OPM Information Security and Privacy Policy Addendum (FY12)

Chief Information Officer (CIO)

Information Technology Security and Privacy (ITSP)

March 2012

Table of Contents

Appendicies

Revision History

Version Number	Version Date	Revision Summary
0.1	March 2012	Initial Version

EXECUTIVE SUMMARY

The OPM Information Security and Privacy Policy Handbook (ISPP) was published in March of 2011. OPM Information Technology Security and Privacy (ITSP) has the responsibility to periodically review and update the 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 one 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
- Agency Risk Management
- Independent Verification and Validation
- Contingency Plan Testing
- System Characterization
- Passwords and Password Resets
- Reduction in use of Social Security Numbers

Content in these topic areas are labeled as either SUPPLEMENTAL or REVISION. SUPPLEMENTAL refers to policy statements that supplement, but do not replace the current policy in ISPP. REVISION refers to the policy statements that replace the existing policy requirements in the ISPP. The next major update to the ISPP will incorporate all information still relevant at the time in this Policy addendum.

1. INTRODUCTION

The OPM Information Security and Privacy Policy addendum provides revised or supplemental security and privacy policy to the OPM Information Security and Privacy Policy (ISPP). This addendum covers several security and privacy topic areas. Each topic area is containcd in its own section. Each section includes either a label 'REVISION' or '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 contractor must comply with the policy in the addendum.
SUPPLEMENTAL	This policy is in addition to the contents of the ISPP. ISPP policy is still valid.	OPM personnel and contractors must comply with the ISPP **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.

1.2 *Scope and Applicability*

The policies in this document, the same as the policies in the ISPP, 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 thc 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 authorizcd 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.

This Information Security and Privacy Policy (ISPP) does not include specific procedures to implement these policies. Procedures will be developed separately and maintained by the CISO.

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 and this ISPP addendum, but where no specific role is identified, it is assumed that the system owner is responsible to security policy implementation.

1.3 *Compliance, Enforcement, and Exceptions*

This ISPP addendum follows the same compliance, enforcement, and exceptions as the ISPP itself as documented in section 1.3 of the OPM ISPP. Refer to section 1.3, *Compliance, Enforcement, and Exceptions* of the ISPP.

1.4 *Document Approval / Update*

This OPM Information Security and Privacy Policy Addendum is approved. 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.

[Insert Name] 3/27/2012
OPM/CIO/ITSP Date
Chief Information Security Officer

[Insert Name] 04/22/2012
OPM/CIO Date
Chief Information Officer

2. INFORMATION SECURITY CONTINUOUS MONITORING

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

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

The Information System Security Officer/Designated Security Officer (ISSO/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). SOs shall report the security state of the information system to appropriate organizational officials ***at least annually***.

The results of the annual security assessment must be provided to ITSP utilizing the Annual System Security Report (ASSR) template.

For new security authorizations and re-authorizations, the testing accomplished during the security assessment meets the annual Federal Information Security Management Act (FISMA) testing requirement. Therefore, a separate ASSR is not required. The anniversary date of the authorization shall be used as the due date for the ASSR.

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 results of all SIAs during the year shall be included in the annual ASSR.

The continuous monitoring of system security controls is based on a number factors that is 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.
- Weaknesses through inheritance.

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

Remediation evidence shall be recorded within ASSR when weaknesses are immediately corrected. Planned corrective actions shall be entered into the POA&Ms for weakness 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. CONTRACTOR / EXTERNAL SYSTEMS OVERSIGHT

SUPPLEMENTAL: Supplemental guidance to the OPM ISPP

OPM information security and privacy policies apply to all OPM information systems whether they are hosted at OPM sites or hosted external to OPM (ie 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.

- 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 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 DHS information.

- Security clauses in contracts and Statements of Work for information technology services must be reviewed by Information Technology Security and Privacy (ITSP) prior to execution of services.

- OPM Program Offices must ensure a site assessment is performed at the site where contracted information technology services are rendered. The assessment results must be provided to ITSP for review.

4. AGENCY RISK MANAGEMENT

OPM Agency Risk Management policies follow NIST guidelines including the multitiered approach to Risk Management. OPM addresses risk at the three tiers identified by NIST (NIST SP 800-39, *Managing Information Security Risk, Organization, Mission, and Information System View.*) The three tiered approach is comprised of risk management functions that are applied at three levels across the Agency, including Agency level (Tier 1), Mission/Business Process level (Tier 2), and System level (Tier 3).

