EPA Classification No.:	CIO-2150.3-P-12.1	CIO Approval Date:	08/06/2012
CIO Transmittal No.:	12-003	Review Date:	08/06/2015

Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19, dated 07/07/2005

INFORMATION SECURITY – INTERIM PLANNING PROCEDURES

V3.6

JULY 17, 2012

1. PURPOSE

The purpose of this procedure is to facilitate the implementation of Environmental Protection Agency (EPA) security control requirements for the Planning control family, as identified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 3 *Recommended Security Controls for Federal Information Systems and Organizations*.

2. SCOPE AND APPLICABILITY

These procedures cover all EPA information and information systems to include information and information systems used, managed, or operated by a contractor, another agency, or other organization on behalf of the agency.

These procedures apply to all EPA employees, contractors, and all other users of EPA information and information systems that support the operation and assets of EPA.

3. AUDIENCE

These procedures apply to all EPA employees, contractors, and all other users of EPA information and information systems that support the operations and assets of EPA.

4. BACKGROUND

Based on federal requirements and mandates, the EPA is responsible for ensuring that all offices within the Agency meet the minimum security requirements defined in the Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*. All EPA information systems must meet the security requirements through the use of the security controls defined in the NIST SP 800-53, Revision 3 *Recommended Security Controls for Federal Information Systems and Organizations*. This chapter addresses the procedures and standards set forth by EPA, and in compliance with, the planning family of controls found in NIST SP 800-53, Revision 3.

5. AUTHORITY

- E-Government Act of 2002, Public Law 107-347, Title III*, Federal Information Security Management Act (FISMA)* as amended
- Freedom of Information Act (FOIA), 5 U.S.C. § 552, as amended by Public Law 104-231, 110 Stat. 3048, Electronic Freedom of Information Act Amendments of 1996
- Clinger-Cohen Act of 1996, Public Law 104-106
- Paperwork Reduction Act of 1995 (44 USC 3501-3519)
- Privacy Act of 1974 (5 USC § 552a) as amended
- USA PATRIOT Act of 2001, Public Law 107-56
- Code of Federal Regulations, Part 5 Administrative Personnel, Subpart C—*Employees Responsible for the Management or Use of Federal Computer Systems*, Section 930.301 through 930.305 (5 C.F.R 930.301-305)
- Office of Management and Budget (OMB) Memorandum M-00-07, "*Incorporating and Funding Security in Information Systems Investments*," February 2000
- OMB Memorandum M-03-22, "*OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*," September 2003
- OMB Memorandum M-06-16," *Protection of Sensitive Agency Information*," June 2006
- OMB Circular A-11, "*Preparation, Submission and Execution of the Budget*," June 2006
- OMB Circular A-123, "*Revisions to OMB Circular A-123, Management's Responsibility for Internal Control*," December 2004
- OMB Circular A-130, "*Management of Federal Information Resources*," Appendix III, "*Security of Federal Information Resources*," November 2000
- Federal Information Processing Standards (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004
- FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006
- EPA Information Security Program Plan
- EPA Information Security Policy

6. PROCEDURES

<u>PL-2 – System Security Plan</u>

a. A System Security Plan (SSP) that describes the processes, procedures, and security controls currently being used or planned to be implemented to manage and secure the information system to meet security requirements, including rationale for the tailoring and supplemental decisions that must be developed, documented, updated, and implemented for the information system.

    i. The System Owner (SO) is responsible for the SSP.

    ii. The Information Security Officer (ISO) and Information System Security

Officer (ISSO) shall assist with developing the SSP.

