individuals affected; (3) the likelihood that the information is accessible and usable; (4) the likelihood the breach may lead to harm; and (5) the organization's ability to mitigate the risk of harm.

When considering the likelihood that a breach may lead to harm (e.g., loss of the information could result in identity theft or fraud), organizations should consider the guidance provided by the President's Identity Theft Task Force.[61] The impact levels identified by the Task Force will help determine when and how notification should be provided. By appropriately applying the five risk factors, it is likely notification will be given only in those instances where there is a reasonable risk of harm. Organizations should keep in mind that notification when a breach poses little or no risk of harm could create unnecessary concern and confusion.

[59] OMB M-07-16, *Safeguarding Against & Responding to Breach of Personally Identifiable Information*.
[60] Id.
[61] OMB, Executive Office of the President, *Recommendations for Identity Theft Related Data Breach Notification* (Sep. 26, 2009), *available at* www.whitehouse.gov/omb/memoranda/fy2006/task_force_theft_memo.pdf

In general, organizations should consider the timeliness, source, and contents of all notifications, and the media to be used. After applying the risk factors above, organizations should provide notification without unreasonable delay following the discovery of a breach, consistent with the needs of law enforcement, national security, and any measures necessary to determine the scope of the breach and, if applicable, to restore the integrity of the computerized data system compromised before notification is given. Decisions to delay notification should be made in writing by an organization's senior leadership. Similarly, written notification to individuals and the public should be issued by the organization head, or a senior-level individual. The contents of the notification should be concise, conspicuous, and in plain language. The best means for providing notification will depend on the number of individuals impacted and what contact information is available. OMB M-07-16 provides additional explanation and guidance to assist the SAOP/CPO in carrying out this important responsibility.

Technologies

Where possible, organizations should leverage automated incident-reporting tools. The use of such tools will help enforce organizational requirements for reporting, promote accuracy, and provide an archival repository through which organizations can conduct various analyses of their privacy programs. For example, DLP tools can support the identification and reporting of certain electronic locations of PII, or the sharing of unprotected (e.g., unencrypted) PII through email going out to the Internet. Web scanning tools can assist the SAOP/CPO in identifying compliance issues related to PII collected or unintentionally exposed on the organization's externally-facing web sites.

Privacy incident management and response can be a telling indicator for measuring the effectiveness of an organization's privacy program. The SAOP/CPO should work with the CIO/CISO to ensure that privacy incidents are reported. The SAOP/CPO should also assist the CIO/CISO in identifying, investigating, and mitigating any privacy breaches resulting from a security breach.

Element 5 – Notice and Redress for Individuals

Introduction

As required by the Privacy Act, organizations must establish and publish in the Federal Register redress policies and procedures to enable individuals to request access to information federal organizations collect about them. Organizations must also facilitate the amendment or correction of data that is not accurate, relevant, timely, or complete.[62]

Notice

The SAOP/CPO is responsible for ensuring that organizations provide notice to the public - through Privacy Act Statements, online and other public-facing privacy policies, PIAs, and SORNs - about how a program, system, or technology will impact their privacy. For example, the notice will describe how PII will be used, shared, retained, disclosed, and destroyed. In general, notice should be provided prior to and/or at the time of information collection or creation, unless otherwise directed by applicable laws, directives, policies, or regulations.

Notice should inform individuals about (1) what information is being collected; (2) the purpose of the collection; (3) how the information is used; (4) to whom the information is disclosed and shared; (5) individuals' rights under the Privacy Act to access and amend or correct their records to the extent practicable; and (6) the types of redress programs available. To the extent practicable, notice should also state how long the information is retained and what the consequences are for failure to provide the information requested.

