3.13 PROGRAM MANAGEMENT

PROGRAM MANAGEMENT CONTROLS

[FISMA], [PRIVACT], and [OMB A-130] require federal agencies to develop, implement, and provide oversight for organization-wide information security and privacy programs to help ensure the confidentiality, integrity, and availability of federal information processed, stored, and transmitted by federal information systems and to protect individual privacy. The program management (PM) controls described in this section are implemented at the organization level and not directed at individual information systems. The PM controls have been designed to facilitate organizational compliance with applicable federal laws, executive orders, directives, policies, regulations, and standards. The controls are independent of [FIPS 200] impact levels and, therefore, are not associated with the control baselines described in [SP 800-53B].

Organizations document program management controls in the information security and privacy program plans. The organization-wide information security program plan (see PM-1) and privacy program plan (see PM-18) supplement system security and privacy plans (see PL-2) developed for organizational information systems. Together, the system security and privacy plans for the individual information systems and the information security and privacy program plans cover the totality of security and privacy controls employed by the organization.

Quick link to Program Management Summary Table

PM-1 INFORMATION SECURITY PROGRAM PLAN

Control:

a. Develop and disseminate an organization-wide information security program plan that:

   1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;

   2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance;

   3. Reflects the coordination among organizational entities responsible for information security; and

   4. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation;

b. Review and update the organization-wide information security program plan [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*]; and

c. Protect the information security program plan from unauthorized disclosure and modification.

Discussion: An information security program plan is a formal document that provides an overview of the security requirements for an organization-wide information security program and describes the program management controls and common controls in place or planned for meeting those requirements. An information security program plan can be represented in a single document or compilations of documents. Privacy program plans and supply chain risk management plans are addressed separately in PM-18 and SR-2, respectively.

An information security program plan documents implementation details about program management and common controls. The plan provides sufficient information about the controls (including specification of parameters for assignment and selection operations, explicitly or by reference) to enable implementations that are unambiguously compliant with the intent of the plan and a determination of the risk to be incurred if the plan is implemented as intended. Updates to information security program plans include organizational changes and problems identified during plan implementation or control assessments.

Program management controls may be implemented at the organization level or the mission or business process level, and are essential for managing the organization's information security program. Program management controls are distinct from common, system-specific, and hybrid controls because program management controls are independent of any particular system. Together, the individual system security plans and the organization-wide information security program plan provide complete coverage for the security controls employed within the organization.

Common controls available for inheritance by organizational systems are documented in an appendix to the organization's information security program plan unless the controls are included in a separate security plan for a system. The organization-wide information security program plan indicates which separate security plans contain descriptions of common controls.

Events that may precipitate an update to the information security program plan include, but are not limited to, organization-wide assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines.

Related Controls: PL-2, PM-18, PM-30, RA-9, SI-12, SR-2.

Control Enhancements: None.

References: [FISMA], [OMB A-130], [SP 800-37], [SP 800-39].

PM-2 INFORMATION SECURITY PROGRAM LEADERSHIP ROLE

Control: Appoint a senior agency information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.

Discussion: The senior agency information security officer is an organizational official. For federal agencies (as defined by applicable laws, executive orders, regulations, directives, policies, and standards), this official is the senior agency information security officer. Organizations may also refer to this official as the senior information security officer or chief information security officer.

Related Controls: None.

Control Enhancements: None.

References: [OMB M-17-25], [SP 800-37], [SP 800-39], [SP 800-181].

PM-3 INFORMATION SECURITY AND PRIVACY RESOURCES

Control:

a. Include the resources needed to implement the information security and privacy programs in capital planning and investment requests and document all exceptions to this requirement;

b. Prepare documentation required for addressing information security and privacy programs in capital planning and investment requests in accordance with applicable laws, executive orders, directives, policies, regulations, standards; and

c. Make available for expenditure, the planned information security and privacy resources.

Discussion: Organizations consider establishing champions for information security and privacy and, as part of including the necessary resources, assign specialized expertise and resources as needed. Organizations may designate and empower an Investment Review Board or similar group to manage and provide oversight for the information security and privacy aspects of the capital planning and investment control process.

Related Controls: PM-4, SA-2.

Control Enhancements: None.

References: [OMB A-130].

PM-4 PLAN OF ACTION AND MILESTONES PROCESS

Control:

a. Implement a process to ensure that plans of action and milestones for the information security, privacy, and supply chain risk management programs and associated organizational systems:

   1. Are developed and maintained;

   2. Document the remedial information security, privacy, and supply chain risk management actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and

   3. Are reported in accordance with established reporting requirements.

b. Review plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

Discussion: The plan of action and milestones is a key organizational document and is subject to reporting requirements established by the Office of Management and Budget. Organizations develop plans of action and milestones with an organization-wide perspective, prioritizing risk response actions and ensuring consistency with the goals and objectives of the organization. Plan of action and milestones updates are based on findings from control assessments and continuous monitoring activities. There can be multiple plans of action and milestones corresponding to the information system level, mission/business process level, and organizational/governance level. While plans of action and milestones are required for federal organizations, other types of organizations can help reduce risk by documenting and tracking planned remediations. Specific guidance on plans of action and milestones at the system level is provided in CA-5.

Related Controls: CA-5, CA-7, PM-3, RA-7, SI-12.

Control Enhancements: None.

References: [PRIVACT], [OMB A-130], [SP 800-37].

