

**Department of the Interior**  
**Security Control Standard**  
**Personnel Security**

**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>
Chris Peterson	0.1	January 24, 2011	Initial draft
Timothy Brown	0.2	January 25, 2011	Incorporated comments into body text
Timothy Brown	0.21	February 15, 2011	Checked cloud mandated controls
Timothy Brown	1.0	February 17, 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

**REVISION HISTORY .....3**

**TABLE OF CONTENTS .....4**

**SECURITY CONTROL STANDARD: PERSONNEL SECURITY .....5**

    PS-1 PERSONNEL SECURITY POLICY AND PROCEDURES .....5

    PS-2 POSITION CATEGORIZATION .....6

    PS-3 PERSONNEL SCREENING.....6

    PS-4 PERSONNEL TERMINATION .....7

    PS-5 PERSONNEL TRANSFER.....7

    PS-6 ACCESS AGREEMENTS .....8

    PS-7 THIRD-PARTY PERSONNEL SECURITY .....8

    PS-8 PERSONNEL SANCTIONS.....9

## SECURITY CONTROL STANDARD: PERSONNEL SECURITY

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 Personnel Security (PS) 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**.

### ***PS-1 PERSONNEL SECURITY POLICY AND PROCEDURES***

Applicability: Bureaus and Offices

Control: The organization develops, disseminates, and reviews/updates at least annually:

- a. A formal, documented personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
- b. Formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the personnel security family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The personnel security policy can be included as part of the general information security policy for the organization. Personnel security procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the personnel security policy. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

<b>P1</b>	<b>LOW PS-1</b>	<b>MOD PS-1</b>	<b>HIGH PS-1</b>
-----------	-----------------	-----------------	------------------

## ***PS-2 POSITION CATEGORIZATION***

Applicability: All Information Systems

Control: The organization:

- a. Assigns a risk designation to all positions;
- b. Establishes screening criteria for individuals filling those positions; and
- c. Reviews and revises position risk designations at least every three years.

Supplemental Guidance: Position risk designations are consistent with Office of Personnel Management policy and guidance. The screening criteria include explicit information security role appointment requirements (e.g., training, security clearance).

Control Enhancements: None.

References: 5 CFR 731.106(a).

Priority and Baseline Allocation:

<b>P1</b>	<b>LOW PS-2</b>	<b>MOD PS-2</b>	<b>HIGH PS-2</b>
-----------	-----------------	-----------------	------------------

## ***PS-3 PERSONNEL SCREENING***

Applicability: All Information Systems

Control: The organization:

- a. Screens individuals prior to authorizing access to the information system; and
- b. Rescreens individuals according to the following schedule: for national security clearances; a reinvestigation is required during the 5th year for top secret security clearance, the 10th year for secret security clearance, and 15th year for confidential security clearance. For moderate risk law enforcement and high impact public trust level, a reinvestigation is required during the 5<sup>th</sup> year. There is no reinvestigation for other moderate risk positions or any low risk positions.

Supplemental Guidance: Screening and rescreening are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidance, and the criteria established for the risk designation of the assigned position. The organization may define different rescreening conditions and frequencies for personnel accessing the information system based on the type of information processed, stored, or transmitted by the system.

Control Enhancements: None Mandated.

References: 5 CFR 731.106; FIPS Publications 199, 201; NIST Special Publications 800-73, 800-76, 800-78; ICD 704.

Priority and Baseline Allocation:

<b>P1</b>	<b>LOW PS-3</b>	<b>MOD PS-3</b>	<b>HIGH PS-3</b>
-----------	-----------------	-----------------	------------------

## ***PS-4 PERSONNEL TERMINATION***

Applicability: All Information Systems

Control: The organization, upon termination of individual employment:

- a. Terminates information system access;
- b. Conducts exit interviews;
- c. Retrieves all security-related organizational information system-related property; and
- d. Retains access to organizational information and information systems formerly controlled by terminated individual.

Supplemental Guidance: Information system-related property includes, for example, hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes. Exit interviews ensure that individuals understand any security constraints imposed by being former employees and that proper accountability is achieved for all information system-related property. Exit interviews may not be possible for some employees (e.g., in the case of job abandonment, some illnesses, and nonavailability of supervisors). Exit interviews are important for individuals with security clearances. Timely execution of this control is particularly essential for employees or contractors terminated for cause.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

<b>P2</b>	<b>LOW PS-4</b>	<b>MOD PS-4</b>	<b>HIGH PS-4</b>
-----------	-----------------	-----------------	------------------

## ***PS-5 PERSONNEL TRANSFER***

Applicability: All Information Systems

Control: The organization reviews logical and physical access authorizations to information systems/facilities when personnel are reassigned or transferred to other positions within the organization and initiates **[Assignment: organization-defined transfer or reassignment actions]** within five days.

**Supplemental Guidance:** This control applies when the reassignment or transfer of an employee is permanent or of such an extended duration as to make the actions warranted. In addition the organization defines the actions appropriate for the type of reassignment or transfer; whether permanent or temporary. Actions that may be required when personnel are transferred or reassigned to other positions within the organization include, for example: (i) returning old and issuing new keys, identification cards, and building passes; (ii) closing previous information system accounts and establishing new accounts; (iii) changing information system access authorizations; and (iv) providing for access to official records to which the employee had access at the previous work location and in the previous information system accounts.

**Control Enhancements:** None.

**References:** None.

**Priority and Baseline Allocation:**

<b>P2</b>	<b>LOW PS-5</b>	<b>MOD PS-5</b>	<b>HIGH PS-5</b>
-----------	-----------------	-----------------	------------------

## ***PS-6 ACCESS AGREEMENTS***

**Applicability:** All Information Systems

**Control:** The organization:

- a. Ensures that individuals requiring access to organizational information and information systems sign appropriate access agreements prior to being granted access; and
- b. Reviews/updates the access agreements at least annually.

**Supplemental Guidance:** Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Signed access agreements include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with the information system to which access is authorized. Electronic signatures are acceptable for use in acknowledging access agreements unless specifically prohibited by organizational policy. Related control: PL-4.

**Control Enhancements:** None Mandated.

**References:** None.

**Priority and Baseline Allocation:**

<b>P3</b>	<b>LOW PS-6</b>	<b>MOD PS-6</b>	<b>HIGH PS-6</b>
-----------	-----------------	-----------------	------------------

## ***PS-7 THIRD-PARTY PERSONNEL SECURITY***

**Applicability:** All Information Systems

**Control:** The organization:

- a. Establishes personnel security requirements including security roles and responsibilities for third-party providers;
- b. Documents personnel security requirements; and
- c. Monitors provider compliance.

Supplemental Guidance: Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management. The organization explicitly includes personnel security requirements in acquisition-related documents.

Control Enhancements: None.

References: NIST Special Publication 800-35.

Priority and Baseline Allocation:

<b>P1</b>	<b>LOW PS-7</b>	<b>MOD PS-7</b>	<b>HIGH PS-7</b>
-----------	-----------------	-----------------	------------------

## ***PS-8 PERSONNEL SANCTIONS***

Applicability: All Information Systems

Control: The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.

Supplemental Guidance: The sanctions process is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The process is described in access agreements and can be included as part of the general personnel policies and procedures for the organization. Related controls: PL-4, PS-6.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

<b>P3</b>	<b>LOW PS-8</b>	<b>MOD PS-8</b>	<b>HIGH PS-8</b>
-----------	-----------------	-----------------	------------------