UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Chief Information
Officer

OPM Information Security and Privacy Policy Addendum (FY13)

Chief Information Officer (CIO)

Information Technology Security and Privacy (ITSP)

February 2013

Table of Contents

Revision History

Version Number	Version Date	Revision Summary
0.1	February 2013	Initial Draft
1.0	February 2013	Final

EXECUTIVE SUMMARY

The OPM Information Security and Privacy Policy (ISPP) Handbook was published in March of 2011. OPM Information Technology Security and Privacy (ITSP) has the responsibility to periodically review and update policy based on changes to federal regulations, best practices, or organizational operating environment. This policy addendum has been developed to provide new or updated OPM policy statements that are aligned with such changes. This policy addendum combines a variety of policy updates into a single policy addendum that should be utilized when referring to the OPM ISPP. The policy areas covered in the addendum include:

- Information Security Continuous Monitoring;
- Contractor / External System Oversight;
- Passwords and Password Resets;
- System Owner Roles and Responsibilities.

Content in these topic areas are labeled as either SUPPLEMENTAL or REVISION. SUPPLEMENTAL updates refer to policy statements that have been enhanced, not replaced, in the current ISPP Handbook. REVISION refers to the policy statements that replace the existing policy requirements in the ISPP Handbook. The next major update to the ISPP will incorporate all policy addendums and relevant information that were not captured in time for this policy addendum.

1. INTRODUCTION

This security policy addendum provides revised or supplemental security and privacy policy for the OPM Information Security and Privacy Policy (ISPP) Handbook. It covers several security and privacy topic areas. Each topic area is contained in its own section. Each section includes a label of 'REVISION', 'SUPPLEMENTAL', or both. A REVISION refers to policy that is replacing the content currently in the ISPP Handbook. The SUPPLEMENTAL refers to policy or procedures that are in addition to what is in the ISPP Handbook.

Label	Effect	Compliance
REVISION	This policy replaces the contents of the ISPP Handbook for the specific section referenced.	OPM personnel and contractors must comply with the policy in the addendum.
SUPPLEMENTAL	This policy is in addition to the contents of the ISPP. ISPP policy	OPM personnel and contractors must comply with

	is still valid.	the ISPP Handbook **AND** the policy in this addendum.

1.1. *Purpose*

The purpose of this OPM Information Security and Privacy Policy Addendum is to provide updated information security and privacy policies to the current OPM ISPP. This document is an addendum to the OPM ISPP Handbook.

1.2. *Scope and Applicability*

The policies in this document, the same as the policies in the ISPP Handbook, apply to all OPM information resources. OPM information includes data that is owned, sent, received, or processed by the agency and includes information in either physical or digital form. OPM information resources include OPM hardware, software, media, and facilities.

Everyone who uses, manages, operates, maintains, or develops OPM applications or data wherever the applications or data reside must comply with the Information Security and Privacy Policy, unless a specific waiver is obtained from the Chief Information Officer (CIO) or the Chief Information Security Officer (CISO).

The Information Security and Privacy Policy is also relevant to all contractors acting on behalf of OPM and to non-OPM organizations or their representatives who are granted authorized access to OPM information and information systems. Finally, this policy applies to other agencies' systems as delineated in Memorandums of Understanding (MOU) and Interconnection Security Agreements (ISA) with OPM.

System Owners are ultimately responsible for the implementation of security policies to protect their information systems. Roles and responsibilities are called out in the individual security policy statements in the ISPP Handbook, as well as this ISPP addendum. Where no specific role is identified, it is assumed that the system owner is responsible for security policy implementation.

1.3. *Compliance, Enforcement, and Exceptions*

This ISPP addendum follows the same compliance, enforcement, and exceptions as documented in section 1.3 of the ISPP Handbook.

1.4. *Document Approval / Update*

This OPM information security and privacy policy addendum has been approved, as indicated by the signatures below. This approval pertains to the information contained in this document only. Associated security procedures, guidance, or other documentation will be approved separately on a case-by-case basis as needed to support this policy addendum.

Andy Newton — 2/15/2013

Andy Newton
OPM/CIO/ITSP
Chief Information Security Officer

For [signature] — 2/19/13

Matthew Perry
OPM/CIO
Chief Information Officer

2. INFORMATION SECURITY CONTINUOUS MONITORING

Continuous monitoring of OPM information systems is required per the OPM Information Security and Privacy Policy (ISPP) Handbook and the OPM Information Technology FISMA Procedures. The following policy replaces the CA-7 policy documented in the ISPP Handbook.