SUPPLEMENTAL: Supplemental guidance to the OPM ISPP

The OPM Risk Executive is comprised of the CISO, Deputy CIO, Chief of Enterprise Architecture, and Chief of Quality Assurance. The OPM Risk Executive functions as an ad-hoc risk management role. This function, described in section 2.3.1 of the ISPP, is responsible for establishing an organizational risk framework for OPM to ensure risk decisions are determined with an organization perspective. The Risk Executive is responsible to ensuring risk management activities are conducted at Tier 1.

- The CISO shall coordinate Risk Executive meetings as needed to determine or gain acceptance for risk strategies and objectives associated with risks affecting multiple program offices.

- The CISO shall review and provide concurrence for all system and program-specific risk acceptance decisions and convene the Risk Executive as needed to support this effort.

- The Risk Executive shall manage organizational threat and vulnerability information and ensure this is incorporated into standard risk assessment and monitoring requirements, guidance and OPM risk-related templates.

- The Risk Executive shall define the organizational risk environment (risk framing) in coordination with senior leaders to ensure a consistent approach to risk management is defined across organizational strategic plans, policies, and procedures.

OPM program managers are responsible for ensuring risk management activities are conducted at Tier 2. The Tier 2 risk management responsibilities of the OPM program manger include:

- OPM program managers are responsible for defining the business processes that support their program and prioritizing these with respect to strategic goals and objectives of the organization.

- OPM program managers are responsible for defining the types of information needed to support the business processes that support their program and with support from system owners and DSOs, define the criticality of this information.

- OPM program managers with support from system owners and DSOs are responsible for incorporating information security requirements into the mission/business processes.

OPM system owners are responsible for ensuring risk management activities are conducted at Tier 3. These responsibilities include:

- Categorization of their information systems following FIPS 199 Categorization process,

- Allocating security controls respective of the system categorization, and

- Managing the selection, implementation, assessment, authorization and ongoing monitoring of allocated security controls.

5. INDEPENDENT VERIFICATION AND VALIDATION (IV&V)

Information Security Independent Verification and Validation (IV&V) is performed to determine whether information security practices or are being adhered to in an information system environment. The use of IV&V as an assessment mechanism for OPM information systems and organizations supplements the assessments conducted on OPM information systems as part of the Security Assessment and Authorization process. The IV&V may include testing of controls based on the results of an assessment to determine if the assessment was performed following OPM and Federal requirements, or may be used outside of A&A activities to determine the appropriateness of use of an external facility or product.

SUPPLEMENTAL: Supplemental guidance to the OPM ISPP

- Information Technology Security and Privacy (ITSP) shall independently verify and validate the development of A&A packages following OPM security policies and procedures. This IV&V does not include testing or verifying controls are in-place.

- Program Offices and System Owners shall conduct IV&V activities on an ad-hoc basis to ensure compliance with OPM information security and privacy policies and procedures.

6. CONTINGENCY PLAN TESTING

OPM information security policy in the OPM ISPP requires all OPM FISMA reportable information systems to have an Information System Contingency Plan (ISCP). This ISCP is required to be tested at least annually. The Policy and associated procedures are located in the

OPM ISPP and the OPM IT FISMA Security Procedures respectively (both of which are posted on THEO). All ISCPs must follow the OPM ISCP template format. In the event multiple systems are included in a single ISCP, all systems must be clearly identified and must include appropriate details to address contingency operations for each system.

- ISCP test results must be provided to CIO/ITSP each year.
- CIO/ITSP shall maintain the Agency-wide system inventory to include tracking Contingency Plan Testing.

SUPPLEMENTAL: Supplemental guidance to the OPM ISPP

- ITSP is responsible for developing and maintaining an Enterprise Business Impact Assessment to support Agency-wide approach to the development and testing of ISCPs.
- ITSP is responsible for developing and maintaining a standard OPM Business Impact Analysis (BIA) template.
- BIAs must be conducted on Moderate and High Availability systems utilizing the OPM-standard BIA template.
- Contingency Plan testing for applications residing on OPM General Support Systems must be coordinated with the GSS. It is the responsibility of the System Owner to ensure System CP Testing is coordinated with the underlying GSS. The CP Test results must include reference to the coordinated effort.
- ITSP is responsible to review CP results and verify appropriate coordination documented in the test results between OPM general support systems and the applications that reside on them.
- Annual Contingency testing is required for all OPM information systems including those operated out of a contractor or other non-OPM organizational facility. The annual contingency testing requirements must be included in contracts that include contractor operated system that process or store OPM information.
- The OPM Contingency Plan Coordinator is responsible for ensuring contingency testing is coordinated between across program offices