PM-5 SYSTEM INVENTORY

Control: Develop and update [*Assignment: organization-defined frequency*] an inventory of organizational systems.

Discussion: [OMB A-130] provides guidance on developing systems inventories and associated reporting requirements. System inventory refers to an organization-wide inventory of systems, not system components as described in CM-8.

Related Controls: None.

Control Enhancements:

(1) SYSTEM INVENTORY | INVENTORY OF PERSONALLY IDENTIFIABLE INFORMATION

Establish, maintain, and update [*Assignment: organization-defined frequency*] an inventory of all systems, applications, and projects that process personally identifiable information.

Discussion: An inventory of systems, applications, and projects that process personally identifiable information supports the mapping of data actions, providing individuals with privacy notices, maintaining accurate personally identifiable information, and limiting the processing of personally identifiable information when such information is not needed for operational purposes. Organizations may use this inventory to ensure that systems only process the personally identifiable information for authorized purposes and that this processing is still relevant and necessary for the purpose specified therein.

Related Controls: AC-3, CM-8, CM-12, CM-13, PL-8, PM-22, PT-3, PT-5, SI-12, SI-18.

References: [OMB A-130], [IR 8062].

PM-6 MEASURES OF PERFORMANCE

Control: Develop, monitor, and report on the results of information security and privacy measures of performance.

Discussion: Measures of performance are outcome-based metrics used by an organization to measure the effectiveness or efficiency of the information security and privacy programs and the controls employed in support of the program. To facilitate security and privacy risk management, organizations consider aligning measures of performance with the organizational risk tolerance as defined in the risk management strategy.

Related Controls: CA-7, PM-9.

Control Enhancements: None.

References: [OMB A-130], [SP 800-37], [SP 800-39], [SP 800-55], [SP 800-137].

PM-7 ENTERPRISE ARCHITECTURE

Control: Develop and maintain an enterprise architecture with consideration for information security, privacy, and the resulting risk to organizational operations and assets, individuals, other organizations, and the Nation.

Discussion: The integration of security and privacy requirements and controls into the enterprise architecture helps to ensure that security and privacy considerations are addressed throughout the system development life cycle and are explicitly related to the organization's mission and business processes. The process of security and privacy requirements integration also embeds into the enterprise architecture and the organization's security and privacy architectures consistent with the organizational risk management strategy. For PM-7, security and privacy architectures are developed at a system-of-systems level, representing all organizational systems. For PL-8, the security and privacy architectures are developed at a level that represents an individual system. The system-level architectures are consistent with the security and privacy architectures defined for the organization. Security and privacy requirements and control integration are most effectively accomplished through the rigorous application of the Risk Management Framework [SP 800-37] and supporting security standards and guidelines.

Related Controls: AU-6, PL-2, PL-8, PM-11, RA-2, SA-3, SA-8, SA-17.

Control Enhancements:

(1) ENTERPRISE ARCHITECTURE | OFFLOADING

Offload [*Assignment: organization-defined non-essential functions or services*] to other systems, system components, or an external provider.

Discussion: Not every function or service that a system provides is essential to organizational mission or business functions. Printing or copying is an example of a non-essential but supporting service for an organization. Whenever feasible, such supportive but non-essential functions or services are not co-located with the functions or services that support essential mission or business functions. Maintaining such functions on the same system or system component increases the attack surface of the organization's mission-essential functions or services. Moving supportive but non-essential functions to a non-critical system, system component, or external provider can also increase efficiency by putting those functions or services under the control of individuals or providers who are subject matter experts in the functions or services.

Related Controls: SA-8.

References: [OMB A-130], [SP 800-37], [SP 800-39], [SP 800-160-1], [SP 800-160-2].

PM-8 CRITICAL INFRASTRUCTURE PLAN

Control: Address information security and privacy issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

Discussion: Protection strategies are based on the prioritization of critical assets and resources. The requirement and guidance for defining critical infrastructure and key resources and for preparing an associated critical infrastructure protection plan are found in applicable laws, executive orders, directives, policies, regulations, standards, and guidelines.

Related Controls: CP-2, CP-4, PE-18, PL-2, PM-9, PM-11, PM-18, RA-3, SI-12.

Control Enhancements: None.

References: [EO 13636], [OMB A-130], [HSPD 7], [DHS NIPP].

PM-9 RISK MANAGEMENT STRATEGY

Control:

a. Develops a comprehensive strategy to manage:

   1. Security risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of organizational systems; and

   2. Privacy risk to individuals resulting from the authorized processing of personally identifiable information;

b. Implement the risk management strategy consistently across the organization; and

c. Review and update the risk management strategy [*Assignment: organization-defined frequency*] or as required, to address organizational changes.

Discussion: An organization-wide risk management strategy includes an expression of the security and privacy risk tolerance for the organization, security and privacy risk mitigation strategies, acceptable risk assessment methodologies, a process for evaluating security and privacy risk across the organization with respect to the organization's risk tolerance, and approaches for monitoring risk over time. The senior accountable official for risk management (agency head or designated official) aligns information security management processes with strategic, operational, and budgetary planning processes. The risk executive function, led by the senior accountable official for risk management, can facilitate consistent application of the risk management strategy organization-wide. The risk management strategy can be informed by security and privacy risk-related inputs from other sources, both internal and external to the organization, to ensure that the strategy is broad-based and comprehensive. The supply chain risk management strategy described in PM-30 can also provide useful inputs to the organization-wide risk management strategy.

