

---

## APPENDIX J

# PRIVACY CONTROL CATALOG

## PRIVACY CONTROLS, ENHANCEMENTS, AND SUPPLEMENTAL GUIDANCE

The need to protect an individual's privacy is as important today as it was in 1974 when the Privacy Act first sought to balance the government's need to collect information from an individual with a citizen's right to be notified as to how that information was being used, collected, maintained, and disposed of after the requisite period of use. These concerns are also shared in the private sector, where healthcare, financial, and other services continue to be delivered via the web with increasingly higher levels of personalization. The proliferation of social media, Smart Grid, mobile, and cloud computing, as well as the transition from structured to unstructured data and metadata environments, have added significant complexities and challenges for federal organizations in safeguarding privacy. These challenges extend well beyond the traditional information technology security view of protecting privacy which focused primarily on ensuring confidentiality. Now there are greater implications with respect to controlling the integrity of an individual's information, and with ensuring that an individual's information is available on demand. The challenging landscape requires federal organizations to expand their view of privacy, in order to meet citizen expectations of privacy that go beyond information security.

Privacy, with respect to personally identifiable information (PII),<sup>119</sup> is a core value that can be obtained only with appropriate legislation, policies, procedures, and associated controls to ensure compliance with requirements. Protecting the privacy of individuals and their PII that is collected, used, maintained, shared, and disposed of by programs and information systems, is a fundamental responsibility of federal organizations. Privacy also involves each individual's right to decide when and whether to share personal information, how much information to share, and the particular circumstances under which that information can be shared. In today's digital world, effective privacy for individuals depends on the safeguards employed within the information systems that are processing, storing, and transmitting PII and the environments in which those systems operate. Organizations cannot have effective privacy without a basic foundation of information security. Privacy is more than security, however, and includes, for example, the principles of transparency, notice, and choice.

This appendix provides a structured set of controls for protecting privacy and 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. The controls focus on information privacy as a value distinct from, but highly interrelated with, information security. Privacy controls are

---

<sup>119</sup> OMB Memorandum 07-16 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. OMB Memorandum 10-22 further states that "the definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified by examining the context of use and combination of data elements. In performing this assessment, it is important for agencies to recognize that non-PII can become PII, whenever additional information is made publicly available, in any medium and from any source that, when combined with other available information, could be used to identify an individual." NIST Special Publication 800-122 also includes a definition of PII that differs from this appendix because it was focused on the security objective of confidentiality and not privacy in the broad sense. Organizational definitions of PII may vary based on the consideration of additional regulatory requirements. The privacy controls in this appendix apply regardless of the definition of PII by organizations.

the administrative, technical, and physical safeguards employed within organizations to protect and ensure the proper handling of PII.<sup>120</sup> Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary.

The privacy controls in this appendix are based on the Fair Information Practice Principles (FIPPs)<sup>121</sup> embodied in the Privacy Act of 1974, Section 208 of the E-Government Act of 2002, and Office of Management and Budget (OMB) policies. The FIPPs are designed to build public trust in the privacy practices of organizations and to help organizations avoid tangible costs and intangible damages from privacy incidents. There are eight privacy control families, each aligning with one of the FIPPs. The privacy families can be implemented at the organization, department, agency, component, office, program, or information system level, under the leadership and oversight of the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO)<sup>122</sup> and in coordination with the Chief Information Security Officer, Chief Information Officer, program officials, legal counsel, and others as appropriate. Table J-1 provides a summary of the privacy controls by family in the privacy control catalog.

**TABLE J-1: SUMMARY OF PRIVACY CONTROLS BY FAMILY**

ID	PRIVACY CONTROLS
<b>AP</b>	<b>Authority and Purpose</b>
AP-1	Authority to Collect
AP-2	Purpose Specification
<b>AR</b>	<b>Accountability, Audit, and Risk Management</b>
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
AR-7	Privacy-Enhanced System Design and Development
AR-8	Accounting of Disclosures
<b>DI</b>	<b>Data Quality and Integrity</b>
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
<b>DM</b>	<b>Data Minimization and Retention</b>
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal

<sup>120</sup> 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 paper. Organizations can use the privacy controls and the guidance in the paper to develop an organization-wide privacy program or enhance an already existing program.

<sup>121</sup> 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.