7. INFORMATION SYSTEM CHARACTERIZATION

All information systems that process, store, or transmit OPM information must be documented in a System Security Plan, have their controls assessed, and be authorized to operate based on the information contained in the authorization package. OPM authorizing officials are provided flexibility in defining boundaries for OPM information systems, however all information systems must be protected based on the information stored, processed, or transmitted {see system

categorization ISPP Section 5.3.2, Security Categorization (RA-2)}. The OPM system registration process requires the characterization of an information system as a Major Information System, or Minor Information System. A Major Information System can be one of several categories including; General Support System, Major Application, or System of Systems. The following policy supplements the policy stated in ISPP Section 3.1.5, Information System Inventory (PM-5) which includes the following criteria to determine if a system is a Major Information System:

- Systems with a FIPS 199 security categorization level of Moderate and High based on the following criteria;
    - Information contained, processed, stored, or transmitted requires special protection, or the information system is critical to the agency's mission.
- Any system that is called out in a major CPIC (Capital Planning and Investment Control) investment.
- Any system that is comprised of (or contains) an OPM-designated Critical Infrastructure Protection asset.

SUPPLEMENTAL: Supplemental guidance to the OPM ISPP

The following guidelines are provided to help define boundaries for OPM information systems, per NIST SP 800-37 revision 1. An information system contains the following characteristics:

- Information resources are generally under the same direct management control (involves budgetary, programmatic, or operational authority and associated responsibility and accountability.)

- Information resources support the same mission/business objectives or functions and essentially the same operating characteristics and information security requirements; and

- Reside in the same general operating environment (includes, for example, consideration of threat, policy, and management.)

OPM information systems must be characterized as either one of the following per Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources" and NIST SP 800-18, "Guide for Developing Security Plans for Federal Information Systems" definitions:

- General Support System (GSS) - A General Support System (GSS) is defined as "an interconnected set of information resources under the same direct management control which shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people".

- Major Application (MA) - A Major Application (MA) is defined as "an application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate".

- Major Information System - A Major Information System is defined as "an information system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources".

- Minor Application (MI) - An MI is defined as "an application, other than a major application, that requires attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Minor applications are typically included as part of a general support system".

- Parent System (PS) - A Parent System (PS) is defined as a system that has one or more SS/MI and is identified in the OPM FISMA Master Inventory as a GSS, MA or SoS.

- System of Systems (SoS) (and Net –Centric Architecture) - A System of Systems (SoS) is defined as "A complex system composed of subsystems and services that are part of a continuously evolving, complex community of people, devices, information and services interconnected by a network that enhances information sharing and collaboration. Subsystems and services may or may not be developed or owned by the same entity, and, in general, will not be continually present during the full life cycle of the system of systems. Examples of this architecture include service-oriented architectures and cloud computing architectures". The SoS differ from GSS in that they support a single work activity or business function/area and collectively fall within a single security boundary. SoS' are Major Applications.

- Sub-System (SS) - A Sub-System is defined as "a major subdivision or component of an information system consisting of information, information technology, and personnel that perform one or more specific functions." Sub-Systems are usually MA that fall with in the security boundary of a GSS or SoS.

8. PASSWORDS AND PASSWORD RESETS

OPM system owners are required to ensure their systems are utilizing PIV credentials for identifying and authenticating OPM employees and contractors as well as users from other Federal Agencies. A waiver will only be granted for this requirement with appropriate justification, approved by the Authorizing Official, the CISO, and the CIO. Systems that utilize passwords for authentication as either an alternative process to PIV cards, or as a secondary authentication mechanism, must follow OPM security policy for passwords. The following

password policies are documented in the OPM ISPP Section 7.3.5, Authenticator Management (IA-5):

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

- Enforce minimum password complexity of:
  - At least 8 characters for non-privileged accounts; and at least 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) changed character when new passwords are created;
- 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 8 characters long and shall be in alphanumeric format (any combination of numbers and/or letters).
- Blackberry passwords shall be at least 8 alphanumeric characters.
- Passwords for machine/process accounts may not expire.

SUPPLEMENTAL: Supplemental guidance to the OPM ISPP

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 stolen password:

- Passwords provided after successful user identification must be temporary and require the user to change the password upon 1st login with this password.

- Temporary password 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., password sent to user's email registered with the system, phone call from system support to 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 can not 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?