Organizations are encouraged to supplement traditional notice methods with more transparent methods outlined in OMB M-10-06, *Open Government Directive* (e.g., webpage(s), organization-designated Open Government Webpage).[63]

Managing Privacy Complaints and Redress

As noted above, the Privacy Act requires organizations to make public information regarding procedures for an individual to access his or her information and to correct or amend inaccurate information. Organizations should also have in place policies and procedures for managing privacy complaints or inquiries. Such procedures should ensure that all complaints are recorded, tracked, and addressed.[64] Where feasible, organizations should establish an automated tracking process to capture and manage privacy complaints, to promote compliance with written policies and procedure, and to ensure all complaints are addressed.

---

[62] 5 U.S.C. § 552a(d).
[63] *Available at* http://www.whitehouse.gov/omb/assets/memoranda_2010/m10-06.pdf.
[64] OMB M-08-21 *FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management* requires organizations to include in their FISMA report the number of written privacy complaints and divides them into the following categories: Process and Procedural, Redress, Operational, and Referrals (July 14, 2008). Accurate categorization and reporting of complaints can also aid in directing education and training resources to mitigate areas of greatest concern.

Organizations should also address, where applicable, procedures for coordinating redress among the entities that control the information in question or who are the nexus of the complaint.

An organization should provide avenues for effective redress for the misuse or mishandling of personal information or to correct inaccurate PII. An organization's procedures should allow individuals to have their PII corrected or amended and allow individuals to seek redress for privacy-related complaints and violations involving the processing of their information. Redress policies and procedures should facilitate the public's ability to file a complaint online, by mail, or facsimile and to provide for a speedy evaluation and response. In addition, redress should be commensurate with the harm, if any, involved with the loss or misuse of PII by the organization.

Redress can include amending or correcting a person's PII, or in the case of a PII breach, providing credit monitoring or identity theft protection. Examples of redress can also include implementing or amending existing organization policies or changing procedures in a way that addresses the concerns raised by a complainant or enhancing the manner in which the organization protects employee PII to prevent future privacy incidents. If administrative redress options are not sufficient, the Privacy Act provides individuals with the right to bring civil actions to compel monetary redress or further administrative action.[65]

Documentation

The SAOP/CPO should play a leading role in defining robust redress policies and procedures for an organization. These policies and procedures should include clearly defined roles and responsibilities and provide detailed complaint/resolution procedures including the following:

- Procedures for providing information to the public, in plain language and easy-to-read formats, that explain redress seekers rights, the process for complaining or seeking redress and appealing adverse decisions, a general timeline for the process, and the privacy policy regarding the personal information used in the process; [66]
- A training program that educates employees, contractors, vendors, and others as appropriate about the redress policies, procedures, standards, and access points;
- A description of the overall complaint and redress process including: how to submit a request for access to information or to file a complaint regarding the misuse or mishandling of information; the information required to process the request or complaint; and the ways in which complaints can be submitted to the organization (e.g., mail, email, telephone, website application, etc.);
- Establishing service standards for logging and responding to redress requests and appeals in a timely manner;

[65] 5 U.S.C § 552a(g).
[66] Organizations should develop information on their redress procedures in languages appropriate for the people seeking redress.

- Procedures for ensuring that annotations and corrections are propagated throughout all primary and secondary systems, to prevent the same information from producing adverse impacts in the future;
- Procedures for appealing the organization's initial determination that emphasize impartiality, transparency, and fairness; and
- Record management procedures to ensure the redress request is handled appropriately throughout the redress process.

Reporting

Organizations should track privacy complaints for purposes of internal and external reporting. This information should be used to identify areas within an organization that may require further review or education and training.

Notice and redress are essential to implementing transparency and individual participation – two fundamental fair information practice principles.

Element 6 – Privacy Training and Awareness

Introduction

Privacy training and awareness programs are key elements of building a culture of privacy throughout an organization. Training programs test and reinforce the implementation of privacy policy, providing a critical element of an effective privacy program. The SAOP/CPO has primary responsibility for ensuring that federal employees and contractors receive mandated privacy training. Training and awareness programs can provide valuable feedback to help refine and improve privacy management and reduce the risk of privacy incidents throughout the organization.