<sup>122</sup> All federal agencies and departments designate an SAOP/CPO as the senior organizational official with the overall organization-wide responsibility for information privacy issues. OMB Memorandum 05-08 provides guidance for the designation of SAOPs/CPOs. The term SAOP/CPO as used in this appendix means an organization’s senior privacy leader, whose job title may vary from organization to organization.

ID	PRIVACY CONTROLS
DM-3	Minimization of PII Used in Testing, Training, and Research
<b>IP</b>	<b>Individual Participation and Redress</b>
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
<b>SE</b>	<b>Security</b>
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
<b>TR</b>	<b>Transparency</b>
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
<b>UL</b>	<b>Use Limitation</b>
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

There is a strong similarity between the structure of the privacy controls in this appendix and the structure of the security controls in Appendices F and G. For example, the control AR-1 (Governance and Privacy Program) requires organizations to develop privacy plans that can be implemented at the organizational or program level. These plans can also be used in conjunction with security plans to 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 fundamental concepts associated with managing information security risk helps to ensure that the employment of privacy controls is carried out in a cost-effective and risk-based manner while simultaneously meeting compliance requirements. Standardized privacy controls and assessment procedures (developed to evaluate the effectiveness of the controls) will provide a more disciplined and structured approach for satisfying federal privacy requirements and demonstrating compliance with those requirements.

In summary, the Privacy Appendix achieves several important objectives. The appendix:

- Provides a structured set of privacy controls, based on best practices, that helps organizations comply with applicable federal laws, Executive Orders, directives, instructions, regulations, policies, standards, guidance, and organization-specific issuances;
- Establishes a linkage and relationship between privacy and security controls for purposes of enforcing respective privacy and security requirements that may overlap in concept and in implementation within federal information systems, programs, and organizations;
- Demonstrates the applicability of the NIST Risk Management Framework in the selection, implementation, assessment, and ongoing monitoring of privacy controls deployed in federal information systems, programs, and organizations; and
- Promotes 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.

## HOW TO USE THIS APPENDIX

The privacy controls outlined in this publication are primarily for use by an organization's Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) when working with program managers, mission/business owners, information owners/stewards, Chief Information Officers, Chief Information Security Officers, information system developers/integrators, and risk executives to determine how best to incorporate effective privacy protections and practices (i.e., privacy controls) within organizational programs and information systems and the environments in which they operate. The privacy controls facilitate the organization's efforts to comply with privacy requirements affecting those organizational programs and/or systems that collect, use, maintain, share, or dispose of personally identifiable information (PII) or other activities that raise privacy risks. While the security controls in Appendix F are allocated to the low, moderate, and high baselines in Appendix D, the privacy controls are selected and implemented based on the privacy requirements of organizations and the need to protect the PII of individuals collected and maintained by organizational information systems and programs, in accordance with federal privacy legislation, policies, directives, regulations, guidelines, and best practices.

Organizations analyze and apply each privacy control with respect to their distinct mission/business and operational needs based on their legal authorities and obligations. Implementation of the privacy controls may vary based upon this analysis (e.g., organizations that are defined as *covered entities* pursuant to the Health Insurance Portability and Accountability Act [HIPAA] may have additional requirements that are not specifically enumerated in this publication). 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, mission/business process level, and information system 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. Similarly, organizations subject to the Confidential Information Protection and Statistical Efficiency Act (CIPSEA), implement the privacy controls consistent with that Act. All organizations implement the privacy controls consistent with the Privacy Act of 1974, 5 U.S.C. § 552a, subject to any exceptions and/or exemptions.

Privacy control enhancements described in Appendix J reflect best practices which organizations should strive to achieve, but are not mandatory. Organizations should decide when to apply control enhancements to support their particular missions/business functions. Specific *overlays* for privacy, developed in accordance with the guidance in Section 3.2 and Appendix I, can also be considered to facilitate the tailoring of the security control baselines in Appendix D with the requisite privacy controls to ensure that both security and privacy requirements can be satisfied by organizations. Many of the security controls in Appendix F provide the fundamental information protection for confidentiality, integrity, and availability within organizational information systems and the environments in which those systems operate—protection that is essential for strong and effective privacy.

Organizations document the agreed upon privacy controls to be implemented in organizational programs and information systems and the environments in which they operate. At the discretion of the implementing organization, privacy controls may be documented in a distinct privacy plan or incorporated into other risk management documents (e.g., system security plans). Organizations also establish appropriate assessment methodologies to determine the extent to which the privacy controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting designated privacy requirements. Organizational assessments of privacy controls can be conducted either by the SAOP/CPO alone or jointly with the other organizational risk management offices including the information security office.