REVISION: ISPP section 5.2.6 Continuous Monitoring (CA-7)

The Information System Security Officer (ISSO), Designated Security Officer (DSO) and technical managers, in consultation with the System Owners (SO), Authorizing Official (AO), and Chief Information Security Officer (CISO) shall assess all security controls in an information system during the initial security authorization (see CA-6). Subsequent to the initial authorization and in accordance with Office of Management and Budget (OMB) and Office of Personnel Management (OPM) policy, all security controls shall be assessed as part of continuous monitoring activities (ongoing security operations). For new security authorizations and reauthorizations, the Security Assessment Report (SAR), included in the security authorization package, meets the continuous monitoring reporting requirement. Further continuous monitoring reporting shall be based on the security categorization of the system. SOs shall report the security state of the information system to appropriate organizational officials according to the following schedule:

- Continuous Monitoring Security Reports must be provided to IT Security and Privacy office (ITSP) for High Impact Systems ***at least quarterly***.

- Continuous Monitoring Security Reports must be provided to ITSP for Moderate and Low Impact Systems ***at least semiannually***.

Assessment and testing of security controls of a system's security-relevant changes, including the implementation of POA&Ms, that occur out of the authorization/reauthorization cycle, but do not constitute a "major change" to the information system, shall be documented in a Security Impact Assessment (SIA).

The continuous monitoring of system security controls is based on a number of factors that are unique to each information system and operating environment. With this understanding, the SO shall detail the information system's Information Security Continuous Monitoring Plan (ISCMP) in their System Security Plan (SSP). System Owners shall consider the following criteria when developing their ISCMP:

- OPM IT Security Policy requirements

- The Federal Information Processing Standard (FIPS) 199 Security Categorization and impact levels for Confidentiality, Integrity and Availability
- The current threat environment of the information system
- The volatility of security controls
- Recent system changes and/or POA&M implementations

In some circumstances, based on the security risk and volatility of a security control, assessment/testing of security controls may occur more frequently (i.e. weekly vulnerability scans for HIGH Impact Systems versus the annual review of the SSP).

Remediation evidence shall be recorded within the Continuous Monitoring Security Report when weaknesses are immediately corrected. Planned corrective actions shall be entered into the POA&Ms for weaknesses not immediately corrected.

Information systems and their constituent components shall be included within a configuration/change management process to ensure baseline security configurations are maintained.

3. PATCH MANAGEMENT

Security-relevant software updates (e.g. patches, service packs, and hotfixes) must be installed in a timely manner to prevent vulnerabilities from remaining open for extended periods of time.

SUPPLEMENTAL: Supplemental guidance to the OPM ISPP Section 6.9.2 Flaw Remediation (SI-2)

SOs shall ensure that patches that remediate recently announced software flaws are installed according to the following schedule:

- Patches that remediate Critical-risk software flaws must be installed within ***one (1) week***;
- Patches that remediate High-risk software flaws must be installed within ***two (2) weeks***;
- Patches that remediate Medium-risk software flaws must be installed within ***three (3) weeks***; and
- Patches that remediate Low-risk software flaws must be installed within ***four (4) weeks***.

4. CONTRACTOR / EXTERNAL SYSTEMS OVERSIGHT

SUPPLEMENTAL: Supplemental guidance to the OPM ISPP Handbook

OPM information security and privacy policies apply to all OPM information systems whether they are hosted at OPM sites or hosted external to OPM (i.e. contractor or other Federal Agency). It is the responsibility of the OPM system owner to ensure systems or services hosted

by non-OPM organizations comply with OPM information security and privacy policies. The following policies related to contractor systems support the existing policies identified in the OPM ISPP Handbook.

- No contractor may hold any of the following IT security roles: DSO, ISSO, SO and AO. Program Offices are responsible for appointing federal personnel for these roles.

- All contracts for information technology support or services must include specific security requirements consistent with OPM information security and privacy policies.

- All contracted information technology services must comply with applicable OPM information security and privacy policies.

- Information security and privacy requirements for contracted information technology services must address how sensitive information is to be handled and protected at the contractor's site, including any information collected, stored, processed, or transmitted using the contractor's computer systems, the background investigation and/or clearances required, and the facility security required.