Related Controls: AC-1, AU-1, AT-1, CA-1, CA-2, CA-5, CA-6, CA-7, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PL-2, PM-2, PM-8, PM-18, PM-28, PM-30, PS-1, PT-1, PT-2, PT-3, RA-1, RA-3, RA-9, SA-1, SA-4, SC-1, SC-38, SI-1, SI-12, SR-1, SR-2.

Control Enhancements: None.

References: [OMB A-130], [SP 800-30], [SP 800-37], [SP 800-39], [SP 800-161], [IR 8023].

PM-10 AUTHORIZATION PROCESS

Control:

a. Manage the security and privacy state of organizational systems and the environments in which those systems operate through authorization processes;

b. Designate individuals to fulfill specific roles and responsibilities within the organizational risk management process; and

c. Integrate the authorization processes into an organization-wide risk management program.

Discussion: Authorization processes for organizational systems and environments of operation require the implementation of an organization-wide risk management process and associated security and privacy standards and guidelines. Specific roles for risk management processes include a risk executive (function) and designated authorizing officials for each organizational system and common control provider. The authorization processes for the organization are integrated with continuous monitoring processes to facilitate ongoing understanding and acceptance of security and privacy risks to organizational operations, organizational assets, individuals, other organizations, and the Nation.

Related Controls: CA-6, CA-7, PL-2.

Control Enhancements: None.

References: [SP 800-37], [SP 800-39], [SP 800-181].

PM-11 MISSION AND BUSINESS PROCESS DEFINITION

Control:

a. Define organizational mission and business processes with consideration for information security and privacy and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and

b. Determine information protection and personally identifiable information processing needs arising from the defined mission and business processes; and

c. Review and revise the mission and business processes [*Assignment: organization-defined frequency*].

Discussion: Protection needs are technology-independent capabilities that are required to counter threats to organizations, individuals, systems, and the Nation through the compromise of information (i.e., loss of confidentiality, integrity, availability, or privacy). Information protection and personally identifiable information processing needs are derived from the mission and business needs defined by organizational stakeholders, the mission and business processes designed to meet those needs, and the organizational risk management strategy. Information protection and personally identifiable information processing needs determine the required controls for the organization and the systems. Inherent to defining protection and personally identifiable information processing needs is an understanding of the adverse impact that could result if a compromise or breach of information occurs. The categorization process is used to make such potential impact determinations. Privacy risks to individuals can arise from the compromise of personally identifiable information, but they can also arise as unintended consequences or a byproduct of the processing of personally identifiable information at any stage of the information life cycle. Privacy risk assessments are used to prioritize the risks that are created for individuals from system processing of personally identifiable information. These risk assessments enable the selection of the required privacy controls for the organization and systems. Mission and business process definitions and the associated protection requirements are documented in accordance with organizational policies and procedures.

Related Controls: CP-2, PL-2, PM-7, PM-8, RA-2, RA-3, RA-9, SA-2.

Control Enhancements: None.

References: [OMB A-130], [FIPS 199],[SP 800-39], [SP 800-60-1], [SP 800-60-2], [SP 800-160-1].

PM-12 INSIDER THREAT PROGRAM

Control: Implement an insider threat program that includes a cross-discipline insider threat incident handling team.

Discussion: Organizations that handle classified information are required, under Executive Order 13587 [EO 13587] and the National Insider Threat Policy [ODNI NITP], to establish insider threat programs. The same standards and guidelines that apply to insider threat programs in classified environments can also be employed effectively to improve the security of controlled unclassified and other information in non-national security systems. Insider threat programs include controls to detect and prevent malicious insider activity through the centralized integration and analysis of both technical and nontechnical information to identify potential insider threat concerns. A senior official is designated by the department or agency head as the responsible individual to implement and provide oversight for the program. In addition to the centralized integration and analysis capability, insider threat programs require organizations to prepare department or agency insider threat policies and implementation plans, conduct host-based user monitoring of individual employee activities on government-owned classified computers, provide insider threat awareness training to employees, receive access to information from offices in the department or agency for insider threat analysis, and conduct self-assessments of department or agency insider threat posture.

Insider threat programs can leverage the existence of incident handling teams that organizations may already have in place, such as computer security incident response teams. Human resources records are especially important in this effort, as there is compelling evidence to show that some types of insider crimes are often preceded by nontechnical behaviors in the workplace, including ongoing patterns of disgruntled behavior and conflicts with coworkers and other colleagues. These precursors can guide organizational officials in more focused, targeted monitoring efforts. However, the use of human resource records could raise significant concerns for privacy. The participation of a legal team, including consultation with the senior agency official for privacy, ensures that monitoring activities are performed in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Related Controls: AC-6, AT-2, AU-6, AU-7, AU-10, AU-12, AU-13, CA-7, IA-4, IR-4, MP-7, PE-2, PM-16, PS-3, PS-4, PS-5, PS-7, PS-8, SC-7, SC-38, SI-4, PM-14.

Control Enhancements: None.

References: [EO 13587], [NITP12], [ODNI NITP].

PM-13 SECURITY AND PRIVACY WORKFORCE

Control: Establish a security and privacy workforce development and improvement program.