***Implementation Tip***

- Select and implement privacy controls based on the privacy requirements of organizations and the need to protect the personally identifiable information (PII) of individuals collected and maintained by systems and programs.
- Coordinate privacy control selection and implementation with the organizational Risk Executive Function, mission/business owners, enterprise architects, Chief Information Officer, SAOP/CPO, and Chief Information Security Officer.
- View the privacy controls in Appendix J from the same perspective as the Program Management controls in Appendix G—that is, the controls are implemented for each organizational information system irrespective of the FIPS 199 categorization for that system.
- Select and implement the optional privacy control enhancements when there is a demonstrated need for additional privacy protection for individuals and PII.
- Apply the privacy controls consistent with any specific exceptions and exemptions included in legislation, Executive Orders, directives, policies, and regulations (e.g., law enforcement or national security considerations).

**FAMILY: AUTHORITY AND PURPOSE**

This family ensures that organizations: (i) identify the legal bases that authorize a particular personally identifiable information (PII) collection or activity that impacts privacy; and (ii) specify in their notices the purpose(s) for which PII is collected.

**AP-1 AUTHORITY TO COLLECT**

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

Supplemental Guidance: Before collecting PII, the organization determines whether the contemplated collection of PII is legally authorized. Program officials consult with the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) and legal counsel regarding the authority of any program or activity to collect PII. The authority to collect PII is documented in the System of Records Notice (SORN) and/or Privacy Impact Assessment (PIA) or other applicable documentation such as Privacy Act Statements or Computer Matching Agreements. Related controls: AR-2, DM-1, TR-1, TR-2.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. § 552a (e); Section 208(c), E-Government Act of 2002 (P.L. 107-347); OMB Circular A-130, Appendix I.

**AP-2 PURPOSE SPECIFICATION**

Control: The organization describes the purpose(s) for which personally identifiable information (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 Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (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, the purposes are clearly described in the related privacy compliance documentation, including but not limited to Privacy Impact Assessments (PIAs), System of Records Notices (SORNs), and Privacy Act Statements provided at the time of collection (e.g., 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, authorized uses of PII, and on the contents of the notice. Related controls: AR-2, AR-4, AR-5, DM-1, DM-2, TR-1, TR-2, UL-1, UL-2.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. § 552a (e)(3)(A)-(B); Sections 208(b), (c), E-Government Act of 2002 (P.L. 107-347).

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

This family enhances public confidence through effective controls for governance, monitoring, risk management, and assessment to demonstrate that organizations are complying with applicable privacy protection requirements and minimizing overall privacy risk.

**AR-1 GOVERNANCE AND PRIVACY PROGRAM**

Control: The organization:

- a. Appoints a Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (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 personally identifiable information (PII) by programs and information systems;
- b. Monitors federal privacy laws and policy for changes that affect the privacy program;
- c. Allocates [*Assignment: organization-defined allocation of budget and staffing*] sufficient resources to implement and operate the organization-wide privacy program;
- d. Develops a strategic organizational privacy plan for implementing applicable privacy controls, policies, and procedures;
- e. Develops, disseminates, and implements operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII; and
- f. Updates privacy plan, policies, and procedures [*Assignment: organization-defined frequency, at least biennially*].

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 an SAOP/CPO with the authority, mission, resources, and responsibility to develop and implement a multifaceted privacy program. The SAOP/CPO, in consultation with legal counsel, information security officials, and others as appropriate: (i) ensures the development, implementation, and enforcement of privacy policies and procedures; (ii) defines roles and responsibilities for protecting PII; (iii) determines the level of information sensitivity with regard to PII holdings; (iv) identifies the laws, regulations, and internal policies that apply to the PII; (v) monitors privacy best practices; and (vi) monitors/audits compliance with identified privacy controls.

To further accountability, the SAOP/CPO develops 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 the SAOP/CPO. 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 Privacy Impact Assessments (PIA) and System of Records Notices (SORN). 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, 5 U.S.C. § 552a; E-Government Act of 2002 (P.L. 107-347); Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541; 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. Documents and implements a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of personally identifiable information (PII); and
- b. Conducts Privacy Impact Assessments (PIAs) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures.

Supplemental Guidance: Organizational privacy risk management processes operate across the life cycles of all mission/business processes that collect, use, maintain, share, or dispose of PII. The tools and processes for managing risk are specific to organizational missions and resources. They include, but are not limited to, the conduct of PIAs. The PIA is both a process and the document that is the outcome of that process. 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 (e.g., 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.

