

NIST Special Publication 800-53
DRAFT APPENDIX J



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

Security and Privacy Controls for Federal Information Systems and Organizations

(Proposed Title Change)

I N F O R M A T I O N S E C U R I T Y

Caution: This draft Privacy Appendix is intended to become part of NIST Special Publication 800-53, Revision 4, when the document is updated in December 2011. The material is being released for public review and comment and will be modified accordingly prior to final publication.

INITIAL PUBLIC DRAFT

APPENDIX J: PRIVACY CONTROL CATALOG

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

July 2011



U.S. Department of Commerce
Gary Locke, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Director

Notes to Reviewers

With the increasing dependency on information systems, dramatic advances in information technologies, and significant growth in new applications of those technologies in such areas as cloud computing, Smart Grid, and mobile computing, information security and privacy are taking on new levels of importance in the public and private sectors. Privacy, with respect to personally identifiable information, is a core value that can be achieved only with appropriate legislation, policies, and associated controls to ensure compliance with requirements. In today's digital world, effective privacy for individuals depends on a solid foundation of information security safeguards in the information systems that are processing, storing, and transmitting personally identifiable information. Privacy and security controls in federal information systems, programs, and organizations are complementary and mutually reinforcing in trying to achieve the privacy and security objectives of organizations.

Appendix J, *Privacy Control Catalog*, is a new addition to NIST's family of standards and guidelines that will be incorporated into the 2011 update to Special Publication 800-53, Revision 4, projected for release in December 2011. Due to the importance and special nature of the material in this Appendix, it is being publicly vetted separately from the other changes to the publication which will be released later this year. The objectives of the Privacy Appendix are fourfold:

- Provide a structured set of privacy controls, based on international standards and best practices, that help organizations enforce requirements deriving from federal privacy legislation, policies, regulations, directives, standards, and guidance;
- Establish a linkage and relationship between privacy and security controls for purposes of enforcing respective privacy and security requirements which may overlap in concept and in implementation within federal information systems, programs, and organizations;
- Demonstrate the applicability of the NIST Risk Management Framework in the selection, implementation, assessment, and monitoring of privacy controls deployed in federal information systems, programs, and organizations; and
- Promote closer cooperation between privacy and security officials within the federal government to help achieve the objectives of senior leaders/executives in enforcing the requirements in federal privacy legislation, policies, regulations, directives, standards, and guidance.

Reviewers will observe a strong similarity in the structure of the privacy controls in Appendix J and the security controls in Appendix F. Moreover, the use of privacy plans in conjunction with security plans will provide an opportunity for organizations to select the appropriate set of security and privacy controls in accordance with organizational mission/business requirements and the environments in which the organizations operate. Incorporating the principles and concepts associated with managing information security risk, ensures that the employment of privacy controls is both effective in meeting compliance requirements and doing so in a cost-effective, risk-based manner. In addition to the basic privacy controls described in the Appendix, NIST plans to develop appropriate assessment procedures to allow organizations to evaluate the effectiveness of the controls. Standardized privacy controls and assessment procedures will provide a more disciplined and structured approach for satisfying federal privacy requirements and demonstrating compliance to those requirements.

Your feedback to us, as always, is important. We appreciate each and every contribution from our reviewers. The very insightful comments from both the public and private sectors continue to help shape our publications and ensure that they meet the needs of our customers.

-- RON ROSS
PROJECT LEADER
FISMA IMPLEMENTATION PROJECT
JOINT TASK FORCE TRANSFORMATION INITIATIVE

Acknowledgements

This publication was developed by the National Institute of Standards and Technology and the Privacy Committee of the Federal Chief Information Officer (CIO) Council. In particular, we wish to thank the members of the Privacy Committee's Best Practices Subcommittee and its Privacy Controls Appendix Working Group—Claire Barrett, Chris Brannigan, Pamela Carcirieri, Debra Diener, Deborah Kendall, Martha Landesberg, Steven Lott, Lewis Oleinick, and Roanne Shaddox—for their valuable insights, subject matter expertise, and overall contributions in helping to develop the content for this appendix to Special Publication 800-53. We also wish to recognize and thank Erika McCallister, Toby Levin, James McKenzie, Julie McEwen, and Richard Graubart for their significant contributions to this project. A special note of thanks goes to Peggy Himes and Elizabeth Lennon for their superb technical editing and administrative support. The authors also gratefully acknowledge and appreciate the significant contributions from individuals, groups, and organizations in the public and private sectors, whose thoughtful and constructive comments improved the overall quality, thoroughness, and usefulness of this publication.

Draft

Public comment period: July 19 through September 2, 2011

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Electronic mail: sec-cert@nist.gov

APPENDIX J

PRIVACY CONTROL CATALOG

PRIVACY CONTROLS, ENHANCEMENTS, AND SUPPLEMENTAL GUIDANCE

Protecting the privacy of personally identifiable information (PII)¹ collected, used, maintained, shared, and disposed of by federal programs and information systems is a fundamental responsibility of federal organizations.² This Appendix complements the security controls described in Appendix F and provides a structured set of controls for protecting privacy.³ It also serves as a roadmap for organizations to use in identifying and implementing privacy controls concerning the entire life cycle of PII, whether in paper or electronic form.⁴ The controls focus on information privacy as a value distinct from, but highly interrelated with, information security. Organizations cannot have effective privacy without a solid foundation of information security. However, privacy is more than security and confidentiality and includes the principles of transparency and notice and choice, for example. The privacy controls are based on the Fair Information Practice Principles (FIPPs) embodied in the Privacy Act of 1974, the E-Government Act of 2002 (Section 208), and related Office of Management and Budget (OMB) guidance.⁵ They are designed to build public trust in an organization's privacy practices and to help organizations avoid tangible costs and intangible damages stemming from privacy incidents.