Mandatory Training

OMB M-07-16 requires that:

> "all agencies must initially train employees (including managers) on their privacy and security responsibilities before permitting access to organization information and information systems. Thereafter, agencies must provide at least annual refresher training to ensure employees continue to understand their responsibilities. Additional or advanced training should also be provided commensurate with increased responsibilities or change in duties.
>
> Both initial and refresher training must include acceptable rules of behavior and the consequences when the rules are not followed. For agencies implementing telework and other authorized remote access programs, training must also include the rules of such programs."[67]

Mandatory privacy training can be provided during new hire orientation or coincide with other existing activities, such as ethics training, but must be job-specific and commensurate with employees' responsibilities.

The SAOP/CPO should oversee mandatory privacy training program development and ensure that it addresses compliance with the Privacy Act, E-Government Act, other privacy-specific requirements and guidance,[68] and organization policies, procedures, and penalties for violations. Annual training should cover safeguards for protecting personal information, and for reporting and responding to incidents involving the breach of PII. Organizations should track mandatory training through the use of registration sheets, signed acknowledgment forms, or online acknowledgements and periodic checks.

[67] *See* OMB M-07-16, Attachment 1, Section A.2.d.
[68] Agency privacy-specific requirements could include, for example, HIPAA, the Health Information Technology for Economic and Clinical Health (HITECH) Act, and the Children's Online Privacy Protection Act (COPPA).

Role-based Training for Employees and Contractors

OMB M-07-16 requires that organizations provide targeted, role-based training to managers, Privacy Act Officers and individuals with privacy responsibilities as needed to fulfill specific privacy management responsibilities.[69] Additional or advanced training should be provided, commensurate with increased responsibilities or changes in duties, to those employees and contractors who handle PII. An organization should provide advanced training to ensure that individuals are fully aware of privacy protection requirements specific to the data and records they process and as outlined in the applicable SORN and /or PIAs. Privacy training should be provided commensurate with clearly defined roles and: (1) before authorizing access to the information system or performing assigned duties; (2) when required by system changes; and (3) as the sensitivity of the PII warrants.

Awareness Training

Organizations should augment privacy training for all individuals with creative methods that promote ongoing awareness of privacy and security responsibilities (e.g. mouse pads, placards, weekly tips). Privacy awareness programs usually focus on and enforce broad topics, such as how to identify new risks, how to mitigate privacy risks, and how and when to report privacy incidents. Awareness programs can also be interactive and thematic in order to generate employee interest. For example, organizations can hold privacy weeks or campaigns where employee activities are centered on a relevant privacy theme (e.g., securing PII) and employees engage in activities related to the privacy theme. Awareness training can even include periodic broadcast messages or emails reminding employees of an organization's privacy policies, addressing a recent incident, or informing employees of a recent change in law that affects privacy.

Training Delivery Systems

Where feasible, the SAOP/CPO should work with the CIO to offer privacy and awareness training online via computer-based training (CBT) or an internal learning management system (LMS)/training delivery system (TDS). CBT has many benefits including the ability to systematically track and verify compliance with privacy training requirements. CBT also allows an organization to tailor privacy training based on staff level, position, and access to PII and accommodates busy schedules by giving employees the flexibility to conduct training at their own pace. CBT can be interactive and, if desired, can give instant feedback as to whether a person understood the topics covered and can apply them using real-life scenarios.

Privacy training and awareness help build a culture of privacy within the organization. Employees and contractors can be the weak link in the chain if not properly trained and educated to protect privacy.

[69] *See* OMB M-07-16, Attachment 4, Section A

Element 7 – Accountability

Introduction

Accountability is a key principle of the FIPPs and the FEA-SPP Privacy Control Families. The organization, under the direction of the SAOP/CPO, is accountable for compliance with all applicable privacy protection requirements, including all legal authorities and established policies and procedures that protect privacy and govern the collection, use, dissemination, and maintenance of PII. This also includes auditing for the use of PII to demonstrate compliance with established privacy controls. Accountability through effective monitoring and measurement controls builds public trust by demonstrating that an organization is complying with all of its applicable privacy protection requirements.