Control Enhancements: None.

References: Section 208, E-Government Act of 2002 (P.L. 107-347); Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541; OMB Memoranda 03-22, 05-08, 10-23.

## **AR-3 PRIVACY REQUIREMENTS FOR CONTRACTORS AND SERVICE PROVIDERS**

Control: The organization:

- a. Establishes privacy roles, responsibilities, and access requirements 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, information providers, information processors, and other organizations providing information system development, information technology services, and other outsourced applications. Organizations consult with legal counsel, the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO), and contracting officers about applicable laws, directives, policies, or regulations that may impact implementation of this control. Related control: AR-1, AR-5, SA-4.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. § 552a(m); Federal Acquisition Regulation, 48 C.F.R. Part 24; OMB Circular A-130.

**AR-4 PRIVACY MONITORING AND AUDITING**

Control: The organization monitors and audits privacy controls 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 personally identifiable information (PII), 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 that access to PII is only on a *need-to-know* basis; and (v) ensure that 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; (iii) assess contractor compliance with privacy requirements; and (iv) ensure that corrective actions identified as part of the assessment process are tracked and monitored until audit findings are corrected. The organization Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) coordinates monitoring and auditing efforts with information security officials and ensures that the results are provided to senior managers and oversight officials. Related controls: AR-6, AR-7, AU-1, AU-2, AU-3, AU-6, AU-12, CA-7, TR-1, UL-2.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. § 552a; Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541; Section 208, E-Government Act of 2002 (P.L. 107-347); OMB Memoranda 03-22, 05-08, 06-16, 07-16; OMB Circular A-130.

**AR-5 PRIVACY AWARENESS AND TRAINING**

Control: The organization:

- a. Develops, implements, and updates a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures;
- b. Administers basic privacy training [*Assignment: organization-defined frequency, at least annually*] and targeted, role-based privacy training for personnel having responsibility for personally identifiable information (PII) or for activities that involve PII [*Assignment: organization-defined frequency, at least annually*]; and
- c. Ensures that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements [*Assignment: organization-defined frequency, at least annually*].

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 and the consequences of failing to carry out those responsibilities, 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 Privacy Impact Assessments (PIAs) or System of Records Notices (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: AR-3, AT-2, AT-3, TR-1.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. § 552a(e); Section 208, E-Government Act of 2002 (P.L. 107-347); 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), Congress, and other oversight bodies, as appropriate, 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 internal and external privacy reporting, organizations promote accountability and transparency in organizational privacy operations. Reporting also helps organizations to 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 Senior Agency Official for Privacy (SAOP) reports to OMB; (ii) reports to Congress required by the *Implementing Regulations of the 9/11 Commission Act*; and (iii) other public reports required by specific statutory mandates or internal policies of organizations. The organization Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) consults with legal counsel, where appropriate, to ensure that organizations meet all applicable privacy reporting requirements.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. § 552a; Section 208, E-Government Act of 2002 (P.L. 107-347); Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541; Section 803, 9/11 Commission Act, 42 U.S.C. § 2000ee-1; Section 804, 9/11 Commission Act, 42 U.S.C. § 2000ee-3; Section 522, Consolidated Appropriations Act of 2005 (P.L. 108-447); OMB Memoranda 03-22; OMB Circular A-130.

#### **AR-7 PRIVACY-ENHANCED SYSTEM DESIGN AND DEVELOPMENT**

Control: The organization designs information systems to support privacy by automating privacy controls.

Supplemental Guidance: To the extent feasible, when designing organizational information systems, organizations employ technologies and system capabilities that automate privacy controls on the collection, use, retention, and disclosure of personally identifiable information (PII). By building privacy controls into system design and development, organizations mitigate privacy risks to PII, thereby reducing the likelihood of information system breaches and other privacy-related incidents. Organizations also conduct periodic reviews of systems to determine the need for updates to maintain compliance with the Privacy Act and the organization's privacy policy. Regardless of whether automated privacy controls are employed, organizations regularly monitor information system use and sharing of PII to ensure that the use/sharing is consistent with the authorized purposes identified in the Privacy Act and/or in the public notice of organizations, or in a manner compatible with those purposes. Related controls: AC-6, AR-4, AR-5, DM-2, TR-1.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. § 552a(e)(10); Sections 208(b) and (c), E-Government Act of 2002 (P.L. 107-347); OMB Memorandum 03-22.