Privacy controls are the administrative, technical, and physical safeguards employed within an organization to protect PII. The privacy control families are intended to be implemented at the organizational, departmental, agency, component, office, program, or information system level, under the privacy leadership of the organization (e.g., Senior Agency Official for Privacy [SAOP], Chief Privacy Officer [CPO]), and in coordination with Chief Information Security

¹OMB Memorandum M-07-16 *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, defines PII 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. NIST Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, defines PII as any information about an individual maintained by an agency, including: (i) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (ii) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. Organizations' definitions of PII may vary based on the consideration of additional regulatory requirements. The privacy controls in this Appendix are intended to apply regardless of an organization's definition of PII.

² The term *organization* means an entity of any size, complexity, or positioning within an organizational structure (e.g., a federal agency or, as appropriate, any of its operational elements).

³ In 2010, the Federal CIO Council Privacy Committee issued a framework for designing and implementing a privacy program entitled *Best Practices: Elements of a Federal Privacy Program (Elements White Paper)*. The privacy controls in this Appendix mirror a number of the elements included in the Elements White Paper. An organization's privacy leadership can use the privacy controls and the guidance included in the Elements White Paper to develop a robust organization-wide privacy program or enhance an already existing program.

⁴ Although NIST Special Publication 800-53 is primarily about protecting information, organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy risks or concerns. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary.

⁵ The FIPPs are widely accepted in the United States and internationally as a general framework for privacy and are reflected in other federal and international laws and policies. In a number of organizations, FIPPs serve as the basis for analyzing privacy risks and determining appropriate mitigation strategies. The Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) also provided information and materials in development of the privacy controls.

Officers, Chief Information Officers, program officials, and legal counsel. In general, privacy controls are implemented within organizations as common controls. Such controls are inherited by multiple information system owners. Table J-1 provides a summary of the privacy controls by family in the privacy control catalog.⁶

TABLE J-1: SUMMARY OF PRIVACY CONTROLS BY FAMILY

CNTL NO.	PRIVACY CONTROLS
TR	Transparency
TR-1	Privacy Notice
TR-2	Dissemination of Privacy Program Information
IP	Individual Participation and Redress
IP-1	Consent
IP-2	Access
IP-3	Redress
IP-4	Complaint Management
AP	Authority and Purpose
AP-1	Authority to Collect
AP-2	Purpose Specification
DM	Data Minimization and Retention
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
UL	Use Limitation
UL-1	Internal Use
UL-2	Information Sharing
UL-3	System Design and Development
DI	Data Quality and Integrity
DI-1	Data Quality
DI-2	Data Integrity
SE	Security
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
AR	Accountability, Audit, and Risk Management
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-4	Privacy Monitoring and Auditing
AR-5	Privacy Awareness and Training
AR-6	Privacy Reporting

⁶ Security controls in the eighteen families in Appendix F are characterized as management, operational, or technical controls. Privacy controls in the eight families in this Appendix, similar to the Program Management (PM) controls in Appendix F, are characterized as management controls.

HOW TO USE THIS APPENDIX

The privacy controls outlined in this publication are primarily for use by organizational privacy officials (e.g., SAOPs, CPOs) when working with program managers, information system developers, information technology project staff, and information security personnel to determine how best to incorporate effective privacy protections and practices (i.e., privacy controls) within those programs and/or systems. These controls facilitate the organization's efforts to comply with privacy requirements affecting those programs and/or systems that collect, use, maintain, share, or dispose of personally identifiable information (PII).

Organizations analyze and apply each privacy control with respect to their distinct mission and operational needs based on their legal authorities and obligations. Implementation of the privacy controls may vary based upon this analysis. This enables organizations to determine the information practices that are compliant with law and policy and those that may need review. It also enables organizations to tailor the privacy controls to meet their defined and specific needs at the organization level, the information system level, and the program level. Organizations with national security or law enforcement authorities take those authorities as well as privacy interests into account in determining how to apply the privacy controls in their operational environments.

Draft

FAMILY: TRANSPARENCY**CLASS: MANAGEMENT**

This family implements Sections 552a (e)(3) and (e)(4) of the Privacy Act and Section 208 of the E-Government Act, which require public notice of an organization's information practices and the privacy impact of government programs and activities.

TR-1 PRIVACY NOTICE

Control: The organization:

- a. Provides effective notice to the public and to individuals regarding: (i) its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of personally identifiable information (PII); (ii) authority for collecting PII; (iii) the choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices; and (iv) the ability to access and have PII amended or corrected if necessary;
- b. Describes: (i) the PII the organization collects and the purpose(s) for which it collects that information; (ii) how the organization uses PII internally; (iii) whether the organization shares PII with external entities and the purposes for such sharing; (iv) whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; (v) how individuals may obtain access to PII for the purpose of having it amended or corrected, where appropriate; and (vi) how the PII will be protected;
- c. Revises its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy; and
- d. Ensures (e.g., through updated public notice) that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.