At the core, organizations are accountable for identifying enterprise, program, and system-specific roles and responsibilities for ensuring that Elements 1 through 6 are successfully executed. In turn, when successfully implemented, each Element itself includes aspects of accountability as follows:

- **Element 1: Leadership**: The organization is responsible for designating a senior-level official as the SAOP/CPO. The SAOP/CPO is accountable to the organization for overseeing the implementation of a robust privacy program that includes the adoption of policies, procedures, and privacy documentation consistent with applicable laws and regulations.
- **Element 2: Privacy Risk Management and Compliance Documentation**: The organization is accountable for identifying privacy risk in its business processes and IT systems and for implementing mechanisms to ensure the organization documents its compliance with laws, regulations, and policies governing the protection of privacy. The organization is accountable for applying a risk-based approach to the management of privacy.
- **Element 3: Information Security**: The organization is accountable for protecting PII that it collects, uses, shares, retains, discloses, and destroys, through appropriate administrative, technical, and physical safeguards.
- **Element 4: Incident Response**: The organization is accountable for having a robust plan for managing incidents involving the potential or actual leakage of PII that includes notification to appropriate senior management and members of the public where appropriate.
- **Element 5: Notice and Redress for Individuals**: The organization is accountable for providing transparency through clear notice to the public about the organization's information handling practices and mechanisms for individual participation to ensure appropriate access, correction, and redress regarding the use of PII.

- **Element 6: Privacy Training and Awareness**: The organization is accountable for implementing its privacy policies and procedures by providing comprehensive and job-specific training for employees and contractors on their PII handling and protection responsibilities.

Additional aspects of accountability include:

- Establishing a Data Integrity Board to oversee and coordinate computer-matching agreements consistent with the Privacy Act.[70]
- Establishing system access agreements before authorizing individual access to personal information and rules of behavior that describe users' responsibilities and expected behavior with regard to information and information system usage.
- Ensuring accountability through various reporting requirements to OMB and Congress and through internal senior management reporting as described below.
- Enforcing accountability through employee performance appraisals, contract clauses, contract awards, and contract performance assessments.

Organizations also are accountable directly to the public for the privacy protections published in SORNs, PIAs, online privacy policies, Privacy Act Statements, and other public documents.

Assessments and Auditing

Organizations may elect to perform self-assessments of activities involving PII to ensure compliance with privacy laws, regulations, internal policies, and any other established privacy controls. The assessments may encompass an entire business process or focus on a single information system or vendor processing PII. An assessment project may involve documenting (through data flow maps) the people, processes, and technologies affecting the flow and use of PII, as well as performing a legal and policy gap analysis and providing a mitigation strategy. The resulting assessment report is useful for providing management and the SAOP/CPO with key insights into business activities requiring further scrutiny for privacy issues. The SAOP/CPO is generally responsible for performing assessments or overseeing assessments performed by staff or a qualified contractor.

Organizations may elect to perform unannounced, self-assessment "walk-throughs" of offices or programs in order to review compliance with policies and procedures requiring the protection of PII in paper or electronic form. Such assessments could result in findings brought to management's attention. Organizations may also engage an internal or external entity to perform an audit of their privacy efforts to verify and demonstrate that they have met legal and policy requirements as well as any other established privacy controls. Audit findings should be provided to senior management to ensure appropriate action is taken to mitigate any identified risks.

[70] 5 U.S.C. § 552a(u).

Organizations must dedicate the appropriate resources necessary to perform internal and/or external assessments and audits, particularly for any high-risk program areas.

Reporting Requirements

Accountability also includes measuring an organization's ability to manage, use, and handle PII, and ensuring accountability for meeting these responsibilities in accordance with privacy laws, regulations, and organization policies and procedures.