- An ISSO responsible for the security of the information system must be designated in writing in accordance with OMB requirements and designated early in the development life cycle in order to adequately participate in creating the SSP.
- The SO or designee shall develop and maintain an SSP for each information system. Authorizing Officials (AOs) shall review and approve SSPs.

iii. Information system management staff and users shall assist management in developing the SSP by identifying any shortcomings or needed improvements to security.

b. The SSP must be consistent with the organization’s enterprise architecture.

c. The operational context of the information system must be described in the SSP in terms of missions and business processes.

d. The full set of security planning results must be documented in the SSP.

i. The SSP is the essential document that provides the background, system description (including the system boundaries), the security categorization (including supporting rationale), the essential personnel, the implementation status, and description of each and every security control.

e. The baseline SSP shall be completed within the Definition Phase of EPA’s system life cycle.

f. The following must be determined to support development of an SSP:

i. Whether the information system is a General Support System (GSS), Major Application (MA), or a minor application.

ii. If a Privacy Impact Assessment (PIA) is required.

- If the information system is or supports a Privacy Act System of Records, this information must be stated in the System of Records.

iii. The FIPS 199 security categorization based on the security objectives of confidentiality, integrity, and availability.

- Refer to *Information Security – Interim Risk Assessment Procedures* for requirements on completing the security categorization.

g. A risk assessment must be completed in order to fully develop and complete an SSP.

h. NIST SP 800-18 (as amended) must be used as guidance on security planning.

i. The version to be used for any new SSP or updates to SSPs will be communicated, along with the date to begin utilizing that version.

ii. The templates provided by EPA must be utilized in developing SSPs.

i. For GSSs, MAs, and minor applications:

i. If the information system is a GSS, the description must identify all GSSs, MAs, and minor applications that it supports.

ii. If the information system is an MA, the description must list the GSSs that support it.

iii. If a GSS or MA supports one or more minor applications, the SSP for that GSS or MA must also address the security requirements for those minor applications.

j. The information system and its operational environment must be described both generally and in technical terms.

i. Information processing flow, including key inputs and outputs, must be described for an MA.

ii. All IT assets, including hardware, software, and (if appropriate) networking/ telecommunications equipment, must be listed and described.

iii. The information system and subsystem authorization boundaries must be explicitly defined.

iv. That description must include applicable diagrams (e.g., network diagrams, system boundary, interconnections, data flow, and high level design).

v. The description must reflect any environmental or technical factors that are of security significance (e.g., versions, protocols, ports, wireless technology, public access, hosting or operation at a facility outside of the organization’s control), as applicable.

vi. Program and regional segment and solutions architects must be consulted, as appropriate.

k. If the information system has any relationship with (e.g., shares data) or connections to information systems outside the Agency, or between internal systems but across system boundaries, the connection must be detailed.

i. The information for each connection must include:

- The name of the connected information system.
- The information system’s organization and point of contact.
- The type of system.
- The authorization for the connection be it a Memorandum of Understanding (MOU), Memorandum of Agreement (MOA), or Interconnection Security Agreement (ISA) as appropriate for the organization and purpose.
  - Refer to *Information Security – Interim Security Assessment and Authorization Procedures* for requirements on system connection agreements.
- The date of the signed connection agreement.
- The FIPS 199 security categorization.
- Certification and accreditation (C&A) status and date.
- The name and title of the interconnected information system’s AO.

l. The laws, regulations, and policies that affect or govern the information system or the information stored, transmitted, or processed by the information system must be listed as authorities and references for the SSP.

m. FIPS 199 security categorization must be utilized to identify the minimum baseline security controls required for the information system.

i. The security control requirements for low, moderate, and high systems are defined in NIST SP 800-53 (as amended) guidance.

n. The SSP must document how the minimum baseline security controls required for the information system are implemented.

o. The minimum baseline security controls must be reviewed and selected within the context of the information system to determine which ones apply to the information system.

   i. Risk assessments must be used to determine if additional controls and/or control enhancements are required.

   ii. The SSP must address every NIST SP 800-53 (as amended) control required for the categorization level of the information system.

   iii. For each baseline security control that is outside of a specific information system's scope, the baseline security control must still be addressed in the SSP with a description of the rationale supporting the scoping decision.