Supplemental Guidance: Effective notice, by virtue of its clarity and comprehensiveness, enables individuals to understand how an organization uses PII generally and, where appropriate, to make an informed decision prior to providing PII to an organization. Effective notice also demonstrates the privacy considerations that the organization has addressed in implementing its information practices. The organization may provide general public notice through a variety of means, as required by law or policy, including System of Records Notices (SORNs), Privacy Impact Assessments (PIAs), in a Web site privacy policy, or in an Information Sharing Privacy Policy. As required by the Privacy Act, the organization also provides direct notice to individuals via Privacy Act Statements on the paper and electronic forms it uses to collect PII.

Organizational SAOPs/CPOs are responsible for the content of the organization's public notices, in consultation with legal counsel and relevant program managers. The public notice requirement in this control is satisfied by an organization's compliance with the public notice provisions of the Privacy Act, the E-Government Act's PIA requirement, with OMB guidance related to federal agency privacy notices, and, where applicable, with policy pertaining to participation in the Information Sharing Environment (ISE). Related controls: AC-8, AP-1, AP-2, IP-1, IP-2, IP-3, PL-5, UL-1, UL-2.

Control Enhancements:

- (1) The organization provides real-time (i.e., at the point of collection) notice when it collects PII.**

References: The Privacy Act of 1974, 5 U.S.C. §§ 552a (e)(3), (e)(4); Public Law 107-347, E-Government Act of 2002, as amended, Section 208(b); OMB Memoranda 03-22, 07-16, 10-22, 10-23; ISE Privacy Guidelines.

TR-2 DISSEMINATION OF PRIVACY PROGRAM INFORMATION

Control: The organization:

- a. Ensures that the public has access to information about its privacy activities and is able to communicate with its privacy officials; and
- b. Ensures that its privacy practices are published in PIAs and SORNs and that all publicly available privacy reports and newsletters are made available either through organizational Web sites or otherwise.

Supplemental Guidance: Privacy officials include, for example, the SAOP and CPO. Organizations employ different mechanisms for informing the public about their privacy practices including, but not limited to, publicly available Web pages, blogs, email distributions, and periodic publications (e.g., quarterly newsletters). The organization also employs a publicly facing email address or phone line that enables the public to provide feedback or direct questions to the privacy office regarding privacy practices. Related controls: AR-6.

Control Enhancements: None.

References: None.

Draft

FAMILY: INDIVIDUAL PARTICIPATION AND REDRESS**CLASS: MANAGEMENT**

This family addresses the need to make individuals active participants in the decision-making process regarding the collection and use of their PII, as required by the Privacy Act. By providing individuals with access to PII and the ability to have their PII corrected or amended, as appropriate, the controls in this family enhance public confidence in organizational decisions made based on the PII.

IP-1 CONSENT

Control: The organization:

- a. Provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of PII prior to its collection;
- b. Provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination and retention of PII; and
- c. Obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII.

Supplemental Guidance: Consent is fundamental to individuals' participation in the decision-making process regarding the collection and use of their PII and the use of technologies that may increase risks to personal privacy. To obtain consent, organizations provide individuals both appropriate notice of the purposes of the PII collection or technology use and a means for individuals to consent to the activity. Organizations tailor the public notice and consent mechanisms to meet operational needs.

Organizations may obtain consent through opt-in, opt-out, or implied consent. Opt-in consent requires individuals to take affirmative action to *allow* organizations to collect or use PII. Opt-out requires individuals to take action to *prevent* the collection or use of such PII. Implied consent occurs where individuals' behavior or failure to object indicates agreement with the collection or use of PII (e.g., by entering and remaining in a building where notice has been posted that security cameras are in use, the individual implies consent to the video recording). Depending upon the nature of the program or information system, it may be appropriate to allow individuals to limit the types of PII they provide and subsequent uses of that PII. Organizational consent mechanisms include a discussion of the consequences to individuals for failure to provide PII. Consequences can vary from organization to organization. Related control: TR-1.

Control Enhancements:

- (1) The organization implements mechanisms to support itemized or tiered consent for specific uses of data.**

Enhancement Supplemental Guidance: For example, organizations can provide individuals itemized choices as to whether they wish to be contacted for any of a variety of purposes. In this situation, organizations construct consent mechanisms to ensure that the organizational operations comply with individual choices.

References: The Privacy Act of 1974, Section 552a (b); Public Law 107-347, E-Government Act of 2002, as amended, Section 208(c); OMB Memoranda 03-22, 10-22.

IP-2 ACCESS

Control: The organization provides individuals the ability to have access to their PII maintained in its system(s) of records in order to determine whether to have the PII corrected or amended, as appropriate.

Supplemental Guidance: Access affords individuals the ability to review PII about them held within organizational systems of records. Access includes timely, simplified, and inexpensive access to

data. Organizational processes for allowing access to records may differ based on legal requirements, resources, or other factors. Organizations: (i) publish rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records; (ii) publish their access procedures in SORNs; and (iii) adhere to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests. Organizational SAOPs/CPOs are responsible for the content of Privacy Act regulations and record request processing, in consultation with legal counsel. Related controls: IP-3, TR-1.

Control Enhancements: None.

References: The Privacy Act of 1974, Section 552a (d); OMB Circular A-130.

IP-3 REDRESS

Control: The organization:

- a. Provides a process for individuals to have inaccurate PII maintained by the organization corrected or amended, as appropriate; and
- b. Establishes a process for disseminating corrections or amendments of the PII to other authorized users of the PII, such as external information sharing partners, and, where feasible and appropriate, notifies affected individuals that their information has been corrected or amended.