Reporting on the status of an organization's privacy program is critical to—

- measure the organization's progress in meeting compliance requirements;
- provide a means of comparing performance across the federal government; and,
- identify vulnerabilities and gaps in policy implementation.

Internal and external reporting is a typical requirement to ensure full accountability. In some instances, automated tools can be utilized to support reporting requirements.

Internal Reporting

Organizations may elect to require internal reporting. Internal reporting may take several forms, such as weekly or monthly reporting to senior management on privacy program activities and progress. Organizations also may require sub-organization or component program progress and compliance reporting to their individual leadership as well as to the SAOP/CPO. Organizations should review incident reporting data at least quarterly to assess both enterprise and component compliance.

External Reporting

FISMA requires each federal agency to develop, document, and implement an agency-wide information security program.[71] Organizations are required to report quarterly and annually to OMB their progress in conducting PIAs and issuing SORNs for IT systems that are required to go through FISMA C&A.[72] OMB requires organizations to use an automated system for submitting reports, thereby enabling OMB to track, monitor, and report to Congress and the public on the progress made by individual organizations in their management of privacy. An organization's quarterly and annual FISMA reports include statistics on required and completed PIAs and SORNs for systems that are operational or that are registered in the organization's FISMA inventory system.

In addition to the above PIA and SORN requirements, OMB requires specific information in the Annual FISMA reports related to privacy. As early as 2009, examples of such reporting requirements have included:

[71] 44 U.S.C. § 3541–49.
[72] *Id.*

- SAOP Responsibilities;
- Information on privacy training and awareness;
- Written privacy policies and procedures;
- Reviews mandated by the Privacy Act, E-Government Act, and the Federal Agency Data Mining Reporting Act of 2007;
- Written privacy complaints;
- Policy compliance reviews;
- Advice provided by the SAOP;
- Agency use of persistent tracking technology;[73] and
- Information on privacy points of contact.

External reporting may also include responding to requests from an organization's OIG or from the GAO seeking information and documentation that demonstrates compliance with applicable privacy laws and regulations.

Certain SAOPs/CPOs may also be required to ensure accountability through other reporting requirements mandated by Congress, such as those set out in the Federal Agency Data Mining Reporting Act for federal agencies that conduct data mining as defined in that Act[74] and section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007.[75] Organizations with multiple privacy reporting requirements should leverage, to the extent possible, existing data calls and reporting lines to streamline the reporting process and reduce the overall administrative burdens on the organization. External reporting requirements should be assessed and incorporated into the organization's privacy compliance responsibilities.

Organizations are responsible for implementing policies, procedures, and programs to protect privacy and PII. Organizations are therefore also required to ensure effective implementation of those policies, procedures, and programs. Organizations can ensure effective implementation through a robust audit and accountability program. A robust audit and accountability program is one that has the requisite audits, reviews, reports, and reporting lines in place to routinely test, measure, and assess the effectiveness of privacy protections.

[73] On June 25, 2010, OMB issued new guidance related to federal organizations' online activities: *Guidance for Online Use of Web Measurement and Customization Technologies* (Memorandum No. M-10-22); and *Guidance for Agency Use of Third-Party Websites and Applications* (Memorandum No. M-10-23). Federal SAOP/CPOs should be prepared to address any instructions on FISMA reporting that may result from the issuance of this new guidance.
[74] 42 U.S.C. § 2000ee-3.
[75] 42 U.S.C. § 2000ee-1.

Conclusion

The elements discussed in this guide serve as a roadmap for organizations wishing to implement a robust privacy program or improve an existing program. These elements are also useful to organizations seeking to appoint an SAOP/CPO or identify the responsibilities for a potential SAOP/CPO. The elements are based on the FEA-SPP Privacy Control Families, and the FIPPs. They reflect best practices identified by those who have experience managing the day-to-day operations of leading federal privacy programs.