**AR-8 ACCOUNTING OF DISCLOSURES**

Control: The organization:

- a. Keeps an accurate accounting of disclosures of information held in each system of records under its control, including:
  - (1) Date, nature, and purpose of each disclosure of a record; and
  - (2) Name and address of the person or agency to which the disclosure was made;
- b. Retains the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer; and
- c. Makes the accounting of disclosures available to the person named in the record upon request.

Supplemental Guidance: The Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) periodically consults with managers of organization systems of record to ensure that the required accountings of disclosures of records are being properly maintained and provided to persons named in those records consistent with the dictates of the Privacy Act. Organizations are not required to keep an accounting of disclosures when the disclosures are made to individuals with a need to know, are made pursuant to the Freedom of Information Act, or are made to a law enforcement agency pursuant to 5 U.S.C. § 552a(c)(3). Heads of agencies can promulgate rules to exempt certain systems of records from the requirement to provide the accounting of disclosures to individuals. Related control: IP-2.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. § 552a (c)(1), (c)(3), (j), (k).

**FAMILY: DATA QUALITY AND INTEGRITY**

This family enhances public confidence that any personally identifiable information (PII) collected and maintained by organizations is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in public notices.

**DI-1 DATA QUALITY**

Control: The organization:

- a. Confirms to the greatest extent practicable upon collection or creation of personally identifiable information (PII), the accuracy, relevance, timeliness, and completeness of that information;
- 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 [*Assignment: organization-defined frequency*]; 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 and relevance 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 (API). The types of measures taken to protect data quality are based on the nature and context of the PII, how it is to be used, and how it was obtained. 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: AP-2, DI-2, DM-1, IP-3, SI-10.

Control Enhancements:

**(1) DATA QUALITY | VALIDATE PII**

**The organization requests that the individual or individual's authorized representative validate PII during the collection process.**

**(2) DATA QUALITY | RE-VALIDATE PII**

**The organization requests that the individual or individual's authorized representative revalidate that PII collected is still accurate [*Assignment: organization-defined frequency*].**

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

**DI-2 DATA INTEGRITY AND DATA INTEGRITY BOARD**

Control: The organization:

- a. Documents processes to ensure the integrity of personally identifiable information (PII) through existing security controls; and

- b. Establishes a Data Integrity Board when appropriate to oversee organizational Computer Matching Agreements<sup>123</sup> 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 or regarding certain computerized comparisons involving federal personnel or payroll records 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 Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (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, AC-22, AU-2, AU-3, AU-6, AU-10, AU-11, DI-1, SC-8, SC-28, UL-2.

Control Enhancements:

- (1) *DATA INTEGRITY AND DATA INTEGRITY BOARD | PUBLISH AGREEMENTS ON WEBSITE*

**The organization publishes Computer Matching Agreements on its public website.**

References: The Privacy Act of 1974, 5 U.S.C. §§ 552a (a)(8)(A), (o), (p), (u); OMB Circular A-130, Appendix I.

---

<sup>123</sup> Organizations enter into Computer Matching Agreements in connection with computer matching programs to which they are a party. With certain exceptions, a computer matching program is any computerized comparison of two or more automated systems of records or a system of records with nonfederal records for the purpose of establishing or verifying the eligibility of, or continuing compliance with, statutory and regulatory requirements by, applicants 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 computerized comparisons of two or more automated federal personnel or payroll systems of records or a system of federal personnel or payroll records with nonfederal records. See Computer Matching and Privacy Protection Act of 1988, 5 U.S.C. § 552a (a)(8)(A).

**FAMILY: DATA MINIMIZATION AND RETENTION**

This family helps organizations implement the data minimization and retention requirements to collect, use, and retain only personally identifiable information (PII) that is relevant and necessary for the purpose for which it was originally collected. Organizations retain PII for only as long as necessary to fulfill the purpose(s) specified in public notices 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 personally identifiable information (PII) elements 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 of PII holdings and establishes and follows a schedule for regularly reviewing those holdings [*Assignment: organization-defined frequency, at least annually*] 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: Organizations take appropriate steps to ensure that 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 Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (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. 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. Organizations coordinate with their federal records officers to ensure that 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-1, AP-2, AR-4, IP-1, SE-1, SI-12, TR-1.

