

**Department of the Interior**  
**Security Control Standard**  
**Program Management**

**April 2011**

Version: 1.1



## Signature Approval Page

Designated Official	
Bernard J. Mazer, Department of the Interior, Chief Information Officer	
<b>Signature:</b>	<b>Date:</b>

## REVISION HISTORY

<b>Author</b>	<b>Version</b>	<b>Revision Date</b>	<b>Revision Summary</b>
Timothy Brown	0.1	February 09, 2011	Initial draft
Louis Eichenbaum	1.0	February 23, 2011	Final review and version change to 1.0
Lawrence K. Ruffin	1.1	April 29, 2011	Final revisions and version change to 1.1

# TABLE OF CONTENTS

<b>REVISION HISTORY .....</b>	<b>3</b>
<b>TABLE OF CONTENTS .....</b>	<b>4</b>
<b>SECURITY CONTROL STANDARD: PROGRAM MANAGEMENT .....</b>	<b>5</b>
PM-1 INFORMATION SECURITY PROGRAM PLAN .....	5
PM-2 SENIOR INFORMATION SECURITY OFFICER .....	6
PM-3 INFORMATION SECURITY RESOURCES .....	7
PM-4 PLAN OF ACTION AND MILESTONES PROCESS .....	7
PM-5 INFORMATION SYSTEM INVENTORY .....	7
PM-6 INFORMATION SECURITY MEASURES OF PERFORMANCE .....	8
PM-7 ENTERPRISE ARCHITECTURE .....	8
PM-8 CRITICAL INFRASTRUCTURE PLAN .....	8
PM-9 RISK MANAGEMENT STRATEGY .....	9
PM-10 SECURITY AUTHORIZATION PROCESS.....	9
PM-11 MISSION/BUSINESS PROCESS DEFINITION .....	10

## SECURITY CONTROL STANDARD: PROGRAM MANAGEMENT

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 describes the required process for selecting and specifying security controls for an information system based on its security categorizing, including tailoring the initial set of baseline security controls and supplementing the tailored baseline as necessary based on an organizational assessment of risk.

This standard specifies organization-defined parameters that are deemed necessary or appropriate to achieve a consistent security posture across the Department of the Interior. In addition to the NIST SP 800-53 Program Management (PM) control family standard, supplemental information is included that establishes an enterprise-wide standard for specific controls within the control family. In some cases additional agency-specific or Office of Management and Budget (OMB) requirements have been incorporated into relevant controls. Where the NIST SP 800-53 indicates the need for organization-defined parameters or selection of operations that are not specified in this supplemental standard, the System Owner shall appropriately define and document the parameters based on the individual requirements, purpose, and function of the information system. The supplemental information provided in this standard is required to be applied when the Authorizing Official (AO) has selected the control, or control enhancement, in a manner that is consistent with the Department's IT security policy and associated information security Risk Management Framework (RMF) strategy.

Additionally, information systems implemented within cloud computing environments shall select, implement, and comply with any additional and/or more stringent security control requirements as specified and approved by the Federal Risk and Authorization Management Program (FedRAMP) unless otherwise approved for risk acceptance by the AO. The additional controls required for implementation within cloud computing environments are readily identified within the Priority and Baseline Allocation table following each control and distinguished by the control or control enhancement represented in **bold red text**.

### ***PM-1 INFORMATION SECURITY PROGRAM PLAN***

Applicability: Bureaus and Offices

Control: The organization:

- a. Develops and disseminates an organization-wide information security program plan that:
  - 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;
  - 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 roles, responsibilities, management commitment, coordination among organizational entities, and compliance;

- 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 at least annually; and
- c. Revises the plan to address organizational changes and problems identified during plan implementation or security control assessments.

Supplemental Guidance: The information security program plan can be represented in a single document or compilation of documents at the discretion of the organization. The plan documents the organization-wide program management controls and organization-defined common controls. 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.

## ***PM-2 SENIOR INFORMATION SECURITY OFFICER***

Applicability: Bureaus and Offices

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 organizational official as the Senior Information Security Officer or Chief Information Security Officer.

Control Enhancements: None.

References: None.

## ***PM-3 INFORMATION SECURITY RESOURCES***

Applicability: Bureaus and Offices

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 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***

Applicability: Bureaus and Offices

Control: The organization implements a process for ensuring that plans of action and milestones for the security program and the associated organizational information systems are maintained and document the remedial information security actions to mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation.

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. The plan of action and milestones updates are based on the findings from security control assessments, security impact analyses, and 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***

Applicability: Bureaus and Offices

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.

Control Enhancements: None.

References: None.

## ***PM-6 INFORMATION SECURITY MEASURES OF PERFORMANCE***

Applicability: Bureaus and Offices

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***

Applicability: Bureaus and Offices

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 also embeds into the enterprise architecture, an integral security architecture consistent with organizational risk management and information security strategies. Security requirements and 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, PM-11, RA-2.

Control Enhancements: None.

References: NIST Special Publication 800-39; Web: [WWW.FSAM.GOV](http://WWW.FSAM.GOV).

## ***PM-8 CRITICAL INFRASTRUCTURE PLAN***

Applicability: Bureaus and Offices

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

Supplemental Guidance: 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.

## ***PM-9 RISK MANAGEMENT STRATEGY***

Applicability: Bureaus and Offices

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; and
- b. Implements that strategy consistently across the organization.

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***

Applicability: Bureaus and Offices

Control: The organization:

- a. Manages (i.e., documents, tracks, and reports) the security state of organizational information systems 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: The security authorization process for information systems requires the implementation of the Risk Management Framework and the employment of associated security standards and guidelines. Specific roles within the risk management process include a designated authorizing official for each organizational information system. Related control: CA-6.

Control Enhancements: None.

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

## ***PM-11 MISSION/BUSINESS PROCESS DEFINITION***

Applicability: Bureaus and Offices

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 an achievable set of protection needs is obtained.

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.