NIST Special Publication 800-53
Revision 4

Security and Privacy Controls for Federal Information Systems and Organizations Appendix G

NOTE: THIS DOCUMENT PROVIDES A MARKUP OF CHANGES MADE TO SP 800-53, REVISION 3 APPENDIX G TO PRODUCE REVISION 4 APPENDIX G. ALTHOUGH A REVIEW WAS MADE TO CONFIRM THE ACCURACY OF THE WORD PROCESSING COMPARISON FUNCTION USED TO IDENTIFY THE CHANGES, THE CHANGES IN SOME CASES WERE CONSIDERABLE, AND THE MARKUP VERSION OF THE CHANGES MAY NOT BE EXACT. AS SUCH, THE MARKUP VERSION SHOULD BE VIEWED AS A GENERAL GUIDE TO THE CHANGES MADE TO REVISION 3 TO PRODUCE REVISION 4 OF SP 800-53. ANY DISCREPANCIES NOTED BETWEEN THE MARKUP AND CLEAN COPIES OF SP 800-53, REVISION 4, PLEASE DEFER TO THE CLEAN COPY FOR THE OFFICIAL VERSION OF CHANGES.

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

http://dx.doi.org/10.6028/NIST.SP.800-53r4

MARKUP COPY

From: Revision 3 – August 2009
To: Revision 4 – April 2013
INCLUDES UPDATES AS OF 05-07-2013

Formatted: Font: 11 pt

April 2013
INCLUDES UPDATES AS OF 05-07-2013: PAGE XVII

U.S. Department of Commerce
Rebecca M. Blank, Acting Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Under Secretary of Commerce for Standards and Technology and Director

APPENDIX G

INFORMATION SECURITY PROGRAMS

ORGANIZATION-WIDE INFORMATION SECURITY PROGRAM MANAGEMENT CONTROLS

The Federal Information Security Management Act (FISMA) requires organizations to develop and implement an organization-wide information security program to address information security for the information and information systems that support the operations and assets of the organization, including those provided or managed by another organization, contractor, or other source. The information security program management (PM) controls described in this appendix are typically implemented at the organization level and not directed at individual organizational information systems. The program management controls have been designed to facilitate compliance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. The controls are independent of any FIPS Publication 200 impact levels and therefore, are not directly associated with any of the security control baselines described in Appendix D. The program management controls do, however, complement the security controls in Appendix F and focus on the programmatic, organization-wide information security requirements that are independent of any particular information system and are essential for managing information security programs. Tailoring guidance can be applied to the program management controls in a manner similar to how the guidance is applied to security controls in Appendix F. Organizations specify the individual or individuals responsible and accountable for the development, implementation, assessment, authorization, and monitoring of the program management controls. Organizations document program management controls in the *information security program plan*. The organization-wide information security program plan supplements the individual security plans developed for each organizational information system. Together, the security plans for the individual information systems and the information security program cover the totality of security controls employed by the organization.

In addition to documenting the information security program management controls, the security program plan provides a vehicle for the organization, in a central repository, to document all security controls from Appendix F that have been designated as *common controls* (i.e., security controls inheritable by organizational information systems).[1] The information security program management controls and common controls contained in the information security program plan are implemented, assessed for effectiveness,[2] and authorized by a senior organizational official, with the same or similar authority and responsibility for managing risk as the authorization officials for information systems. Plans of action and milestones are developed and maintained for the program management and common controls that are deemed through assessment to be less than effective. Information security program management and common controls are also subject to the same continuous monitoring requirements as security controls employed in individual organizational information systems.

Deleted: within the organization

Deleted: information security

Deleted: inherited

Deleted: [3]

[1] Common controls are those security controls that are inheritable by one or more organizational information systems, and thus are separate and distinct from information security program management controls.

[2] Assessment procedures for program management controls and common controls can be found in NIST Special Publication 800-53A.

Cautionary Note

Organizations are required to implement security program management controls to provide a foundation for the organizational information security program. The successful implementation of security controls for organizational information systems depends on the successful implementation of organization-wide program management controls. However, the manner in which organizations implement the program management controls depends on specific organizational characteristics including, for example, the size, complexity, and mission/business requirements of the respective organizations.

PM-1 INFORMATION SECURITY PROGRAM PLAN

Control: The organization:

a. Develops and disseminates 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 coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical); 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. Reviews the organization-wide information security program plan [*Assignment: organization-defined frequency*];

c. Updates the plan to address organizational changes and problems identified during plan implementation or security control assessments; and

d. Protects the information security program plan from unauthorized disclosure and modification.