Supplemental Guidance: Redress supports the ability of individuals to ensure the accuracy of PII held by organizations. Effective redress processes demonstrate organizational commitment to data quality especially in those business functions where inaccurate data may result in inappropriate decisions or denial of benefits and services to individuals. Organizations apply appropriate discretion in determining if records are to be corrected or amended, based on the scope of redress requests, the changes sought, and the impact of the changes.

To provide effective redress, organizations: (i) provide effective notice of the existence of a PII collection; (ii) provide plain language explanations of the processes and mechanisms for requesting access to records; (iii) establish criteria for submitting requests for correction or amendment; (iv) implement resources to analyze and adjudicate requests; (v) implement means of correcting or amending data collections; and (vi) review any decisions that may have been the result of inaccurate information.

Organizational redress processes provide responses to individuals of decisions to deny requests for correction or amendment, including the reasons for those decisions, a means to record individual objections to the organizational decisions, and a means of requesting organizational reviews of the initial determinations. Where PII is corrected or amended, organizations take steps to ensure that all authorized recipients of that PII are informed of the corrected or amended information. In instances where redress involves information obtained from other organizations, redress processes include coordination with organizations that originally collected the information. Related controls: IP-2, TR-1, UL-2.

Control Enhancements: None.

References: The Privacy Act of 1974, Section 552a (d); OMB Circular A-130.

IP-4 COMPLAINT MANAGEMENT

Control: The organization implements a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices.

Supplemental Guidance: Complaints, concerns, and questions from individuals can serve as a valuable source of external input that ultimately improves operational models, uses of technology, data collection practices, and privacy and security safeguards. Organizations provide complaint mechanisms that are readily accessible by the public, include all information necessary for successfully filing complaints (including contact information for the SAOP/CPO or other official

designated to receive complaints), and are easy to use. Organizational complaint management processes include tracking mechanisms to ensure that all complaints received are reviewed and appropriately addressed in a timely manner. Related controls: AR-6, IP-3.

Control Enhancements: None.

References: OMB Circular A-130; OMB Memoranda 07-16, 08-09.

Draft

FAMILY: AUTHORITY AND PURPOSE**CLASS: MANAGEMENT**

This family furthers compliance with the Privacy Act by ensuring that organizations: (i) identify the legal bases that authorize a particular PII collection or activity that impacts privacy; and (ii) specify the purpose(s) for which they collect PII in their notices.

AP-1 AUTHORITY TO COLLECT

Control: The organization determines the legal authority that permits the collection, use, maintenance, and sharing of PII, either generally or in support of a specific program or information system need.

Supplemental Guidance: Before collecting PII in connection with an information system or program, the organization determines whether the contemplated collection of PII is legally authorized. Program officials consult with the SAOP/CPO and legal counsel regarding the authority of any program or activity to collect PII. Related controls: AR-5, DM-1, TR-1.

Control Enhancements: None.

References: The Privacy Act of 1974, Section 552a (e)(3)(A); Public Law 107-347, E-Government Act of 2002, as amended, Section 208(c).

AP-2 PURPOSE SPECIFICATION

Control: The organization describes the purpose(s) for which PII is collected, used, maintained, and shared in its privacy notices.

Supplemental Guidance: Often, statutory language expressly authorizes specific collections and uses of PII. When statutory language is written broadly and thus subject to interpretation, organizations ensure, in consultation with the SAOP/CPO and legal counsel, that there is a close nexus between the general authorization and any specific collection of PII. Once the specific purposes have been identified, they are clearly described in the related privacy compliance documentation, including but not limited to PIAs, SORNs, and Privacy Act Statements on forms organizations use to collect PII. Further, in order to avoid unauthorized collections or uses of PII, personnel who handle PII receive training on the organizational authorities for collecting PII and on the contents of the notice. Related controls: AR-4, AR-5, TR-1, UL-4.

Control Enhancements: None.

References: The Privacy Act of 1974, Section 552a (e)(3)(A)-(B); Public Law 107-347, E-Government Act of 2002, as amended, Section 208(b), (c).

FAMILY: DATA MINIMIZATION AND RETENTION**CLASS: MANAGEMENT**

This family assists organizations in implementing the data minimization and retention elements of the Privacy Act, which requires organizations to collect, use, and retain only PII that is relevant and necessary for the specified purpose for which it was originally collected. Organizations retain PII for only as long as necessary to fulfill the specified purpose(s) and in accordance with a National Archives and Records Administration (NARA)-approved record retention schedule.

DM-1 MINIMIZATION OF PERSONALLY IDENTIFIABLE INFORMATION

Control: The organization:

- a. Identifies the minimum PII elements (e.g., name, address, date of birth) that are relevant and necessary to accomplish the legally authorized purpose of collection;
- b. Limits the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent; and
- c. Conducts an initial evaluation and performs periodic evaluations of its holdings of PII to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.

Supplemental Guidance: The collection of PII is consistent with a purpose authorized by law or regulation. The minimum set of PII elements required to support a specific organization business process may be a subset of the PII the organization is authorized to collect. Program officials consult with the SAOP/CPO and legal counsel to identify the minimum PII elements required by the information system or activity to accomplish the legally authorized purpose.

Organizations can further reduce their privacy and security risks by also reducing their inventory of PII, where appropriate. OMB Memorandum 07-16 requires organizations to conduct both an initial review, and subsequent reviews of their holdings of all PII and ensure, to the maximum extent practicable, that such holdings are accurate, relevant, timely, and complete. Organizations are also directed by OMB to reduce their holdings to the minimum necessary for the proper performance of a documented organizational business purpose. Reductions in organizational holdings of PII are consistent with NARA retention schedules.