Privacy and issues surrounding the protection of PII will continue to be a factor for federal organizations as technologies advance and programs that require the collection, use, storage, dissemination and destruction of PII proliferate. As a result, organizations will be required to assess their privacy protection needs and quickly and effectively identify and implement sound privacy practices. Implementing the elements outlined in this document will assist organizations in fulfilling those requirements while ensuring accountability to the affected individuals and to the general public.

Appendix I: Frequently Used Abbreviations and Acronyms

Acronym List	
C&A	Certification and Accreditation
CBT	Computer-Based (or Web-Based) Training
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COTS	Commercial Over the Counter Software
CPO	Chief Privacy Officer
DLP	Data Loss Prevention
DIB	Data Integrity Board
FACA	Federal Advisory Committee Act
FEA-SPP	Federal Enterprise Architecture – Security and Privacy Profile
FIPPs	Fair Information Practice Principles
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
GAO	Government Accountability Office
ISSO	Information System Security Officer
IT	Information Technology
NARA	National Archives and Records Administration
NIST	National Institutes of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
PAO	Privacy Act Officer
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PTA	Privacy Threshold Analysis
SAOP	Senior Agency Official for Privacy
SDLC	System Development Life Cycle
SOR	System of Records
SORN	Systems of Records Notice
SPII	Sensitive Personally Identifiable Information
SSN	Social Security Number
US-CERT	United States Computer Emergency Readiness Team

Appendix II: Laws, Directives, OMB and NIST Guidance, and GAO Reports

Each organization will have its own legally and policy-based compliance requirements. The following is a comprehensive but not complete list of requirements sources that generally apply to all federal organizations. Their applicability is dependent upon the organization's mission and mandates.

Federal Requirements[76]

Administrative Procedure Act (5 U.S.C. §§ 551, 554-558)

Bank Secrecy Act (31 U.S.C. §§ 5311-5330, 31 C.F.R. § 103)

Census Confidentiality Statute (13 U.S.C. § 9)

Children's Online Privacy Protection Act of 1998 (15 U.S.C. §§ 6501 et seq., 16 C.F.R. § 312)

Communications Assistance for Law Enforcement (47 U.S.C. § 1001)

Computer Security Act (40 U.S.C. § 1441)

Confidential Information Protection and Statistical Efficiency Act of 2002 (Pub. L. No. 107-347, Title V, Dec. 17, 2002, 116 Stat. 2962)

Criminal Justice Information Systems (42 U.S.C. § 3789g)

Drug and Alcoholism Abuse Confidentiality Statutes (21 U.S.C. § 1175; 42 U.S.C. § 290dd-3)

Employee Polygraph Protection Act (29 U.S.C. § 2001, et seq.)

E-Government Act of 2002 (Pub. L. No. 107-347, 116 Stat. 2899)

Family Educational Rights and Privacy Act ("FERPA", 20 U.S.C. § 1232g; 34 C.F.R § 99)

Federal Agency Data Mining Reporting Act of 2007 (42 U.S.C. § 2000ee-3)

Federal Records Act of 1950 (44 U.S.C. Ch 31)

Federal Information Security Management Act of 2002 ("FISMA", 44 U.S.C. § 3541, et seq.)

Freedom of Information Act ("FOIA", 5 U.S.C. § 552)

Gramm-Leach-Bliley Act ("GLBA", Pub. L. No. 106-102, 113 Stat. 1338)

Health Insurance Portability and Accountability Act of 1996 ("HIPAA", Pub. L. No. 104-191)

Health Information Technology for Economic and Clinical Health Act ("HITECH Act", 42 U.S.C. §§ 300jj et seq.; 17901 et seq.)

Homeland Security Presidential Directive-12 (HSPD-12): *Policies for Common Identification Standard for Federal Employees and Contractors*

[76] http://uscode.house.gov/.

Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (42 U.S.C. § 2000ee-1)

Intelligence Reform and Terrorism Prevention Act (Pub. L No. 108-458)

Paperwork Reduction Act of 1980 (44 U.S.C. § 3501, et seq.)

Privacy Act of 1974, as amended (5 U.S.C. § 552a)

Right to Financial Privacy Act (12 U.S.C. § 3401 et seq.)

Sarbanes-Oxley Act of 2002 (Pub. L. No. 107-204, 116 Stat. 745)

Tax Reform Act (26 U.S.C. §§ 6103, 6108, 7609)

Section 522 of the Transportation, Treasury, and Independent Agencies, and General Government Appropriations Act of 2005 (Pub. L. No. 108-447, div. H, Dec. 8, 2004, 118 Stat. 2809)

Office of Management and Budget (OMB) Guidance[77]

Privacy Act Implementation (July 9, 1975)

Privacy Act Responsibilities for Implementing the Personal Responsibility and Work Opportunity Reconciliation Act of 1996 (November 3, 1997)

M-99-05, *Instructions on Complying with President's Memorandum of May 14, 1998, "Privacy and Personal Information in Federal Records"* (January 7, 1999)

Biennial Privacy Act and Computer Matching Reports (June 1998)

M-99-18, *Privacy Policies on Federal Web Sites* (June 2, 1999)

OMB Circular A-130, Appendix I, *Federal Agency Responsibilities for Maintaining Records About Individuals* (2000)

Status of Biennial Reporting Requirements under the Privacy Act and the Computer Matching and Privacy Protection Act (June 21, 2000)

M-00-13, *Privacy Policies and Data Collection on Federal Web Sites* (June 22, 2000) *(Rescinded by OMB M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies (June 25, 2010))*

Letter from Roger Baker to John Spotila on Federal agency use of Web cookies (July 28, 2000)

Letter from John Spotila to Roger Baker, clarification of OMB Cookies Policy (September 5, 2000)

M-01-05, *Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy* (December 20, 2000)

M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* (September 30, 2003)

M-05-04, *Policies for Federal Agency Public Websites* (December 17, 2004)

[77] www.omb.gov.

M-05-08, *Designation of Senior Agency Officials for Privacy* (February 11, 2005)

M-05-15, *FY 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management* (June 13, 2005)

M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors* (August 5, 2005).

M-06-15, *Safeguarding Personally Identifiable Information* (May 22, 2006)

M-06-16, *Protection of Sensitive Agency Information* (June 23, 2006)

M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments* (July 12, 2006)

M-06-20, *FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management* (July 17, 2006)

Recommendations for Identity Theft Related Data Breach Notification (September 20, 2006)

M-07-16, *Safeguarding Against & Responding to Breach of Personally Identifiable Information* (May 22, 2007)

M-07-19, *FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management* (July 25, 2007)

M-07-20, *FY 2007 E-Government Act Reporting Instructions* (August 14, 2008)

M-08-09, *New FISMA Privacy Reporting Requirements for FY 2008* (January 18, 2008)

M-08-21, *FY 2008 Reporting Instructions for the FISMA and Agency Privacy Management* (July 14, 2008)

M-09-29, *FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management* (August 20, 2009)

M-10-06, *Open Government Directive* (December 8, 2009)

M-10-22, *Guidance for Online Use of Web Measurement and Customization Technologies* (June 25, 2010)

M-10-23, *Guidance for Agency Use of Third-Party Websites and Applications* (June 25, 2010)

National Institute of Standards and Technology (NIST) Guidance[78]

FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems* (February 2004)

FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems* (March 2006)

NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook* (October 1995)

[78] http://csrc.nist.gov/

NIST SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems* (September 1998)

NIST SP 800-16, *Information Technology Security Training Requirements* (April 1998)

NIST SP 800-30, *Risk Management Guide for Information Technology Systems* (July 2002)

NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems* (February 2010)