- Statements of work and contracts shall require that at the end of the contract the contractor must return all information and IT resources provided during the life of the contract and must certify that all OPM information has been purged from any contractor-owned system used to process information. A decommissioning plan must be submitted for review and approval by the contracting parties and OPM.

- Security clauses in contracts and Statements of Work for information technology services must be reviewed by Information Technology Security and Privacy (ITSP) during the acquisition process and prior to contract award.

- OPM System Owners must ensure that an annual security controls assessment is performed by a government employee or an independent third party at the site where contracted information technology services are rendered. The assessment results must be provided to ITSP for review using OPM's standard templates.

5. ACCESS PERMISSIONS

Access control policies (e.g., identity-based policies, role-based policies, attribute-based policies) and access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) are employed by OPM to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system. In addition to enforcing authorized access at the information system level,

access enforcement mechanisms are employed at the application level, when necessary to provide increased information security for OPM.

SUPPLEMENTAL: Supplemental guidance to the OPM ISPP Handbook, Section 7.1.3 Access Enforcement (AC-3)

SOs shall ensure that access permissions are reviewed ***at least every two years*** in accordance with the OPM IT Security FISMA Procedures.

6. USER IDENTIFIERS

Organizational users include OPM employees or individuals the organization deems to have equivalent status of employees (e.g., contractors, interns, etc.). Adequate controls shall be implemented and maintained on systems to confirm user identity prior to access. The access protection measures shall provide assurance of individual accountability through identification and authentication of each information system user.

Non-organizational users typically include individuals of the public, retired Federal employees (annuitants), non OPM Federal employees, applicants, etc. In accordance with the E-Authentication E-Government initiative, authentication of non-organizational users accessing federal information systems may be required to protect federal, proprietary, or privacy-related information (with exceptions noted for national security systems). Accordingly, an E-Authentication Risk Assessment is used in determining the authentication needs of the organization.

SUPPLEMENTAL: Supplemental guidance to the OPM ISPP Section 7.3.2 Identification and Authentication – Organizational Users (IA-2)

SOs shall ensure that organizational users are not identified by social security number (SSN) when feasible.

SUPPLEMENTAL: Supplemental guidance to the OPM ISPP Section 7.3.8 Identification and Authentication – Non-Organizational Users (IA-8)

SOs shall ensure that non-organizational users are not identified by social security number (SSN) when feasible.

7. PASSWORDS AND PASSWORD RESETS

The following policy replaces IA-5 policy documented in the Information Security and Privacy Policy (ISPP) Handbook.

REVISION: ISPP Section 7.3.5 Authenticator Management (IA-5)

SOs shall ensure implementation of authenticators (e.g., passwords, tokens, biometrics, Public Key Infrastructure (PKI) certificates, key cards) that prevent unauthorized access to systems.

Users shall maintain authenticators and protect them from inadvertent disclosure. Measures to safeguard user authenticators include, for example, maintaining possession of individual authenticators, not loaning or sharing authenticators with others, and reporting lost or compromised authenticators immediately. Administration of the authentication data shall include procedures to disable lost or stolen tokens, smart cards, or passwords, and include procedures for the recovery of cryptographic keys.

Information system authenticators for users and devices shall be managed by:

- Verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator;
- Establishing initial authenticator content for authenticators defined by the organization;
- Ensuring that authenticators have sufficient strength of mechanism for their intended use;
- Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
- Changing default content of authenticators upon information system installation;
- Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate);
- Changing/refreshing authenticators (references for authentication types are listed below);
- Protecting authenticator content from unauthorized disclosure and modification; and
- Requiring users and devices to implement specific measures to safeguard authenticators.

OPM requires Personal Identity Verification (PIV) cards to gain access to information systems in accordance with Homeland Security Presidential Directive (HSPD)-12, Federal Information Processing Standard (FIPS 201), and OMB Memorandum M-11-11 when feasible. PIV cards may use a combination of authenticator mechanisms (i.e., card holder unique identifier (CHUID), PKI certificate, or biometrics) depending upon the assurance level required.