9. REDUCTION IN USE OF SOCIAL SECURITY NUMBERS

The social security number (SSN) has been widely used within the Federal government for many years as a means to identify and authenticate individuals. The SSN is highly valuable for identity thieves because it is often a necessary (if not necessarily sufficient) item of information that a thief needs to open new accounts in the victim's name. One of the most practical and cost-effective ways to prevent breaches is to collect and maintain sensitive data only when it is necessary to do so. Executive Order 9397 initially authorized all Federal agencies to use the SSN as a primary means of identification for individuals working for, or with OPM. This blanket use has since been rescinded, and no longer applicable to the federal government.

SUPPLEMENTAL: Supplemental guidance to the OPM ISPP

This guidance identifies the acceptable uses of the SSN, describes how authorized uses should be documented and presents alternatives for SSN use. **Any use of the SSN not provided for in this addendum will be considered unnecessary and shall be eliminated.** The use of the term "SSN" relates to all forms of SSN use, to include truncated or masked SSNs.

Acceptable Uses

Acceptable uses of the SSN are those that are provided for by law, require interoperability with organizations outside of OPM, or are required by "operational necessities". This term can be defined as "the result of inability to alter systems, processes or forms, due to costs or unacceptable level of risk. These collections will be highly scrutinized and ease of use or unwillingness to change are not acceptable justifications.

- For any program deemed as using the SSN unnecessarily, a Plan of Action and Milestones (POA&M) must be developed for the elimination of SSN use.

Below are general categories of use that may continue to be acceptable for SSN usage. Judgment will need to be used, based on the event that even though an acceptable use may loosely meet one or more of the justifications, does not mean that a specific justification is acceptable. The specific legislative or regulatory language must be examined to determine if the use of SSNs is acceptable.

1. Retirement Operations – SSN is primarily used for the entire life cycle of the retirement benefits and services offering, as a way to identify eligibility for benefits.

2. Law Enforcement – Almost all law enforcement application utilizes SSN in order to report and track individuals. This includes, but is not limited to, state criminal histories, Federal Bureau of Investigation records checks, etc.

3. Security Clearance Investigation or Verification – The initiation, conduct, or verification of security clearances requires the use of the SSN. The SSN is the single identifier that is consistent across the Security Investigation process.

4. Interactions with Financial Institutions – Federal law requires that individuals who hold accounts with financial institutions must provide the SSN as part of the process to open accounts. It may, therefore, be required for systems, processes or forms that interface with or act on behalf of individuals or organizations in transactions with financial institutions to provide the SSN.

5. Federal Employment – Federal statute requires that all persons employed within the United States must provide an SSN or comparable identifier to prove their identity for eligibility for employment by the U.S. Federal Government.

6. Administration of Federal Worker's Compensation – The Federal Worker's Compensation program continues to track individuals through the use of SSN. As such, systems, processes or forms that interacts with or provides information for the administration of this system or associated systems may be required to retain SSN.

7. Federal Taxpayer Identification Number – The application of Federal and State income tax programs rely on the use of SSN. As such, systems that have any function that pertains to the collection, payment, or record keeping of this use must contain SSN.

8. Computer Matching – Systems, processes, or forms that interact with other Government agencies may require the continued use of SSN as the primary identifier until such time as the applications to which they are linked move to another means of identification for transferring, matching, or checking information.

9. Legacy System Interface – Many systems, processes, forms that do not meet the criteria in the previous eight items for the continued use of the SSN may not be able to transition to another identifier in a timely manner due to the excessive cost associated with the change. In these cases, the continued use of SSN may be acceptable for a specified period of time, provided that a Plan of Action and Milestone (POA&M) is in place for the migration away from the SSN in the future.

10. Other Cases – The previous categories may not include all uses of the SSN delineated by law. Should a system owner be able to show sufficient grounds that a use case not specified in the first eight items of this section is required by law, then the process may continue to use the SSN. Any system or process that seeks to use this clause as justification must provide documentation in order to continue use under this justification.

Documenting Authorized Uses

Any system, process or form that collects, maintains or disseminates PII, to include SSN, must properly document the authority for that use. Without such justification, it is unacceptable to collect, maintain or disseminate SSN. The authorization for use is governed by the OPM Information Technology Security and Privacy (ITSP) under the Office of the Chief Information Officer (OCIO).

Alternatives

One of the primary reasons that many systems, processes or forms collect and use SSN is the ability for greater efficiency and use of just one identifier. With this use, increased risk exists for identity theft. To counteract this risk, alternatives to the SSN shall be used whenever possible. Examples include, the elimination of personal identifiers, use of an alternative personal identifier, or use of biometrics, etc. Contact the ITSP to discuss potential alternatives to SSN use.