Supplemental Guidance: Information security program plans can be represented in single documents or compilations of documents at the discretion of organizations. The plans document the program management controls and organization-defined common controls. Information security program plans provide sufficient information about the program management controls/common controls (including specification of parameters for any *assignment* and *selection* statements either explicitly or by reference) to enable implementations that are unambiguously compliant with the intent of the plans and a determination of the risk to be incurred if the plans are implemented as intended.

The security plans for individual information systems and the organization-wide information security program plan together, provide complete coverage for all security controls employed within the organization. Common controls are documented in an appendix to the organization's information security program plan unless the controls are included in a separate security plan for an information system (e.g., security controls employed as part of an intrusion detection system providing organization-wide boundary protection inherited by one or more organizational information systems). The organization-wide information security program plan will indicate which separate security plans contain descriptions of common controls.

Organizations have the flexibility to describe common controls in a single document or in multiple documents. In the case of multiple documents, the documents describing common controls are included as attachments to the information security program plan. If the information security program plan contains multiple documents, the organization specifies in each document the organizational official or officials responsible for the development, implementation, assessment, authorization, and monitoring of the respective common controls. For example, the organization may require that the Facilities Management Office develop, implement, assess, authorize, and continuously monitor common physical and environmental protection controls from the PE family when such controls are not associated with a particular information system but instead, support multiple information systems. Related control: PM-8.

Control Enhancements: None.

References: None.

Deleted: <#>Provides sufficient information about the program management controls and common controls (including specification of parameters for any *assignment* and *selection* operations either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the plan and a determination of the risk to be incurred if the plan is implemented as intended;¶ Includes

Deleted: and

Deleted: Revises

Deleted: The i

Deleted: a

Deleted: document

Deleted: compilation

Deleted: the organization. The plan documents the organization-wide

PM-2 SENIOR INFORMATION SECURITY OFFICER

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

Supplemental Guidance: The security officer described in this control is an organizational official. For a federal agency (as defined in applicable federal laws, Executive Orders, directives, policies, or regulations) 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.

Deleted: organizational

Control Enhancements: None.

References: None.

PM-3 INFORMATION SECURITY RESOURCES

Control: The organization:

a. Ensures that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement;

b. Employs a business case/Exhibit 300/Exhibit 53 to record the resources required; and

c. Ensures that information security resources are available for expenditure as planned.

Supplemental Guidance: Organizations consider establishing champions for information security efforts 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-related aspects of the capital planning and investment control process. Related controls: PM-4, SA-2.

Control Enhancements: None.

References: NIST Special Publication 800-65.

PM-4 PLAN OF ACTION AND MILESTONES PROCESS

Control: The organization:

Deleted: implements

a. Implements a process for ensuring that plans of action and milestones for the security program and associated organizational information systems:

1. Are developed and maintained;

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

Deleted: mitigate

3. Are reported in accordance with OMB FISMA reporting requirements.

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

Supplemental Guidance: The plan of action and milestones is a key document in the information security program and is subject to federal reporting requirements established by OMB. With the increasing emphasis on organization-wide risk management across all three tiers in the risk management hierarchy (i.e., organization, mission/business process, and information system), organizations view plans of action and milestones from an organizational 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 security control assessments and

Deleted: The plan

Deleted: the

Deleted: , security impact analyses,

continuous monitoring activities. OMB FISMA reporting guidance contains instructions regarding organizational plans of action and milestones. Related control: CA-5.

Control Enhancements: None.

References: OMB Memorandum 02-01; NIST Special Publication 800-37.

PM-5 INFORMATION SYSTEM INVENTORY

Control: The organization develops and maintains an inventory of its information systems.

Supplemental Guidance: This control addresses the inventory requirements in FISMA. OMB provides guidance on developing information systems inventories and associated reporting requirements. For specific information system inventory reporting requirements, organizations consult OMB annual FISMA reporting guidance.

Control Enhancements: None.

References: Web: www.omb.gov.

Deleted: None

PM-6 INFORMATION SECURITY MEASURES OF PERFORMANCE

Control: The organization develops, monitors, and reports on the results of information security measures of performance.

Supplemental Guidance: Measures of performance are outcome-based metrics used by an organization to measure the effectiveness or efficiency of the information security program and the security controls employed in support of the program.