The information system for password-based authentication shall enforce minimum password complexity of:

- At least ***eight (8)*** characters for non-privileged accounts; and at least ***twelve (12)*** characters for privileged accounts
- 3 of the following 4 attributes:
    - Uppercase letters (A-Z)
    - Lower case letters (a-z)

- Numbers (0-9)
- Special characters (!, “, #, $, %, &, *, +, -, :, <, =, >, ?, @, [,], _, {, })

- Enforce ***at least one (1) character to be changed*** from the previous password to the new password when passwords are reset;

- Encrypt passwords in storage and in transmission (Passwords shall not be stored in clear text or in any easily reversible form in batch files, automatic login scripts, software macros, terminal function keys, or in any location where an unauthorized person might discover them);

- Enforce password minimum and maximum lifetime restrictions of ***one (1) day minimum and 60 day maximum***;

- Prohibit password reuse for ***twenty four (24)*** generations;

- Lock an account after ***three (3)*** consecutive invalid login attempts *(Reference AC-7)*.

Exceptions:

- Mainframe passwords shall be ***eight (8)*** characters long and shall be in alphanumeric format (any combination of numbers and/or letters).

- Blackberry passwords shall be at least ***eight (8)*** alphanumeric characters.

- Passwords for machine/process accounts may not expire. An approved Form 1665 is required.

Additional password management requirements include:

- Passwords shall be audited on a regular basis for compliance to ensure strength of passwords is sufficient. If a password is guessed or cracked during an audit, the user shall change it.
- Temporary passwords shall be changed upon initial login.
- The system shall provide a mechanism that notifies the user when a password change is required.
- Passwords shall not be visible on screen or any other output device.
- User passwords shall not be hard-coded into software.
- When providing user identifiers (userID) and passwords to users, two different media (telephone, postal, e-mail, or a secure Web site) shall be used. One medium to deliver the userID and another medium to deliver the password to prevent account compromise.

- Collection of userIDs and/or passwords shall not be permitted, except for purposes of authorized network, system, or security administration.
- The following list outlines additional recommendations, or safeguards for users:
- Passwords shall not contain any of the following:
    - UserID or any part of your full name
    - Dictionary words or common names (e.g., Betty, Fred, Rover)
    - Portions of associated account names (e.g., userID, login name)
    - Consecutive character strings (e.g., abcdef, 12345)
    - Simple keyboard patterns (e.g., qwerty, asdfgh)
    - Generic passwords (i.e., password consisting of a variation of the word "password" (e.g., P@sswOrdl))
- Shall not reveal a password over the phone to ANYONE.
- Shall *only* reveal a password in an email message if it is a temporary password.
- Shall not reveal a password to the Help Desk.
- Shall not discuss a password in front of others.
- Shall not hint at the format of a password (e.g., "my family name").
- Shall not reveal a password on questionnaires or security forms.
- Shall not share passwords with anyone including management, co-workers, administrative assistants, or secretaries.
- Shall not store hard copies of passwords in common areas (e.g., writing down the password and sticking it to the side of a monitor, under keyboard, etc.). If passwords, such as emergency passwords or administrator passwords must be written down, they shall be placed in a sealed envelope and secured in a locked container.
- Shall immediately notify supervisors and the respective Help Desk if an account or password is suspected to have been compromised, and change all passwords.

Reference the *LAN Complex Passwords* standard for network users and the *Sysplex Security Policy and Procedures* for Mainframe user identification and authentication requirements.

The information system for **PKI-based authentication** shall:

- Validate certificates by constructing a certification path with status information to an accepted trust anchor (i.e., certificate revocation lists or online certificate status protocol responses);
- Enforce authorized access to the corresponding private key; and
- Map the authenticated identity to the user account.

The registration process to receive ***HSPD-12 PIV smartcards and other PKI authenticators*** shall be carried out in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor).

Cardholder and PKI certificate Personal Identification Numbers (PIN) are not subject to aging criteria that are required for traditional passwords. The term "PIN" and "password" are not synonymous. National Institute of Standards and Technology (NIST) SP 800-53 control IA-5, regarding Authenticator Management, distinguishes between password expiration requirements and PKI certificate requirements. FIPS PUB 201-1 defines the logical functions for PIV credentials including:

- Proof of the identity of the cardholder to the card
- Proof of the identity of the cardholder to a remote entity (i.e., application, system)

NIST SP 800-73-3, Interfaces for Personal Identity Verification–Part 2: End-Point PIV Card Application Card Command Interface is an additional reference for PIN requirements.

PINs accomplish the intent of category (1) above, validating cardholder identity to the PIV card. Knowledge of a PIN is the means by which an individual can be authenticated to the PIV Card Application. Passwords accomplish the intent of category (2) above by validating cardholder identity to a remote entity, application, or system.