Control Enhancements:

- (1) MINIMIZATION OF PERSONALLY IDENTIFIABLE INFORMATION | LOCATE / REMOVE / REDACT / ANONYMIZE PII**  
**The organization, where feasible and within the limits of technology, locates and removes/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.**

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

References: The Privacy Act of 1974, 5 U.S.C. §552a (e); Section 208(b), E-Government Act of 2002 (P.L. 107-347); OMB Memoranda 03-22, 07-16.

**DM-2 DATA RETENTION AND DISPOSAL**

Control: The organization:

- a. Retains each collection of personally identifiable information (PII) for [*Assignment: organization-defined time period*] to fulfill the purpose(s) identified in the notice or as required by law;
- b. Disposes of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and
- c. Uses [*Assignment: organization-defined techniques or methods*] 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. 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. Methods of storage include, for example, electronic, optical media, or paper.

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 System of Records Notice) to inform the public of any changes in holdings of PII.

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-1, MP-2, MP-3, MP-4, MP-5, MP-6, MP-7, MP-8, SI-12, TR-1.

Control Enhancements:

**(1) DATA RETENTION AND DISPOSAL | SYSTEM CONFIGURATION**

**The organization, where feasible, configures its information systems 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, 5 U.S.C. § 552a (e)(1), (c)(2); Section 208 (e), E-Government Act of 2002 (P.L. 107-347); 44 U.S.C. Chapters 29, 31, 33; OMB Memorandum 07-16; OMB Circular A-130; NIST Special Publication 800-88.

**DM-3 MINIMIZATION OF PII USED IN TESTING, TRAINING, AND RESEARCH**

Control: The organization:

- a. Develops policies and procedures that minimize the use of personally identifiable information (PII) for testing, training, and research; and
- b. Implements controls to protect PII used for testing, training, and research.

Supplemental Guidance: Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. The use of PII in testing, research, and training increases risk of unauthorized disclosure or misuse of the information. If PII must be used, organizations take measures to minimize any associated risks and to authorize the use of and limit the amount of PII for these purposes. Organizations consult with the SAOP/CPO and legal counsel to ensure that the use of PII in testing, training, and research is compatible with the original purpose for which it was collected.

Control Enhancements:**(1)** *MINIMIZATION OF PII USED IN TESTING, TRAINING, AND RESEARCH | RISK MINIMIZATION TECHNIQUES*

**The organization, where feasible, uses techniques to minimize the risk to privacy of using PII for research, testing, or training.**

Supplemental Guidance: Organizations can minimize risk to privacy of PII by using techniques such as de-identification.

References: NIST Special Publication 800-122.

**FAMILY: INDIVIDUAL PARTICIPATION AND REDRESS**

This family addresses the need to make individuals active participants in the decision-making process regarding the collection and use of their personally identifiable information (PII). 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 personally identifiable information (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;
- c. Obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII; and
- d. Ensures 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: Consent is fundamental to the participation of individuals in the decision-making process regarding the collection and use of their PII and the use of technologies that may increase risk to personal privacy. To obtain consent, organizations provide individuals 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 achieve awareness and consent, for example, through updated public notices.

Organizations may obtain consent through opt-in, opt-out, or implied consent. Opt-in consent is the preferred method, but it is not always feasible. Opt-in requires that individuals take affirmative action to *allow* organizations to collect or use PII. For example, opt-in consent may require an individual to click a radio button on a website, or sign a document providing consent. In contrast, opt-out requires individuals to take action to *prevent* the new or continued collection or use of such PII. For example, the Federal Trade Commission's Do-Not-Call Registry allows individuals to opt-out of receiving unsolicited telemarketing calls by requesting to be added to a list. Implied consent is the least preferred method and should be used in limited circumstances. 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 of failure to provide PII. Consequences can vary from organization to organization. Related controls: AC-2, AP-1, TR-1, TR-2.

Control Enhancements:

**(1) CONSENT | MECHANISMS SUPPORTING ITEMIZED OR TIERED CONSENT**

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

Supplemental Guidance: Organizations can provide, for example, 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 organizational operations comply with individual choices.

References: The Privacy Act of 1974, 5 U.S.C. § 552a (b), (e)(3); Section 208(c), E-Government Act of 2002 (P.L. 107-347); OMB Memoranda 03-22, 10-22.

## IP-2 INDIVIDUAL ACCESS

Control: The organization:

- a. Provides individuals the ability to have access to their personally identifiable information (PII) maintained in its system(s) of records;
- b. Publishes rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records;
- c. Publishes access procedures in System of Records Notices (SORNs); and
- d. Adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.