Discussion: Security and privacy workforce development and improvement programs include defining the knowledge, skills, and abilities needed to perform security and privacy duties and tasks; developing role-based training programs for individuals assigned security and privacy roles and responsibilities; and providing standards and guidelines for measuring and building individual qualifications for incumbents and applicants for security- and privacy-related positions. Such workforce development and improvement programs can also include security and privacy career paths to encourage security and privacy professionals to advance in the field and fill positions with greater responsibility. The programs encourage organizations to fill security- and privacy-related positions with qualified personnel. Security and privacy workforce development and improvement programs are complementary to organizational security awareness and training programs and focus on developing and institutionalizing the core security and privacy capabilities of personnel needed to protect organizational operations, assets, and individuals.

Related Controls: AT-2, AT-3.

Control Enhancements: None.

References: [OMB A-130], [SP 800-181].

PM-14 TESTING, TRAINING, AND MONITORING

Control:

a. Implement a process for ensuring that organizational plans for conducting security and privacy testing, training, and monitoring activities associated with organizational systems:

   1. Are developed and maintained; and

   2. Continue to be executed; and

b. Review testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

Discussion: A process for organization-wide security and privacy testing, training, and monitoring helps ensure that organizations provide oversight for testing, training, and monitoring activities and that those activities are coordinated. With the growing importance of continuous monitoring programs, the implementation of information security and privacy across the three levels of the risk management hierarchy and the widespread use of common controls, organizations coordinate and consolidate the testing and monitoring activities that are routinely conducted as part of ongoing assessments supporting a variety of controls. Security and privacy training activities, while focused on individual systems and specific roles, require coordination across all organizational elements. Testing, training, and monitoring plans and activities are informed by current threat and vulnerability assessments.

Related Controls: AT-2, AT-3, CA-7, CP-4, IR-3, PM-12, SI-4.

Control Enhancements: None.

References: [OMB A-130], [SP 800-37], [SP 800-39], [SP 800-53A], [SP 800-115], [SP 800-137].

PM-15 SECURITY AND PRIVACY GROUPS AND ASSOCIATIONS

Control: Establish and institutionalize contact with selected groups and associations within the security and privacy communities:

a. To facilitate ongoing security and privacy education and training for organizational personnel;

b. To maintain currency with recommended security and privacy practices, techniques, and technologies; and

c. To share current security and privacy information, including threats, vulnerabilities, and incidents.

Discussion: Ongoing contact with security and privacy groups and associations is important in an environment of rapidly changing technologies and threats. Groups and associations include special interest groups, professional associations, forums, news groups, users' groups, and peer groups of security and privacy professionals in similar organizations. Organizations select security and privacy groups and associations based on mission and business functions. Organizations share threat, vulnerability, and incident information as well as contextual insights, compliance techniques, and privacy problems consistent with applicable laws, executive orders, directives, policies, regulations, standards, and guidelines.

Related Controls: SA-11, SI-5.

Control Enhancements: None.

References: [OMB A-130].

PM-16 THREAT AWARENESS PROGRAM

Control: Implement a threat awareness program that includes a cross-organization information-sharing capability for threat intelligence.

Discussion: Because of the constantly changing and increasing sophistication of adversaries, especially the advanced persistent threat (APT), it may be more likely that adversaries can successfully breach or compromise organizational systems. One of the best techniques to address this concern is for organizations to share threat information, including threat events (i.e., tactics, techniques, and procedures) that organizations have experienced, mitigations that organizations have found are effective against certain types of threats, and threat intelligence (i.e., indications and warnings about threats). Threat information sharing may be bilateral or multilateral. Bilateral threat sharing includes government-to-commercial and government-to-government cooperatives. Multilateral threat sharing includes organizations taking part in threat-sharing consortia. Threat information may require special agreements and protection, or it may be freely shared.

Related Controls: IR-4, PM-12.

Control Enhancements:

(1) THREAT AWARENESS PROGRAM | AUTOMATED MEANS FOR SHARING THREAT INTELLIGENCE

Employ automated mechanisms to maximize the effectiveness of sharing threat intelligence information.

Discussion: To maximize the effectiveness of monitoring, it is important to know what threat observables and indicators the sensors need to be searching for. By using well-established frameworks, services, and automated tools, organizations improve their ability to rapidly share and feed the relevant threat detection signatures into monitoring tools.

Related Controls: None.

References: None.

PM-17 PROTECTING CONTROLLED UNCLASSIFIED INFORMATION ON EXTERNAL SYSTEMS

Control:

a. Establish policy and procedures to ensure that requirements for the protection of controlled unclassified information that is processed, stored or transmitted on external systems, are implemented in accordance with applicable laws, executive orders, directives, policies, regulations, and standards; and

b. Review and update the policy and procedures [*Assignment: organization-defined frequency*].

Discussion: Controlled unclassified information is defined by the National Archives and Records Administration along with the safeguarding and dissemination requirements for such information and is codified in [32 CFR 2002] and, specifically for systems external to the federal organization, 32 CFR 2002.14h. The policy prescribes the specific use and conditions to be implemented in accordance with organizational procedures, including via its contracting processes.

Related Controls: CA-6, PM-10.

Control Enhancements: None.

References: [32 CFR 2002], [SP 800-171], [SP 800-172], [NARA CUI].