Control Enhancements: None.

References: NIST Special Publication 800-55.

PM-7 ENTERPRISE ARCHITECTURE

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

Supplemental Guidance: The enterprise architecture developed by the organization is aligned with the Federal Enterprise Architecture. The integration of information security requirements and associated security controls into the organization's enterprise architecture helps to ensure that security considerations are addressed by organizations early in the system development life cycle and are directly and explicitly related to the organization's mission/business processes. This process of security requirements integration also embeds into the enterprise architecture, an integral *information security architecture* consistent with organizational risk management and information security strategies. For PM-7, the information security architecture is developed at a system-of-systems level (organization-wide), representing all of the organizational information systems. For PL-8, the information security architecture is developed at a level representing an individual information system but at the same time, is consistent with the information security architecture defined for the organization. Security requirements and security control integration are most effectively accomplished through the application of the Risk Management Framework and supporting security standards and guidelines. The Federal Segment Architecture Methodology provides guidance on integrating information security requirements and security controls into enterprise architectures. Related controls: PL-2, PL-8, PM-11, RA-2, SA-3.

Deleted: This

Deleted: Security requirements and

Control Enhancements: None.

References: NIST Special Publication 800-39; Web: www.fsam.gov.

PM-8 CRITICAL INFRASTRUCTURE PLAN

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

Supplemental Guidance: 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 federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Related controls: PM-1, PM-9, PM-11, RA-3.

Control Enhancements: None.

References: HSPD 7; National Infrastructure Protection Plan.

PM-9 RISK MANAGEMENT STRATEGY

Control: The organization:

a. Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems;

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

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

Supplemental Guidance: An organization-wide risk management strategy includes, for example, an unambiguous expression of the risk tolerance for the organization, acceptable risk assessment methodologies, risk mitigation strategies, a process for consistently evaluating risk across the organization with respect to the organization's risk tolerance, and approaches for monitoring risk over time. The use of a risk executive function can facilitate consistent, organization-wide application of the risk management strategy. The organization-wide risk management strategy can be informed by risk-related inputs from other sources both internal and external to the organization to ensure the strategy is both broad-based and comprehensive. Related control: RA-3.

Control Enhancements: None.

References: NIST Special Publications 800-30, 800-39.

PM-10 SECURITY AUTHORIZATION PROCESS

Control: The organization:

a. Manages (i.e., documents, tracks, and reports) the security state of organizational information systems and the environments in which those systems operate through security authorization processes;

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

c. Fully integrates the security authorization processes into an organization-wide risk management program.

Supplemental Guidance: Security authorization processes for information systems and environments of operation require the implementation of an organization-wide risk management process, a Risk Management Framework, and associated security standards and guidelines. Specific roles within the risk management process include an organizational risk executive (function) and designated authorizing officials for each organizational information system and common control provider. Security authorization processes are integrated with organizational continuous monitoring

Deleted: and

Deleted: that

Deleted: The security

Deleted: process

Deleted: requires

Deleted: the

Deleted: the employment of

Deleted: a

Deleted: official

processes to facilitate ongoing understanding and acceptance of risk to organizational operations and assets, individuals, other organizations, and the Nation. Related control: CA-6.

Control Enhancements: None.

References: NIST Special Publications 800-37, 800-39.

PM-11 MISSION/BUSINESS PROCESS DEFINITION

Control: The organization:

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

b. Determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until achievable protection needs are obtained.

Deleted: an

Deleted: set of

Deleted: is

Supplemental Guidance: Information protection needs are technology-independent, required capabilities to counter threats to organizations, individuals, or the Nation through the compromise of information (i.e., loss of confidentiality, integrity, or availability). Information protection needs are derived from the mission/business needs defined by the organization, the mission/business processes selected to meet the stated needs, and the organizational risk management strategy. Information protection needs determine the required security controls for the organization and the associated information systems supporting the mission/business processes. Inherent in defining an organization's information protection needs is an understanding of the level of adverse impact that could result if a compromise of information occurs. The security categorization process is used to make such potential impact determinations. Mission/business process definitions and associated information protection requirements are documented by the organization in accordance with organizational policy and procedure. Related controls: PM-7, PM-8, RA-2.

Control Enhancements: None.

References: FIPS Publication 199; NIST Special Publication 800-60.