By performing periodic evaluations, organizations reduce risk, ensure that they are collecting only the data specified in the notice, and ensure that the data collected is still relevant and necessary for the purpose(s) specified in the notice. Related controls: AP-2, AR-4, IP-1, IP-2, IP-3, TR-1, SI-12.

Control Enhancements:

- (1) **Where feasible and within the limits of technology, the organization locates and removes or redacts specified PII and/or uses anonymization and de-identification techniques to permit use of the retained information while reducing its sensitivity and reducing the risk resulting from disclosure.**

Enhancement Supplemental Guidance: NIST Special Publication 800-122 provides guidance on anonymization.

References: The Privacy Act of 1974, Section 552a (e)(1), (e)(2); Public Law 107-347, E-Government Act of 2002, as amended, Section 208(b); OMB Memoranda 03-22, 07-16.

DM-2 DATA RETENTION AND DISPOSAL

Control: The organization:

- a. Retains PII for only as long as is necessary to fulfill the purpose(s) identified in the notice or as required by law;
- b. Appropriately disposes of PII when it is no longer necessary to retain it;

- c. Systematically destroys, erases, and/or anonymizes the PII, regardless of the method of storage (e.g., electronic, optical media, or paper-based) in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and
- d. Uses audits and appropriate technology to ensure secure deletion or destruction of PII (including originals, copies, and archived records).

Supplemental Guidance: NARA provides retention schedules that govern the disposition of federal records containing PII. Program officials coordinate with records officers and with NARA to identify appropriate retention periods and disposal methods. NARA may require organizations to retain PII longer than is operationally needed. In those situations, organizations describe such requirements in the notice.

Examples of ways organizations may reduce holdings include reducing the types of PII held (e.g., delete Social Security numbers if their use is no longer needed) or shortening the retention period for PII that is maintained if it is no longer necessary to keep PII for long periods of time (this effort is undertaken in consultation with an organization's records officer to receive NARA approval). In both examples, organizations provide notice (e.g., an updated SORN) to inform the public of any changes in holdings of PII. OMB Memorandum 07-16 requires organizations to develop and publicize, either through a notice in the Federal Register or on their Websites, a schedule for periodic reviews of their holdings to supplement the initial review.

Certain read-only archiving techniques, such as DVDs, CDs, microfilm, or microfiche may not permit the removal of individual records without the destruction of the entire database contained on such media. Related controls: AR-4, AU-11, DM-1, MP-6, SI-12, TR-1.

Control Enhancements: None.

References: The Privacy Act of 1974, 552a (e)(1); Public Law 107-347, E-Government Act of 2002, as amended, Section 208 (e); 44 U.S.C. Chapters 29, 31, 33; OMB Circular A-130; OMB Memorandum 07-16; NIST Special Publication 800-88.

FAMILY: USE LIMITATION**CLASS: MANAGEMENT**

This family is intended to assist organizations in complying with the Privacy Act, which prohibits uses of PII that are either not specified in notices, incompatible with the specified purposes, or not otherwise permitted by law. Implementation of the Controls in this Family will ensure that the scope of PII use is limited accordingly.

UL-1 INTERNAL USE

Control: The organization uses PII internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices.

Supplemental Guidance: Organizations take steps to ensure that they use PII only for legally authorized purposes and in a manner compatible with uses identified in the Privacy Act and/or in its public notices. These steps include monitoring and auditing organizational use of PII, and training organizational personnel on the authorized uses of PII. With guidance from privacy officials (i.e., SAOPs/CPOs) and where appropriate, legal counsel, organizations document processes and procedures for evaluating any proposed new uses of PII to assess whether they fall within the scope of the organizational authorities. Where appropriate, organizations obtain consent from individuals for the new use(s) of PII. Related controls: AP-2, AR-4, AR-5, IP-1, TR-1.

Control Enhancements: None.

References: The Privacy Act of 1974, Section 552a (b)(1).

UL-2 INFORMATION SHARING

Control: The organization:

- a. Shares PII with third parties, including other public and private sector entities, only for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or in a manner compatible with those purposes;
- b. Where appropriate, enters into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, or similar agreements, with third parties that specifically enumerate the purposes for which PII may be used;
- c. Monitors, audits, and trains its staff on the authorized uses and sharing of PII with third parties; and
- d. Establishes and implements a process for evaluating any proposed new instances of sharing PII with third parties to assess whether they are authorized and whether additional or new public notice is required.

Supplemental Guidance: The organization's SAOP/CPO and, where appropriate, legal counsel review and approve any proposed external sharing of PII for consistency with uses described in the existing organizational public notice(s). Where a new instance of external sharing of PII is authorized but not compatible with the purpose(s) specified in existing public notices, or as otherwise permitted by the Privacy Act, the organization reviews, updates, and republishes its PIA, SORN, Web site privacy policy, and other public notices, if any, to include specific descriptions of the new uses(s). Information-sharing agreements also include security protections consistent with the sensitivity of the information being shared. Related controls: AR-4, AR-5, AP-2, DI-2, TR-1.

Control Enhancements: None.

References: The Privacy Act of 1974, Section 552a (b), (c), (e)(3)(C), (o); ISE Privacy Guidelines.

UL-3 SYSTEM DESIGN AND DEVELOPMENT

Control: The organization designs information systems to collect, use, maintain, and share PII only for the authorized purposes specified in the Privacy Act and/or organizational public notice(s) or for uses compatible with those purposes.