PM-18 PRIVACY PROGRAM PLAN

Control:

a. Develop and disseminate an organization-wide privacy program plan that provides an overview of the agency’s privacy program, and:

   1. Includes a description of the structure of the privacy program and the resources dedicated to the privacy program;

   2. Provides an overview of the requirements for the privacy program and a description of the privacy program management controls and common controls in place or planned for meeting those requirements;

   3. Includes the role of the senior agency official for privacy and the identification and assignment of roles of other privacy officials and staff and their responsibilities;

   4. Describes management commitment, compliance, and the strategic goals and objectives of the privacy program;

   5. Reflects coordination among organizational entities responsible for the different aspects of privacy; and

   6. Is approved by a senior official with responsibility and accountability for the privacy risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; and

b. Update the plan [*Assignment: organization-defined frequency*] and to address changes in federal privacy laws and policy and organizational changes and problems identified during plan implementation or privacy control assessments.

Discussion: A privacy program plan is a formal document that provides an overview of an organization's privacy program, including a description of the structure of the privacy program, the resources dedicated to the privacy program, the role of the senior agency official for privacy and other privacy officials and staff, the strategic goals and objectives of the privacy program, and the program management controls and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks. Privacy program plans can be represented in single documents or compilations of documents.

The senior agency official for privacy is responsible for designating which privacy controls the organization will treat as program management, common, system-specific, and hybrid controls. Privacy program plans provide sufficient information about the privacy program management and common controls (including the specification of parameters and assignment and selection operations explicitly or by reference) to enable control implementations that are unambiguously compliant with the intent of the plans and a determination of the risk incurred if the plans are implemented as intended.

Program management controls are generally implemented at the organization level and are essential for managing the organization's privacy program. Program management controls are distinct from common, system-specific, and hybrid controls because program management controls are independent of any particular information system. Together, the privacy plans for individual systems and the organization-wide privacy program plan provide complete coverage for the privacy controls employed within the organization.

Common controls are documented in an appendix to the organization's privacy program plan unless the controls are included in a separate privacy plan for a system. The organization-wide privacy program plan indicates which separate privacy plans contain descriptions of privacy controls.

Related Controls: PM-8, PM-9, PM-19.

Control Enhancements: None.

References: [PRIVACT], [OMB A-130].

PM-19 PRIVACY PROGRAM LEADERSHIP ROLE

Control: Appoint a senior agency official for privacy with the authority, mission, accountability, and resources to coordinate, develop, and implement, applicable privacy requirements and manage privacy risks through the organization-wide privacy program.

Discussion: The privacy officer is an organizational official. For federal agencies—as defined by applicable laws, executive orders, directives, regulations, policies, standards, and guidelines—this official is designated as the senior agency official for privacy. Organizations may also refer to this official as the chief privacy officer. The senior agency official for privacy also has roles on the data management board (see PM-23) and the data integrity board (see PM-24).

Related Controls: PM-18, PM-20, PM-23, PM-24, PM-27.

Control Enhancements: None.

References: [OMB A-130].

PM-20 DISSEMINATION OF PRIVACY PROGRAM INFORMATION

Control: Maintain a central resource webpage on the organization's principal public website that serves as a central source of information about the organization's privacy program and that:

a. Ensures that the public has access to information about organizational privacy activities and can communicate with its senior agency official for privacy;

b. Ensures that organizational privacy practices and reports are publicly available; and

c. Employs publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to privacy offices regarding privacy practices.

Discussion: For federal agencies, the webpage is located at www.[agency].gov/privacy. Federal agencies include public privacy impact assessments, system of records notices, computer matching notices and agreements, [PRIVACT] exemption and implementation rules, privacy reports, privacy policies, instructions for individuals making an access or amendment request, email addresses for questions/complaints, blogs, and periodic publications.

Related Controls: AC-3, PM-19, PT-5, PT-6, PT-7, RA-8.

Control Enhancements:

(1) DISSEMINATION OF PRIVACY PROGRAM INFORMATION | PRIVACY POLICIES ON WEBSITES, APPLICATIONS, AND DIGITAL SERVICES

Develop and post privacy policies on all external-facing websites, mobile applications, and other digital services, that:

(a) Are written in plain language and organized in a way that is easy to understand and navigate;

(b) Provide information needed by the public to make an informed decision about whether and how to interact with the organization; and

(c) Are updated whenever the organization makes a substantive change to the practices it describes and includes a time/date stamp to inform the public of the date of the most recent changes.

Discussion: Organizations post privacy policies on all external-facing websites, mobile applications, and other digital services. Organizations post a link to the relevant privacy policy on any known, major entry points to the website, application, or digital service. In addition, organizations provide a link to the privacy policy on any webpage that collects personally identifiable information. Organizations may be subject to applicable laws, executive orders, directives, regulations, or policies that require the provision of specific information to the public. Organizational personnel consult with the senior agency official for privacy and legal counsel regarding such requirements.

Related Controls: None.

References: [PRIVACT], [OMB A-130], [OMB M-17-06].

PM-21 ACCOUNTING OF DISCLOSURES

Control:

a. Develop and maintain an accurate accounting of disclosures of personally identifiable information, including:

1. Date, nature, and purpose of each disclosure; and

2. Name and address, or other contact information of the individual or organization to which the disclosure was made;

b. Retain the accounting of disclosures for the length of the time the personally identifiable information is maintained or five years after the disclosure is made, whichever is longer; and

c. Make the accounting of disclosures available to the individual to whom the personally identifiable information relates upon request.