PM-12 INSIDER THREAT PROGRAM

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

Supplemental Guidance: Organizations handling classified information are required, under Executive Order 13587 and the National Policy on Insider Threat, to establish insider threat programs. The standards and guidelines that apply to insider threat programs in classified environments can also be employed effectively to improve the security of Controlled Unclassified Information in non-national security systems. Insider threat programs include security controls to detect and prevent malicious insider activity through the centralized integration and analysis of both technical and non-technical information to identify potential insider threat concerns. A senior organizational official is designated by the department/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 as a minimum, prepare department/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 all offices within the department/agency (e.g., human resources, legal, physical security, personnel security, information technology, information system security, and law enforcement) for insider threat analysis, and conduct self-assessments of department/agency insider threat posture.

Insider threat programs can leverage the existence of incident handling teams 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 (e.g., ongoing patterns of disgruntled behavior and conflicts with coworkers and other colleagues). These precursors can better inform and guide organizational officials in more focused, targeted monitoring efforts. The participation of a legal team is important to ensure that all monitoring activities are performed in accordance with appropriate legislation, 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, PS-3, PS-4, PS-5, PS-8, SC-7, SC-38, SI-4, PM-1, PM-14.

Control Enhancements: None.

References: Executive Order 13587.

PM-13 INFORMATION SECURITY WORKFORCE

Control: The organization establishes an information security workforce development and improvement program.

Supplemental Guidance: Information security workforce development and improvement programs include, for example: (i) defining the knowledge and skill levels needed to perform information security duties and tasks; (ii) developing role-based training programs for individuals assigned information security roles and responsibilities; and (iii) providing standards for measuring and building individual qualifications for incumbents and applicants for information security-related positions. Such workforce programs can also include associated information security career paths to encourage: (i) information security professionals to advance in the field and fill positions with greater responsibility; and (ii) organizations to fill information security-related positions with qualified personnel. Information security workforce development and improvement programs are complementary to organizational security awareness and training programs. Information security workforce development and improvement programs focus on developing and institutionalizing core information security capabilities of selected personnel needed to protect organizational operations, assets, and individuals. Related controls: AT-2, AT-3.

Control Enhancements: None.

References: None.

PM-14 TESTING, TRAINING, AND MONITORING

Control: The organization:

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

   1. Are developed and maintained; and

   2. Continue to be executed in a timely manner;

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

Supplemental Guidance: This control ensures that organizations provide oversight for the security testing, training, and monitoring activities conducted organization-wide and that those activities are coordinated. With the importance of continuous monitoring programs, the implementation of information security across the three tiers 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 organizational assessments supporting a variety of security controls. Security training activities, while typically focused on individual information systems and specific roles, also necessitate coordination across all organizational elements. Testing, training, and monitoring plans and activities are informed by current threat and vulnerability assessments. Related controls: AT-3, CA-7, CP-4, IR-3, SI-4.

Control Enhancements: None.

References: NIST Special Publications 800-16, 800-37, 800-53A, 800-137.

PM-15 CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS

Control: The organization establishes and institutionalizes contact with selected groups and associations within the security community:

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

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

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

Supplemental Guidance: Ongoing contact with security groups and associations is of paramount importance in an environment of rapidly changing technologies and threats. Security groups and associations include, for example, special interest groups, forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations. Organizations select groups and associations based on organizational missions/business functions. Organizations share threat, vulnerability, and incident information consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Related control: SI-5.

Control Enhancements: None.

References: None.

PM-16 THREAT AWARENESS PROGRAM

Control: The organization implements a threat awareness program that includes a cross-organization information-sharing capability.

Supplemental Guidance: Because of the constantly changing and increasing sophistication of adversaries, especially the advanced persistent threat (APT), it is becoming more likely that adversaries may successfully breach or compromise organizational information systems. One of the best techniques to address this concern is for organizations to share threat information. This can include, for example, sharing threat events (i.e., tactics, techniques, and procedures) that organizations have experienced, mitigations that organizations have found are effective against certain types of threats, threat intelligence (i.e., indications and warnings about threats that are likely to occur). Threat information sharing may be bilateral (e.g., government-commercial cooperatives, government-government cooperatives), or multilateral (e.g., organizations taking part in threat-sharing consortia). Threat information may be highly sensitive requiring special agreements and protection, or less sensitive and freely shared. Related controls: PM-12, PM-16.

Control Enhancements: None.

References: None.