Supplemental Guidance: To the extent feasible, when designing new information systems the organization employs technologies that automate privacy controls on the collection, use, and disclosure of PII. By building privacy controls into system design, the organization mitigates privacy risks to PII, thereby reducing the likelihood of system breaches and other privacy incidents. The organization also conducts periodic reviews of the collection, use, and disclosure of PII to assess compliance with the Privacy Act and the organization's privacy policy. Regardless of whether the organization employs automated privacy controls, it regularly monitors system use and sharing of PII to ensure that it is consistent with the authorized purposes identified in the Privacy Act and/or in the organization's public notice, or in a manner compatible with those purposes. Related controls: AC-6, AR-4, AR-5, TR-1.

Control Enhancements: None.

References: Public Law 107-347, E-Government Act of 2002, as amended, Section 208(b), (c); OMB Memorandum 03-22.

Draft

FAMILY: DATA QUALITY AND INTEGRITY**CLASS: MANAGEMENT**

This family ensures compliance with Section 552a (e)(2) of the Privacy Act of 1974 and enhances public confidence that any PII collected and maintained by the organization is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in the public notice.

DI-1 DATA QUALITY

Control: The organization:

- a. Confirms to the extent feasible upon collection or creation of PII, the accuracy, relevance, timeliness, and completeness of that PII;
- b. Collects PII directly from the individual to the greatest extent practicable;
- c. Checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems; and
- d. Issues guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.

Supplemental Guidance: Organizations take reasonable steps to confirm the accuracy of PII. Such steps may include, for example, editing and validating addresses as they are collected or entered into information systems using automated address verification look-up application programming interfaces (APIs). The types of measures taken to protect data quality may be based on the nature and context of the PII, how it is to be used, and how it was obtained. The measures taken to validate the accuracy of PII that is used to make determinations about the rights, benefits, or privileges of individuals under federal programs may be more comprehensive than those used to validate less sensitive PII. Additional steps may be necessary to validate PII that is obtained from sources other than individuals or the authorized representatives of individuals.

When PII is of a sufficiently sensitive nature (e.g., when it is used for annual reconfirmation of a taxpayer's income for a recurring benefit), organizations incorporate mechanisms into information systems and develop corresponding procedures for how frequently, and by what method, the information is to be updated. Related controls: IP-3, SI-10.

Control Enhancements:

- (1) **Where feasible, the organization's systems are configured to record the date PII is collected, created, or updated and when PII is to be deleted or archived under an approved record retention schedule.**

References: The Privacy Act of 1974, Section 552a (e)(5); OMB Memorandum 07-16; Treasury and General Government Appropriations Act for Fiscal Year 2001 (Public Law 106-554, app C § 515, 114 Stat. 2763A-153-4); Paperwork Reduction Act (44 U.S.C. § 3501 et seq.); OMB Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies.

DI-2 DATA INTEGRITY

Control: The organization:

- a. Documents processes to ensure the integrity of PII through existing security controls; and
- b. Establishes a Data Integrity Board when appropriate, to oversee organizational computer matching agreements and to ensure that those agreements comply with the computer matching provisions of the Privacy Act.

Supplemental Guidance: Organizations conducting or participating in computer matching agreements with other organizations regarding applicants for and recipients of financial assistance or payments under federal benefit programs, and applicants for and holders of positions as federal personnel, establish a Data Integrity Board to oversee and coordinate their implementation of such matching

agreements. In many organizations, the Data Integrity Board is led by the SAOP/CPO. The Data Integrity Board ensures that controls are in place to maintain both the quality and the integrity of data shared under computer matching agreements. Related controls: AC-1, AC-3, AC-4, AC-6, AC-17, AU-2, AU-3, AU-6, AU-10, AU-11, DI-1, SC-8, SC-9, SI-9, UL-2.

Control Enhancements: None.

References: The Privacy Act of 1974, Section 552a (u); OMB Circular A-130, Appendix I.

Draft

FAMILY: SECURITY**CLASS: MANAGEMENT**

This family supplements the security controls in Appendix F to ensure administrative, technical, and physical measures are in place to protect PII collected or maintained by organizations against loss, unauthorized access, or disclosure, as required by the Privacy Act, and to ensure that organizational planning and responses to privacy incidents comply with OMB policies and guidance. The controls in this family are implemented in coordination with information security personnel using the existing NIST Risk Management Framework.

SE-1 INVENTORY OF PERSONALLY IDENTIFIABLE INFORMATION

Control: The organization:

- a. Establishes, maintains, and regularly updates a PII inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing PII; and
- b. Provides each update of the PII inventory to the CIO or other information security officials to support the establishment of appropriate information security requirements for all new or modified information systems containing PII.

Supplemental Guidance: The PII inventory enables organizations to implement effective administrative, technical, and physical security policies and procedures to protect PII consistent with Appendix F, and to mitigate risks of PII exposure. As one method of gathering information for its PII inventory, organizations may extract the following information elements from PIAs of information systems containing PII: (i) the name and acronym for each system identified; (ii) the types of PII contained in that system; (iii) classification of level of sensitivity of all types of PII, as combined in that system; and (iv) classification of level of potential risk for damage to affected individuals and organizations if PII is exposed. Related controls: AR-1, AR-4, AR-5, AT-1, DI-2, DM-1, PM-5, UL-2, UL-3, UL-4.

Control Enhancements: None.

References: The Privacy Act of 1974, Section 552a (e) (10); Public Law 107-347 E-Government Act of 2002, as amended, Section 208(b)(2); OMB Memorandum 03-22; OMB Circular A-130, Appendix I; NIST Special Publications 800-37, 800-122.