NIST SP 800-39, *DRAFT Managing Risk from Information Systems: An Organizational Perspective, Second Public Draft* (April 2008)

NIST SP 800-50, *Building Information Technology Security Awareness and Training Program* (October 2003)

NIST SP 800-53, *Recommended Security Controls for Federal Information Systems* (Rev. 3, August 2009)

NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems* (July 2008)

NIST SP 800-59, *Guideline for Identifying an Information System as a National Security System* (August 2003)

NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories* (August 2008)

NIST SP 800-61, *Computer Security Incident Handling Guide* (March 2008)

NIST SP 800-64, *Security Considerations in the System Development Lifecycle* (October 2008)

NIST SP 800-83, *Guide to Malware Incident Prevention and Handling* (November 2005)

NIST SP 800-100, *Information Security Handbook: A Guide for Managers* (October 2006)

NIST SP 800-122, *Guide to Protecting the Confidentiality of PII* (April 2010).

Government Accountability Office (GAO) Reports[79]

GAO-09-759T, *Governments Have Acted to Protect PII, but Vulnerabilities Remain*

GAO-09-136, *Continued Efforts Needed to Address Significant Weaknesses at IRS*

GAO-08-795T, *Congress Should Consider Alternatives for Strengthening Protection of PII*

GAO-08-536, *Alternatives Exist for Enhancing Protection of Personally Identifiable Information*

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

GAO-07-935T, *Agencies Report Progress, but Sensitive Data Remain at Risk*

GAO-07-870, *DHS Needs to Immediately Address Significant Weaknesses in Systems Supporting US-VISIT*

[79] http://www.gao.gov/

GAO-07-837, *Despite Reported Progress, Federal Agencies Need to Address Persistent Weaknesses*

GAO-07-751T, *Persistent Weaknesses Highlight Need for Further Improvement*

GAO-07-657, *Lessons Learned about Data Breach Notification*

GAO-07-1003T, *Homeland Security Needs to Enhance Effectiveness of Its Program*

GAO-06-897T, *Leadership Needed to Address Weaknesses and Privacy Issues at Veterans Affairs*

GAO-06-866T, *Leadership Needed to Address Information Security Weaknesses and Privacy Issues*

GAO-06-833T, *Preventing and Responding to Improper Disclosures of Personal Information*

Selected Federal Privacy Resources

Federal Identity Management Homepage, http://www.idmanagement.gov

Information Sharing Environment Privacy Guidelines, www.ise.gov

Internal Revenue Service Privacy Policy Homepage, www.irs.gov/privacy

OMB MAX Homepage, https://max.omb.gov/maxportal/

U.S. Census Bureau, Data Protection and Privacy Policy Homepage, www.census.gov/privacy

U.S. Department of Defense, Defense Privacy Office, http://privacy.defense.gov/govwide/U.S. Department of Energy Privacy Homepage, http://management.energy.gov/FOIA/privacy.htm

U.S. Department of Justice, Office of Justice Programs, *Justice Information Sharing Privacy and Civil Liberties,* www.it.ojp.gov/default.aspx?area=privacy&page=1265

U.S. Department of Justice, Office of Privacy and Civil Liberties, Privacy Act of 1974 Overview (2010), www.justice.gov/opcl/1974privacyact-overview.htm

U.S. Department of Homeland Security Privacy Office Homepage, www.dhs.gov/privacy

U.S. Department of Health & Human Services Privacy Act Homepage, www.hhs.gov/foia/privacy

U.S. Department of the Interior Privacy Program, http://www.doi.gov/ocio/privacy/DOI_Privacy_guidelines_and_references.html

U.S. General Services Administration Privacy Act System of Records Notices, http://www.gsa.gov/Portal/gsa/ep/contentView.do?contentType=GSA_BASIC&contentId=21567

U.S. Office of Personnel Management, http://www.opm.gov/feddata/html/privacy.asp

U.S. Postal Service Privacy Office Homepage, www.usps.com/privacyoffice