      - Refer to Section 9 of this document for the definition of scoping guidance.

p. Compensating controls may only be employed for information systems provided they meet the following criteria:

   i. The compensating control must be selected from the NIST SP 800-53 (as amended) security control catalog.

   ii. A complete and convincing documented rationale must be provided for how the compensating control provides an equivalent security capability or level of protection.

   iii. An explanation must be provided why the control specified in the minimum security control baseline could not be employed.

   iv. The residual risk of implementing the compensating control in lieu of the control established in the minimum security control baseline must be accepted and approved by the AO.

q. Any additional or equivalent system-specific security controls that are required due to the unique mission objectives, federal regulations, statutory, and other requirements pertaining to the information or information system must be determined, referenced and documented in the SSP and in relevant acquisition documents.

   i. Controls, such as those specified in Government Accountability Office (GAO) publications, Joint Financial Management Improvement Program (JFMIP) requirements documents for financial systems, Federal Information System Controls Audit Manual (FISCAM), OMB Circular A-123, "Management's Responsibility for Internal Control," or other related sources, must be determined, implemented, maintained, and documented in the SSP and in relevant acquisition documents.

   ii. The required control that specifies more protection takes precedence over another offering lesser protection, when differing requirements are specified.

      - For example, a JFMIP control that is "mandatory" for a financial system must be implemented even if the NIST SP 800-53 (as amended) specified control is not required at that system categorization level. Contrarily, a NIST SP 800-53 (as amended) control that is required at a given system categorization level must be implemented even if the JFMIP requirements indicate that control is "optional."

r. If any section of the SSP becomes large enough to be a standalone document, the SO must summarize the important items in the document, reference the stand-alone document in the body of the SSP, and include it as an attachment to the SSP.
   i. For example, a Contingency Plan may become too large to include within the SSP and may be more appropriate as a standalone document that the SSP references.

s. The SSP must be reviewed and approved by the AO or designated representative prior to plan implementation.

t. If requested, the information system's SSP must be made available to the SO, ISSO, ISO, or managers of connected systems.
   i. The only sections of an SSP permitted to be made available to users of the information system are the rules of behavior, remote access requirements, or flexi-place requirements.
   ii. Otherwise, the SSP is considered sensitive and is prohibited from being released to unauthorized personnel.

u. The SSP must be periodically reviewed and maintained in close coordination with the ISSO and ISO for the information system.
   i. The SSP must be reviewed to address any system/organizational changes or problems identified during plan implementation, operations and maintenance, or subsequent to security control assessments.
   ii. The SSP must be reviewed, and updated (if appropriate), at least annually or when a significant change occurs to the information system's operating environment or security requirements.
      - The SSP must be updated when impacted by unforeseen significant events, such as a breach, a new threat, or previously unknown vulnerability.
      - Planned significant changes must be defined in advance and identified in the SSP as well as in the configuration management process.
      - A significant change includes a change in the points of contact, system architecture, system status, system interconnections, system scope, or C&A status.
      - The SSP must be updated to factor in planned information system enhancements, to ensure that required security-related activities are planned for in advance.
   iii. The SSP must be updated based on the results of the continuous monitoring process.
   iv. The document review history must be updated to reflect the date the review was performed.

v. Prior to information system retirement and disposal, the SSP must be reviewed to ensure the minimum security controls defined in the SSP remain in effect until the system has been fully retired and disposed.

i. Controls pertaining to disposal must be documented, from planning through implementation.

w. Appropriate individuals within the organization must remain cognizant of and fulfill their responsibilities to develop, review, and update SSPs.

x. The SSP must be signed and approved by a management official.