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 resources, legal requirements, or other factors. The organization Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) is responsible for the content of Privacy Act regulations and record request processing, in consultation with legal counsel. Access to certain types of records may not be appropriate, however, and heads of agencies may promulgate rules exempting particular systems from the access provision of the Privacy Act. In addition, individuals are not entitled to access to information compiled in reasonable anticipation of a civil action or proceeding. Related controls: AR-8, IP-3, TR-1, TR-2.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. §§ 552a (c)(3), (d)(5), (e) (4); (j), (k), (t); OMB Circular A-130.

## IP-3 REDRESS

Control: The organization:

- a. Provides a process for individuals to have inaccurate personally identifiable information (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 use 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. Individuals may appeal an adverse decision and have incorrect information amended, where appropriate.

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, TR-2, UL-2.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. § 552a (d), (c)(4); 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 Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (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:

**(1)** *COMPLAINT MANAGEMENT | RESPONSE TIMES*

**The organization responds to complaints, concerns, or questions from individuals within [Assignment: organization-defined time period].**

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

**FAMILY: SECURITY**

This family supplements the security controls in Appendix F to ensure that technical, physical, and administrative safeguards are in place to protect personally identifiable information (PII) collected or maintained by organizations against loss, unauthorized access, or disclosure, and to ensure that 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 and in accordance with the existing NIST Risk Management Framework.

**SE-1 INVENTORY OF PERSONALLY IDENTIFIABLE INFORMATION**

Control: The organization:

- a. Establishes, maintains, and updates [*Assignment: organization-defined frequency*] an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing personally identifiable information (PII); and
- b. Provides each update of the PII inventory to the CIO or information security official [*Assignment: organization-defined frequency*] to support the establishment of 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 their PII inventories, organizations may extract the following information elements from Privacy Impact Assessments (PIA) for 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 information system; and (iv) classification of level of potential risk of substantial harm, embarrassment, inconvenience, or unfairness to affected individuals, as well as the financial or reputational risks to organizations, if PII is exposed. Organizations take due care in updating the inventories by identifying linkable data that could create PII. Related controls: AR-1, AR-4, AR-5, AT-1, DM-1, PM-5, UL-3.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. § 552a (e) (10); Section 208(b)(2), E-Government Act of 2002 (P.L. 107-347); OMB Memorandum 03-22; OMB Circular A-130, Appendix I; FIPS Publication 199; 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 privacy incidents 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 that relate to personally identifiable information (PII). The organization Privacy Incident Response Plan is developed under the leadership of the SAOP/CPO. The 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 oversight organizations or affected individuals is appropriate and to provide that notice accordingly; (iii) a privacy risk assessment process to determine the extent of harm, embarrassment, inconvenience, or unfairness to affected individuals and, where appropriate, to take steps to mitigate any such risks; (iv) internal

procedures to ensure prompt reporting by employees and contractors of any privacy incident to information security officials and the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO), consistent with organizational incident management structures; and (v) internal procedures for reporting noncompliance with organizational privacy policy by employees or contractors to appropriate management or oversight officials. Some organizations may be required by law or policy to provide notice to oversight organizations in the event of a breach.

Organizations may also choose to integrate Privacy Incident Response Plans with Security Incident Response Plans, or keep the plans separate. Related controls: AR-1, AR-4, AR-5, AR-6, AU-1 through 14, IR-1 through IR-8, RA-1.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. § 552a (e), (i)(1), and (m); Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541; OMB Memoranda 06-19, 07-16; NIST Special Publication 800-37.

**FAMILY: TRANSPARENCY**

This family ensures that organizations provide public notice of their information practices and the privacy impact of their 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, the categories of those 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; and (vi) how the PII will be protected; and
- c. Revises its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change.

Supplemental Guidance: Effective notice, by virtue of its clarity, readability, 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), or in a website 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, or on separate forms that can be retained by the individuals.

The organization Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) is 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).<sup>124</sup> Changing PII practice or policy without prior notice is disfavored and should only be undertaken in consultation with the SAOP/CPO and counsel. Related controls: AP-1, AP-2, AR-1, AR-2, IP-1, IP-2, IP-3, UL-1, UL-2.