Discussion: The purpose of accounting of disclosures is to allow individuals to learn to whom their personally identifiable information has been disclosed, to provide a basis for subsequently advising recipients of any corrected or disputed personally identifiable information, and to provide an audit trail for subsequent reviews of organizational compliance with conditions for disclosures. For federal agencies, keeping an accounting of disclosures is required by the [PRIVACT]; agencies should consult with their senior agency official for privacy and legal counsel on this requirement and be aware of the statutory exceptions and OMB guidance relating to the provision.

Organizations can use any system for keeping notations of disclosures, if it can construct from such a system, a document listing of all disclosures along with the required information. Automated mechanisms can be used by organizations to determine when personally identifiable information is disclosed, including commercial services that provide notifications and alerts. Accounting of disclosures may also be used to help organizations verify compliance with applicable privacy statutes and policies governing the disclosure or dissemination of information and dissemination restrictions.

Related Controls: AC-3, AU-2, PT-2.

Control Enhancements: None.

References: [PRIVACT], [OMB A-130].

PM-22 PERSONALLY IDENTIFIABLE INFORMATION QUALITY MANAGEMENT

Control: Develop and document organization-wide policies and procedures for:

a. Reviewing for the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle;

b. Correcting or deleting inaccurate or outdated personally identifiable information;

c. Disseminating notice of corrected or deleted personally identifiable information to individuals or other appropriate entities; and

d. Appeals of adverse decisions on correction or deletion requests.

Discussion: Personally identifiable information quality management includes steps that organizations take to confirm the accuracy and relevance of personally identifiable information throughout the information life cycle. The information life cycle includes the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposition of personally identifiable information. Organizational policies and procedures for personally identifiable information quality management are important because inaccurate or outdated personally identifiable information maintained by organizations may cause problems for individuals. Organizations consider the quality of personally identifiable information involved in business functions where inaccurate information may result in adverse decisions or the denial of benefits and services, or the disclosure of the information may cause stigmatization. Correct information, in certain circumstances, can cause problems for individuals that outweigh the benefits of organizations maintaining the information. Organizations consider creating policies and procedures for the removal of such information.

The senior agency official for privacy ensures that practical means and mechanisms exist and are accessible for individuals or their authorized representatives to seek the correction or deletion of personally identifiable information. Processes for correcting or deleting data are clearly defined and publicly available. Organizations use discretion in determining whether data is to be deleted or corrected based on the scope of requests, the changes sought, and the impact of the changes. Additionally, processes include the provision of responses to individuals of decisions to deny requests for correction or deletion. The responses include the reasons for the decisions, a means to record individual objections to the decisions, and a means of requesting reviews of the initial determinations.

Organizations notify individuals or their designated representatives when their personally identifiable information is corrected or deleted to provide transparency and confirm the completed action. Due to the complexity of data flows and storage, other entities may need to be informed of the correction or deletion. Notice supports the consistent correction and deletion of personally identifiable information across the data ecosystem.

Related Controls: PM-23, SI-18.

Control Enhancements: None.

References: [OMB A-130], [OMB M-19-15], [SP 800-188].

PM-23 DATA GOVERNANCE BODY

Control: Establish a Data Governance Body consisting of [*Assignment: organization-defined roles*] with [*Assignment: organization-defined responsibilities*].

Discussion: A Data Governance Body can help ensure that the organization has coherent policies and the ability to balance the utility of data with security and privacy requirements. The Data Governance Body establishes policies, procedures, and standards that facilitate data governance so that data, including personally identifiable information, is effectively managed and maintained in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidance. Responsibilities can include developing and implementing guidelines that support data modeling, quality, integrity, and the de-identification needs of personally identifiable information across the information life cycle as well as reviewing and approving applications to release data outside of the organization, archiving the applications and the released data, and performing post-release monitoring to ensure that the assumptions made as part of the data release continue to be valid. Members include the chief information officer, senior agency information security officer, and senior agency official for privacy. Federal agencies are required to establish a Data Governance Body with specific roles and responsibilities in accordance with the [EVIDACT] and policies set forth under [OMB M-19-23].

Related Controls: AT-2, AT-3, PM-19, PM-22, PM-24, PT-7, SI-4, SI-19.

Control Enhancements: None.

References: [EVIDACT], [OMB A-130], [OMB M-19-23], [SP 800-188].

PM-24 DATA INTEGRITY BOARD

Control: Establish a Data Integrity Board to:

a. Review proposals to conduct or participate in a matching program; and

b. Conduct an annual review of all matching programs in which the agency has participated.

Discussion: A Data Integrity Board is the board of senior officials designated by the head of a federal agency and is responsible for, among other things, reviewing the agency's proposals to conduct or participate in a matching program and conducting an annual review of all matching programs in which the agency has participated. As a general matter, a matching program is a computerized comparison of records from two or more automated [PRIVACT] systems of records or an automated system of records and automated records maintained by a non-federal agency (or agent thereof). A matching program either pertains to Federal benefit programs or Federal personnel or payroll records. At a minimum, the Data Integrity Board includes the Inspector General of the agency, if any, and the senior agency official for privacy.

Related Controls: AC-4, PM-19, PM-23, PT-2, PT-8.

Control Enhancements: None.

References: [PRIVACT], [OMB A-130], [OMB A-108].