The process of PIN entry, validating a cardholder to a card or an individual to a PKI certificate, occurs locally on a number pad or cardholder controlled system. The PIN never traverses an unprotected medium, and thus significantly limits exposure. Passwords may traverse an unprotected network, and thus the use of passwords to validate cardholder identity to a remote entity, application, or system increases exposure. The increased risk of password exposure is mitigated by the use of password aging techniques. The longevity of cardholder and PKI certificate PINs far exceed that of passwords due to the significantly limited exposure to attack, and thus are not subject to the same aging criteria required for traditional passwords. ***However, it is a recommended best practice that cardholders periodically change their PIN.***

SUPPLEMENTAL: Supplemental guidance to the OPM ISPP Section 7.3.5 Authenticator Management (IA-5)

The following conditions must be adhered to for OPM information systems (including those operated or maintained by a contractor) that rely on password reset functionality for users that allows a user to reset a forgotten or compromised password:

- Passwords provided after successful user identification must be temporary and require the user to change the password upon the initial login with this password.

- Password resets or temporary passwords must not be provided through the application interface; a secondary means of transmission must be utilized to provide the temporary password using user information registered with the system (i.e. a temporary password or a hyperlink to a secure password reset website may be sent to the user's email registered

with the system or a phone call from system support to the user's phone number registered with the system.)

- Emails sent to users with their temporary password must not contain the user ID.

Information systems must limit the use of 'secret questions' to verify identity prior to allowing a user to utilize a password reset function. The use of 'secret questions' must be implemented such that an attacker cannot easily guess the answer.

- Secret questions must avoid commonly guessed fact-based answers such as city of birth, year of graduation, number of siblings.
- Multiple questions must be used, as opposed to a single question and answer.
- Easily obtained/guessed questions must not be utilized, such as:
  - What is your favorite sports team?
  - What city were you born in?
  - What year did you graduate High School / College?
  - How many siblings do you have?

APPENDIX A: ACRONYMS

Acronym	Expansion
A&A	Assessment and Authorization
CIO	Chief Information Officer
CIRT	Computer Incident Response Team
CISO	Chief Information Security Officer
CISSP	Certified Information System Security Professional
CPO	Chief Privacy Officer
DSO	Designated Security Officer
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
GSS	General Support System
HR	Human Resources
IG	Inspector General
IPD	Initial Public Draft
IS	Information System
ISCP	Information System Contingency Plan
ISCM	Information Security Continuous Monitoring
IT	Information Technology
ITSP	Information Technology Security and Privacy (group)
ITSWG	Information Technology Security Working Group
IV&V	Independent Verification and Validation
MA	Major Application
MI	Minor Application
NIST	National Institute of Standards and Technology
NMG	Network Management Group
OGC	Office of General Counsel
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PO	Program Office
POA&M	Plan of Actions and Milestones
PS	Parent System
PUB	Publication
RMF	Risk Management Framework
SitRoom	OPM Situation Room
SoS	System of Systems

SP	Special Publication
SS	Sub-System
SSN	Social Security Number
SSP	System Security Plan
US-CERT	United States Computer Emergency Readiness Team

APPENDIX B: REFERENCES

- (NIST) National Institute of Standards and Technology. (2010). Special Publication 800-53 revision 3 Recommended Security Controls for Federal Information Systems and Organizations.
- (NIST) National Institute of Standards and Technology. (2010). Special Publication 800-39 Managing Information Security Risk, Organization, Mission, and Information System View.
- (NIST) National Institute of Standards and Technology. (2010). Special Publication 800-37 revision 1 Guide for Applying the Risk Management Framework to Federal Information Systems.
- (NIST) National Institute of Standards and Technology. (2010). Special Publication 800-34 revision 1 Contingency Planning Guide for Federal Information Systems.
- OMB Circular No. A-130, Revised (Transmittal Memorandum No. 4), Management of Federal Information Resources, November 30, 2000.
- (OPM) Office of Personnel Management. (2011). IT Security and Privacy Policy Handbook.
- (OPM) Office of Personnel Management. (2011). Information Technology Security FISMA Procedures.
- (OPM) Office of Personnel Management. (2010). Privacy Impact Assessment Guide.
- (OPM) Office of Personnel Management. (2011). Security Assessment and Authorization Guide.
- (OPM) Office of Personnel Management. (2010) IT Strategic Plan 2010 – 2013.
- Public Law 107-347, Federal Information Security Management Act of 2002 (Title III of the E-Government Act of 2002), as amended.