Control Enhancements:

**(1) PRIVACY NOTICE | REAL-TIME OR LAYERED NOTICE**

**The organization provides real-time and/or layered notice when it collects PII.**

Supplemental Guidance: Real-time notice is defined as notice at the point of collection. A layered notice approach involves providing individuals with a summary of key points in the organization's privacy policy. A second notice provides more detailed/specific information.

<sup>124</sup> The Information Sharing Environment is an approach that facilitates the sharing of terrorism and homeland security information. The ISE was established by the Intelligence Reform and Terrorism Prevention Act of 2004, Public Law 108-458, 118 Stat. 3638. See the ISE website at: [www.ise.gov](http://www.ise.gov).

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

## TR-2 SYSTEM OF RECORDS NOTICES AND PRIVACY ACT STATEMENTS

Control: The organization:

- a. Publishes System of Records Notices (SORNs) in the Federal Register, subject to required oversight processes, for systems containing personally identifiable information (PII);
- b. Keeps SORNs current; and
- c. Includes Privacy Act Statements on its forms that collect PII, or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected.

Supplemental Guidance: Organizations issue SORNs to provide the public notice regarding PII collected in a system of records, which the Privacy Act defines as “a group of any records under the control of any agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifier.” SORNs explain how the information is used, retained, and may be corrected, and whether certain portions of the system are subject to Privacy Act exemptions for law enforcement or national security reasons. Privacy Act Statements provide notice of: (i) the authority of organizations to collect PII; (ii) whether providing PII is mandatory or optional; (iii) the principal purpose(s) for which the PII is to be used; (iv) the intended disclosures (routine uses) of the information; and (v) the consequences of not providing all or some portion of the information requested. When information is collected verbally, organizations read a Privacy Act Statement prior to initiating the collection of PII (for example, when conducting telephone interviews or surveys). Related control: DI-2.

Control Enhancements:

- (1) *SYSTEM OF RECORDS NOTICES AND PRIVACY ACT STATEMENTS | PUBLIC WEBSITE PUBLICATION*  
**The organization publishes SORNs on its public website.**

References: The Privacy Act of 1974, 5 U.S.C. § 552a (e)(3); OMB Circular A-130.

## TR-3 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 Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO); and
- b. Ensures that its privacy practices are publicly available through organizational websites or otherwise.

Supplemental Guidance: Organizations employ different mechanisms for informing the public about their privacy practices including, but not limited to, Privacy Impact Assessments (PIAs), System of Records Notices (SORNs), privacy reports, publicly available web pages, email distributions, blogs, and periodic publications (e.g., quarterly newsletters). Organizations also employ publicly facing email addresses and/or phone lines that enable the public to provide feedback and/or direct questions to privacy offices regarding privacy practices. Related control: AR-6.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. § 552a; Section 208, E-Government Act of 2002 (P.L. 107-347); OMB Memoranda 03-22, 10-23.

**FAMILY: USE LIMITATION**

This family ensures that organizations only use personally identifiable information (PII) either as specified in their public notices, in a manner compatible with those specified purposes, or as 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 personally identifiable information (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 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 the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) 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-2, AR-3, AR-4, AR-5, IP-1, TR-1, TR-2.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. § 552a (b)(1).

**UL-2 INFORMATION SHARING WITH THIRD PARTIES**

Control: The organization:

- a. Shares personally identifiable information (PII) externally, only for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or for a purpose that is 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 describe the PII covered and specifically enumerate the purposes for which the PII may be used;
- c. Monitors, audits, and trains its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII; and
- d. Evaluates any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.

Supplemental Guidance: The organization Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) and, where appropriate, legal counsel review and approve any proposed external sharing of PII, including with other public, international, or private sector entities, for consistency with uses described in the existing organizational public notice(s). When a proposed new instance of external sharing of PII is not currently authorized by the Privacy Act and/or specified in a notice, organizations evaluate whether the proposed external sharing is compatible with the purpose(s) specified in the notice. If the proposed sharing is compatible, organizations review, update, and republish their Privacy Impact Assessments (PIAs), System of Records Notices (SORNs), website privacy policies, and other public notices, if any, to include specific descriptions of the new uses(s) and obtain consent where appropriate and feasible. Information-sharing agreements also include security protections consistent with the sensitivity of the information being shared. Related controls: AR-3, AR-4, AR-5, AR-8, AP-2, DI-1, DI-2, IP-1, TR-1.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. § 552a (a)(7), (b), (c), (e)(3)(C), (o); ISE Privacy Guidelines.

---

## Acknowledgements

This appendix 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 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.