10. PRIVACY INCIDENT RESPONSE

The Federal Information Security Management Act (FISMA) requires that all Federal Agencies have a security program that includes procedures for detecting, reporting, and responding to security incidents. In compliance with FISMA, the Office of Personnel Management (OPM) has developed Agency-wide information security and privacy policies documented in the OPM Information Security and Privacy Policy Handbook that includes Incident Response (IR) policies. These addendum policies supplement the IR policies in the OPM ISPP, and are specific to Incidents involving PII.

REVISION: ISPP section 4.6 Managing Privacy Incidents

The PII incident response and reporting process involves actions from various personnel across OPM. It is important that individuals understand their roles in order to ensure appropriate response and reporting actions are taken with regard to security incidents. The following roles and responsibilities are specific to the OPM incident response and reporting process, these roles may have other OPM responsibilities, but these responsibilities outlined here are intended to focus on their specific duties related to incident response and reporting.

- The Chief Information Officer (CIO) is responsible for:
    - Ensuring an OPM IR capability is established and implemented at OPM that handles Privacy Incidents in compliance with FISMA and OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information.*
- The Chief Privacy Officer (CPO) is responsible for providing day-to-day guidance of the incident response management process, including data discovery, analysis, response, escalation, tracking, and reporting.
    - Approval of Privacy Incident Notification activities, including signing notification letters to affected individuals.
- The Chief Information Security Officer (CISO) is responsible for carrying out the CPO responsibilities to include the development of OPM-wide incident response and reporting policies.
    - Has oversight responsibility for the OPM Computer Incident Response Team (CIRT).
    - Responsible for providing oversight in the investigation and, if needed, external communication of OCIO related privacy incidents.
- OPM Federal Investigative Services is responsible for investigating incidents related to Government Background Investigations.
- OPM Program Offices are responsible for ensuring privacy incidents within their offices and associated with their information systems are identified and reported following OPM policy:
    - Supporting the investigation, response, tracking, and reporting of Privacy incidents within their program and information systems to include support for determining appropriate notification procedures, sending and tracking notification letters to affected individuals in the event these actions are required.
- The Office of Inspector General (OIG) provides law enforcement authority and investigative support to any incident handling initiatives. If criminal activity is suspected, OIG must be

notified immediately. As determined by the OIG, other law enforcement support may be called in to assist in the investigation of a privacy incident.

- The Office of General Counsel (OGC) provides legal guidance for any privacy incident. If external notification is required, the OGC will review and approve all external communications to affected individuals as a result of a privacy incident.
- The Communications and Public Liaison (CPL) will review and approve all external communications to affected individuals as a result of a privacy incident.
- The OPM Computer Incident Response Team (CIRT) is responsible for:
    - Assisting in handling privacy incidents on behalf of the OPM CPO including:
        - discovery of, and response to, activities that might otherwise interrupt the day-to-day operations of the OPM infrastructure, and formalizing reporting of incidents to the Chief, NMG, ITSP, and the CIO.
        - Developing quarterly reports for US-CERT on security and privacy incidents at OPM. The Chief, NMG, in consultation with the CIRT, immediately reports serious incidents or other OMB or US-CERT IT security-related requests for information to US-CERT.
- The OPM SitRoom (OPM Situation Room) is responsible for:
    - Understanding the PII incident reporting process and procedures.
    - Acting as entry point for incidents involving PII, receiving information related to the incident and notifying:
    - Capturing incident information into a report that shall be provided to the organization conducting the investigation.
    - Assessing the initial level of risk associated with the confirmed or suspected incident.
    - Reporting all privacy incidents to US-CERT within one hour of being notified of the incident.
- OPM Employees / Contractors are responsible for:
    - Capturing relevant information about the suspected or confirmed breach.
    - Reporting any privacy incident or suspected privacy incident to their First-Line Supervisor immediately when becoming aware of the risk – regardless of the time or day of the week following the established reporting procedure. If supervisor is not available, employees are responsible for reporting to the Situation Room.

- Completing Information Technology Security and Privacy Training annually.

- OPM Supervisors and Managers are responsible for:
  - Ensuring full compliance with all OPM policies.
  - Understanding the PII incident reporting process and procedures.
  - Ensuring employees are made aware of the reporting procedures and the security policies in place to protect OPM information systems, employees, and property.
  - Reporting privacy incidents, for which OPM has responsibility, identified by individuals that fall under their supervision chain to the Situation Room within one hour of notification risk – regardless of the time or day of the week following the established reporting procedure.
  - Ensuring that the CIRT and SitRoom are immediately updated on changes to initially reported information.

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.