PM-25 MINIMIZATION OF PERSONALLY IDENTIFIABLE INFORMATION USED IN TESTING, TRAINING, AND RESEARCH

Control:

a. Develop, document, and implement policies and procedures that address the use of personally identifiable information for internal testing, training, and research;

b. Limit or minimize the amount of personally identifiable information used for internal testing, training, and research purposes;

c. Authorize the use of personally identifiable information when such information is required for internal testing, training, and research; and

d. Review and update policies and procedures [*Assignment: organization-defined frequency*].

Discussion: The use of personally identifiable information in testing, research, and training increases the risk of unauthorized disclosure or misuse of such information. Organizations consult with the senior agency official for privacy and/or legal counsel to ensure that the use of personally identifiable information in testing, training, and research is compatible with the original purpose for which it was collected. When possible, organizations use placeholder data to avoid exposure of personally identifiable information when conducting testing, training, and research.

Related Controls: PM-23, PT-3, SA-3, SA-8, SI-12.

Control Enhancements: None.

References: [OMB A-130].

PM-26 COMPLAINT MANAGEMENT

Control: Implement a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational security and privacy practices that includes:

a. Mechanisms that are easy to use and readily accessible by the public;

b. All information necessary for successfully filing complaints;

c. Tracking mechanisms to ensure all complaints received are reviewed and addressed within [*Assignment: organization-defined time period*];

d. Acknowledgement of receipt of complaints, concerns, or questions from individuals within [*Assignment: organization-defined time period*]; and

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

Discussion: Complaints, concerns, and questions from individuals can serve as valuable sources of input to organizations and ultimately improve operational models, uses of technology, data collection practices, and controls. Mechanisms that can be used by the public include telephone hotline, email, or web-based forms. The information necessary for successfully filing complaints includes contact information for the senior agency official for privacy or other official designated to receive complaints. Privacy complaints may also include personally identifiable information which is handled in accordance with relevant policies and processes.

Related Controls: IR-7, IR-9, PM-22, SI-18.

Control Enhancements: None.

References: [OMB A-130].

PM-27 PRIVACY REPORTING

Control:

a. Develop [*Assignment: organization-defined privacy reports*] and disseminate to:

   1. [*Assignment: organization-defined oversight bodies*] to demonstrate accountability with statutory, regulatory, and policy privacy mandates; and

   2. [*Assignment: organization-defined officials*] and other personnel with responsibility for monitoring privacy program compliance; and

b. Review and update privacy reports [*Assignment: organization-defined frequency*].

Discussion: Through internal and external reporting, organizations promote accountability and transparency in organizational privacy operations. Reporting can also help organizations to determine progress in meeting privacy compliance requirements and privacy controls, compare performance across the federal government, discover vulnerabilities, identify gaps in policy and implementation, and identify models for success. For federal agencies, privacy reports include annual senior agency official for privacy reports to OMB, reports to Congress required by Implementing Regulations of the 9/11 Commission Act, and other public reports required by law, regulation, or policy, including internal policies of organizations. The senior agency official for privacy consults with legal counsel, where appropriate, to ensure that organizations meet all applicable privacy reporting requirements.

Related Controls: IR-9, PM-19.

Control Enhancements: None.

References: [FISMA], [OMB A-130], [OMB A-108].

PM-28 RISK FRAMING

Control:

a. Identify and document:

   1. Assumptions affecting risk assessments, risk responses, and risk monitoring;

   2. Constraints affecting risk assessments, risk responses, and risk monitoring;

   3. Priorities and trade-offs considered by the organization for managing risk; and

   4. Organizational risk tolerance;

b. Distribute the results of risk framing activities to [*Assignment: organization-defined personnel*]; and

c. Review and update risk framing considerations [*Assignment: organization-defined frequency*].

Discussion: Risk framing is most effective when conducted at the organization level and in consultation with stakeholders throughout the organization including mission, business, and system owners. The assumptions, constraints, risk tolerance, priorities, and trade-offs identified as part of the risk framing process inform the risk management strategy, which in turn informs the conduct of risk assessment, risk response, and risk monitoring activities. Risk framing results are shared with organizational personnel, including mission and business owners, information owners or stewards, system owners, authorizing officials, senior agency information security officer, senior agency official for privacy, and senior accountable official for risk management.

Related Controls: CA-7, PM-9, RA-3, RA-7.

Control Enhancements: None.

References: [OMB A-130], [SP 800-39].

PM-29 RISK MANAGEMENT PROGRAM LEADERSHIP ROLES

Control:

a. Appoint a Senior Accountable Official for Risk Management to align organizational information security and privacy management processes with strategic, operational, and budgetary planning processes; and

b. Establish a Risk Executive (function) to view and analyze risk from an organization-wide perspective and ensure management of risk is consistent across the organization.

Discussion: The senior accountable official for risk management leads the risk executive (function) in organization-wide risk management activities.

Related Controls: PM-2, PM-19.

Control Enhancements: None.

References: [SP 800-37], [SP 800-181].

PM-30 SUPPLY CHAIN RISK MANAGEMENT STRATEGY

Control:

a. Develop an organization-wide strategy for managing supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services;

b. Implement the supply chain risk management strategy consistently across the organization; and

c. Review and update the supply chain risk management strategy on [*Assignment: organization-defined frequency*] or as required, to address organizational changes.