SE-2 PRIVACY INCIDENT RESPONSE

Control: The organization:

- a. Develops and implements a Privacy Incident Response Plan; and
- b. Provides an organized and effective response to incidents of unauthorized exposure of organization-controlled PII, in accordance with the organizational Privacy Incident Response Plan.

Supplemental Guidance: In contrast to the Incident Response (IR) family in Appendix F, which concerns a broader range of incidents affecting information security, this control uses the term Privacy Incident to describe only those incidents which relate to PII. An organizational Privacy Incident Response Plan includes: (i) the establishment of a cross-functional Privacy Incident Response Team that reviews, approves, and participates in the execution of the Privacy Incident Response Plan; (ii) a process to determine whether notice to affected individuals is required and, where appropriate, to provide that notice; (iii) a privacy risk assessment process to determine the extent of harm to affected individuals; and (iv) internal procedures to ensure prompt reporting by employees and contractors of any privacy incident to information security officials and privacy officials (i.e., SAOPs/CPOs), consistent with organizational incident management structures. Related controls: AR-1, AR-4, AR-5, AR-6, AU-1 through 14, IR-1 through 8, RA-1.

Control Enhancements: None.

References: The Privacy Act of 1974, Section 552a (e), (i)(1), and (m); The Federal Information Security Management Act of 2002 (FISMA, 44 U.S.C. § 3541, *et seq.*); OMB Memoranda 06-19, 07-16; NIST Special Publication 800-37.

Draft

FAMILY: ACCOUNTABILITY, AUDIT, AND RISK MANAGEMENT**CLASS:** MANAGEMENT

This family is intended to enhance public confidence through effective governance controls, monitoring controls, risk management, and assessment controls to demonstrate that an organization is complying with all applicable privacy protection requirements and minimizing its overall privacy risk.

AR-1 GOVERNANCE AND PRIVACY PROGRAM

Control: The organization:

- a. Appoints an SAOP/CPO accountable for developing, implementing, and maintaining an organization-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of PII by programs and information systems;
- b. Allocates [*Assignment: organization-defined allocation of budget and staffing resources*] to implement and operate the organization-wide privacy program;
- c. Develops, disseminates, and implements privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII;
- d. Develops a privacy plan for implementing applicable privacy controls, policies, and procedures; and
- e. Updates privacy plan, policies, and procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: The development and implementation of a comprehensive governance and privacy program demonstrates organizational accountability for and commitment to the protection of individual privacy. Accountability begins with the appointment of SAOPs/CPOs with the mission, resources, and responsibility to develop and implement a multifaceted privacy program. SAOPs/CPOs, in consultation with legal counsel and information security officials: (i) ensure the development, implementation, and enforcement of privacy policies and procedures; (ii) define roles and responsibilities for protecting PII; (iii) determine the level of information sensitivity with regard to PII holdings; (iv) identify the laws, regulations, and internal policies that apply to the PII; and (v) monitor and audit compliance with identified privacy controls.

To further accountability, the SAOPs/CPOs develop privacy plans to document the privacy requirements of organizations and the privacy and security controls in place or planned for meeting those requirements. The plan serves as evidence of organizational privacy operations and supports resource requests by SAOPs/CPOs. A single plan or multiple plans may be necessary depending upon the organizational structures, requirements, and resources, and the plan(s) may vary in comprehensiveness. For example, a one-page privacy plan may cover privacy policies, documentation, and controls already in place, such as PIAs and SORNs. A comprehensive plan may include a baseline of privacy controls selected from this Appendix and include: (i) processes for conducting privacy risk assessments; (ii) templates and guidance for completing PIAs and SORNs; (iii) privacy training and awareness requirements; (iv) requirements for contractors processing PII; (v) plans for eliminating unnecessary PII holdings; and (vi) a framework for measuring annual performance goals and objectives for implementing identified privacy controls.

Control Enhancements: None.

References: The Privacy Act of 1974, Section 552a; Public Law 107-347, E-Government Act of 2002, as amended; Federal Information Security Management Act of 2002 (FISMA, 44 U.S.C. § 3541, *et seq.*); OMB Memoranda 03-22, 05-08, 07-16; OMB Circular A-130; Federal Enterprise Architecture Security and Privacy Profile.

AR-2 PRIVACY IMPACT AND RISK ASSESSMENT

Control: The organization:

- a. Establishes a privacy risk assessment process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, and use of personally identifiable information;
- b. Conducts a Privacy Impact Assessment (PIA) for information systems and programs in accordance with OMB policy and any existing organizational policies and procedures; and
- c. Follows a documented, repeatable process for conducting, reviewing, and approving Privacy Impact Assessments.

Supplemental Guidance: Organizational privacy risk assessment processes operate across the life cycles of all mission/business processes that collect, use, maintain, share, or dispose of PII. OMB Memorandum 03-22 provides guidance to organizations for implementing the privacy provisions of the E-Government Act of 2002, including guidance on when PIAs are required for information systems. Some organizations may be required by law or policy to extend the PIA requirement to other activities involving PII or otherwise impacting privacy, for example, programs, projects, or regulations. PIAs are conducted to identify privacy risks and identify methods to mitigate those risks. PIAs are also conducted to ensure that programs or information systems comply with legal, regulatory, and policy requirements. PIAs also serve as notice to the public of privacy practices. PIAs are performed before developing or procuring information systems, or initiating programs or projects, that collect, use, maintain, or share PII and are updated when changes create new privacy risks. Related control: PL-5.