Discussion: An organization-wide supply chain risk management strategy includes an unambiguous expression of the supply chain risk appetite and tolerance for the organization, acceptable supply chain risk mitigation strategies or controls, a process for consistently evaluating and monitoring supply chain risk, approaches for implementing and communicating the supply chain risk management strategy, and the associated roles and responsibilities. Supply chain risk management includes considerations of the security and privacy risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services. The supply chain risk management strategy can be incorporated into the organization's overarching risk management strategy and can guide and inform supply chain policies and system-level supply chain risk management plans. In addition, the use of a risk executive function can facilitate a consistent, organization-wide application of the supply chain risk management strategy. The supply chain risk management strategy is implemented at the organization and mission/business levels, whereas the supply chain risk management plan (see SR-2) is implemented at the system level.

Related Controls: CM-10, PM-9, SR-1, SR-2, SR-3, SR-4, SR-5, SR-6, SR-7, SR-8, SR-9, SR-11.

Control Enhancements:

(1) SUPPLY CHAIN RISK MANAGEMENT STRATEGY | SUPPLIERS OF CRITICAL OR MISSION-ESSENTIAL ITEMS

Identify, prioritize, and assess suppliers of critical or mission-essential technologies, products, and services.

Discussion: The identification and prioritization of suppliers of critical or mission-essential technologies, products, and services is paramount to the mission/business success of organizations. The assessment of suppliers is conducted using supplier reviews (see SR-6) and supply chain risk assessment processes (see RA-3(1)). An analysis of supply chain risk can help an organization identify systems or components for which additional supply chain risk mitigations are required.

Related Controls: RA-3, SR-6.

References: [PRIVACT], [FASC18], [EO 13873], [41 CFR 201], [OMB A-130], [OMB M-17-06] [CNSSD 505], [ISO 27036], [ISO 20243], [SP 800-161], [IR 8272].

PM-31 CONTINUOUS MONITORING STRATEGY

Control: Develop an organization-wide continuous monitoring strategy and implement continuous monitoring programs that include:

a. Establishing the following organization-wide metrics to be monitored: [*Assignment: organization-defined metrics*];

b. Establishing [*Assignment: organization-defined frequencies*] for monitoring and [*Assignment: organization-defined frequencies*] for assessment of control effectiveness;

c. Ongoing monitoring of organizationally-defined metrics in accordance with the continuous monitoring strategy;

d. Correlation and analysis of information generated by control assessments and monitoring;

e. Response actions to address results of the analysis of control assessment and monitoring information; and

f. Reporting the security and privacy status of organizational systems to [*Assignment: organization-defined personnel or roles*] [*Assignment: organization-defined frequency*].

Discussion: Continuous monitoring at the organization level facilitates ongoing awareness of the security and privacy posture across the organization to support organizational risk management decisions. The terms "continuous" and "ongoing" imply that organizations assess and monitor their controls and risks at a frequency sufficient to support risk-based decisions. Different types of controls may require different monitoring frequencies. The results of continuous monitoring guide and inform risk response actions by organizations. Continuous monitoring programs allow organizations to maintain the authorizations of systems and common controls in highly dynamic environments of operation with changing mission and business needs, threats, vulnerabilities, and technologies. Having access to security- and privacy-related information on a continuing basis through reports and dashboards gives organizational officials the capability to make effective, timely, and informed risk management decisions, including ongoing authorization decisions. To further facilitate security and privacy risk management, organizations consider aligning organization-defined monitoring metrics with organizational risk tolerance as defined in the risk management strategy. Monitoring requirements, including the need for monitoring, may be referenced in other controls and control enhancements such as, AC-2g, AC-2(7), AC-2(12)(a), AC-2(7)(b), AC-2(7)(c), AC-17(1), AT-4a, AU-13, AU-13(1), AU-13(2), CA-7, CM-3f, CM-6d, CM-11c, IR-5, MA-2b, MA-3a, MA-4a, PE-3d, PE-6, PE-14b, PE-16, PE-20, PM-6, PM-23, PS-7e, SA-9c, SC-5(3)(b), SC-7a, SC-7(24)(b), SC-18b, SC-43b, SI-4.

Related Controls: AC-2, AC-6, AC-17, AT-4, AU-6, AU-13, CA-2, CA-5, CA-6, CA-7, CM-3, CM-4, CM-6, CM-11, IA-5, IR-5, MA-2, MA-3, MA-4, PE-3, PE-6, PE-14, PE-16, PE-20, PL-2, PM-4, PM-6, PM-9, PM-10, PM-12, PM-14, PM-23, PM-28, PS-7, PT-7, RA-3, RA-5, RA-7, SA-9, SA-11, SC-5, SC-7, SC-18, SC-38, SC-43, SI-3, SI-4, SI-12, SR-2, SR-4.

References: [SP 800-37], [SP 800-39], [SP 800-137], [SP 800-137A].

PM-32 PURPOSING

Control: Analyze [*Assignment: organization-defined systems or systems components*] supporting mission essential services or functions to ensure that the information resources are being used consistent with their intended purpose.

Discussion: Systems are designed to support a specific mission or business function. However, over time, systems and system components may be used to support services and functions that are outside of the scope of the intended mission or business functions. This can result in exposing information resources to unintended environments and uses that can significantly increase threat exposure. In doing so, the systems are more vulnerable to compromise, which can ultimately impact the services and functions for which they were intended. This is especially impactful for mission-essential services and functions. By analyzing resource use, organizations can identify such potential exposures.

Related Controls: CA-7, PL-2, RA-3, RA-9.

Control Enhancements: None.

References: [SP 800-160-1], [SP 800-160-2].