Control Enhancements: None.

References: Public Law 107-347, E-Government Act of 2002 (Section 208); OMB Memoranda 03-22, 05-08; Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. § 3541, *et seq.*

AR-3 PRIVACY REQUIREMENTS FOR CONTRACTORS AND SERVICE PROVIDERS

Control: The organization:

- a. Establishes and monitors compliance of privacy requirements including privacy roles and responsibilities for contractors and service providers; and
- b. Includes privacy requirements in contracts and other acquisition-related documents.

Supplemental Guidance: Contractors and service providers include, but are not limited to, service bureaus, information processors, and other organizations providing information system development, information technology services, and other outsourced applications. Organizations consult with legal counsel, the SAOP/CPO, and contracting officers about applicable laws, directives, policies, or regulations that may impact implementation of this control.

Control Enhancements: None.

References: OMB Circular A-130.

AR-4 PRIVACY MONITORING AND AUDITING

Control: The organization monitors and audits privacy controls, federal privacy laws and policy, and internal privacy policy [*Assignment: organization defined frequency*] to ensure effective implementation.

Supplemental Guidance: To promote accountability, organizations identify and address gaps in privacy compliance, management, operational, and technical controls by conducting regular assessments (e.g., internal risk assessments). These assessments can be self-assessments or third-

party audits that result in reports on compliance gaps identified in programs, projects, and information systems. In addition to auditing for effective implementation of all privacy controls identified in this Appendix, organizations assess whether they: (i) implement a process to embed privacy considerations into the life cycle of programs, information systems, mission/business processes, and technology; (ii) monitor for changes to applicable privacy laws, regulations, and policies; (iii) track programs, information systems, and applications that collect and maintain PII to ensure compliance; (iv) ensure access to PII is only on a *need-to-know* basis; and (v) ensure PII is being maintained and used only for the legally authorized purposes identified in the public notice(s).

Organizations also: (i) implement technology to audit for the security, appropriate use, and loss of PII; (ii) perform reviews to ensure physical security of documents containing PII; and (iii) assess contractor compliance with privacy requirements. Organizational SAOPs/CPOs coordinate monitoring and auditing efforts with information security officials and ensure that the results are provided to senior managers and oversight officials. Related controls: AR-6, AU-1, AU-2, AU-3, AU-6, AU-12, TR-1, UL-2.

Control Enhancements: None.

References: The Privacy Act of 1974, Section 552a; Public Law 107-347, E-Government Act of 2002, as amended, Section 208; OMB Memoranda 03-22, 05-08, 07-16.

AR-5 PRIVACY AWARENESS AND TRAINING

Control: The organization:

- a. Develops, implements, and updates: (i) a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures; and (ii) targeted, role-based training for personnel with significant PII responsibilities; and
- b. Ensures that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements.

Supplemental Guidance: Through implementation of a privacy training and awareness strategy, the organization promotes a culture of privacy. Privacy training and awareness programs typically focus on broad topics, such as responsibilities under the Privacy Act of 1974 and E-Government Act of 2002, how to identify new privacy risks, how to mitigate privacy risks, and how and when to report privacy incidents. Privacy training may also target data collection and use requirements identified in public notices, such as PIAs or SORNs for a program or information system. Specific training methods may include: (i) mandatory annual privacy awareness training; (ii) targeted, role-based training; (iii) internal privacy program Websites; (iv) manuals, guides, and handbooks; (v) slide presentations; (vi) events (e.g., privacy awareness week, privacy clean-up day); (vii) posters and brochures; and (viii) email messages to all employees and contractors. Organizations update training based on changing statutory, regulatory, mission, program, business process, and information system requirements, or on the results of compliance monitoring and auditing. Where appropriate, organizations may provide privacy training as part of existing information security training. Related controls: AT-2, AT-3, TR-1.

Control Enhancements: None.

References: The Privacy Act of 1974, Section 552a; Public Law 107-347, E-Government Act of 2002, as amended, Section 208; OMB Memoranda 03-22, 07-16.

AR-6 PRIVACY REPORTING

Control: The organization develops, disseminates, and updates reports to the Office of Management and Budget (OMB) and Congress to demonstrate accountability with specific statutory and regulatory privacy program mandates, and to senior management and other personnel with responsibility for monitoring privacy program progress and compliance.

Supplemental Guidance: Through external and internal privacy reporting, organizations promote accountability and transparency in organizational privacy operations. Reporting also helps organizations determine progress in meeting privacy compliance requirements and privacy controls, compare performance across the federal government, identify vulnerabilities and gaps in policy and implementation, and identify success models. Types of privacy reports include: (i) annual SAOP reports to OMB; (ii) reports to Congress required by the *Implementing Regulations of the 9/11 Commission Act*; or (iii) other public reports required by specific statutory mandates or internal policies of organizations. SAOPs/CPOs consult with legal counsel, where appropriate, to ensure that organizations meet all applicable privacy reporting requirements.

Control Enhancements: None.

References: The Privacy Act of 1974, Section 552a; Public Law 107-347, E-Government Act of 2002, as amended, Section 208; Federal Information Security Management Act of 2002 (FISMA, 44 U.S.C. § 3541, *et seq.*); Section 803 of the 9/11 Commission Act (42 U.S.C. § 2000ee-1); Section 804 of the 9/11 Commission Act (the Federal Agency Data Mining Reporting Act) (42 U.S.C. § 2000ee-3); Consolidated Appropriations Act of 2005 (Section 522); OMB Memoranda 03-22; OMB Circular A-130.

Draft