PL-4 – National Rules of Behavior

a. The National Rules of Behavior (NROB) must be established and readily available to all information system users.

b. The NROB must address and describe the user's responsibilities and expected behavior with regard to information and information system usage, and the consequences of non-compliance to security rules based on the type of information processed by the system.

c. The handling of Personally Identifiable Information (PII) and other EPA sensitive information must be fully addressed in the NROB, and be consistent with agency policy and procedures.

d. EPA shall ensure that NROB contain acknowledgement that the user has no expectation of privacy (a "Consent to Monitor" provision) and that disciplinary actions may result from violations.

e. The NROB must include general rules for all users and targeted rules for specific functions such as information system administration, developers, end users, etc.

f. The NROB must be distributed to and acknowledged in writing by all information system users.

   i. Signed acknowledgement from users indicating that they have read, understand, and agree to abide by the NROB must be received before they receive access to the information system.

   ii. Users must be trained on the NROB before they receive access to the information system.

g. A record that users receive and acknowledge receipt of the NROB must be maintained.

   i. This information must be maintained throughout the entire duration of each user's access.

h. The NROB must be reviewed annually or whenever a significant change to the information system occurs.

   i. If changes to the NROB are required, the revised document must be distributed and accepted by all information system users.

   ii. Records of NROB acknowledgement must be updated when the revised NROB are distributed.

i. Rules of Behavior may be developed for particular systems or applications as deemed necessary by IO's, SO's, or AO's to expand on the NROB to address particular situations or requirements not addressed by the NROB.

    i. System or application level ROBs shall be made available and acknowledged in writing as well as the NROB, both need to be signed by users and tracked.
    ii. A template for suggested ROB wording is provided in Appendix B. This is only suggested wording, not mandatory.

<u>PL-5 – Privacy Impact Assessment</u>

a. Requirements and procedures for conducting Privacy Threshold Analyses (PTAs) and PIAs are contained in EPA's privacy policies and procedures (CIO 2151).

b. The PTA or PIA must be conducted concurrently with information and system categorization to accurately reflect the system's categorization and resulting security control requirements.

c. The PTA or PIA must be reviewed annually in conjunction with the SSP and categorization reviews to ensure that any changes in the type of information collected or the information uses are assessed and the documentation is updated.

d. At a minimum, the PIA shall be reviewed and updated in the event of a significant change to the information system.

    i. The PTA must be revisited when significant changes occur in the type of information processed by the information system.

<u>PL-6 – Security-Related Activity Planning</u>

For moderate and high information systems

a. Security-related activities affecting the information system must be planned and coordinated before such activities are conducted in order to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals.

    i. Organizational planning and coordination must include both emergency and non-emergency (i.e., planned or non-urgent unplanned) situations.

Note: Security-related activities include, for example, security assessments, audits, system hardware and software maintenance, and contingency plan testing/exercises.

b. The SO shall identify and coordinate with the stakeholders and participants for each information system and security-related activity; these persons include, but are not limited to, the following:

    i. Business process owners
    ii. Users
    iii. Security personnel
    iv. Operations support personnel
    v. Appropriate personnel of connected systems

c. Security-related activities, either planned (e.g., SSP development or update, contingency plan test, risk assessments, C&A activities) or out-of-cycle (e.g., Inspector General (IG) audit), must:

    i. Take into account important processing cycles and other known events.

Alternative times must be identified.

ii. Be identified and reflected in, as appropriate, the applicable budget planning documents such as Exhibits 300 and 53.

- Refer to *Information Security – Interim System and Services Acquisition Procedures* for requirements on allocation of resources.
- More detailed plans must support the budget documents, identifying the support and resources needed as well as methods of communicating.
- A Plan of Action and Milestones (POA&M) must also be created, if needed.

7. RELATED DOCUMENTS

- NIST SP 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006
- NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009

8. ROLES AND RESPONSIBILITIES

Authorizing Official (AO)

a. The AO has the following responsibilities with respect to security planning:

i. Accept and approve the residual risk of implementing any compensating control in lieu of the control established in the minimum security control baseline.

ii. Review and approve the SSP.

iii. Review and approve the NROB as part of the SSP.

Senior Agency Information Security Officer (SAISO)

a. The SAISO has the following responsibilities with respect to security planning:

i. Review the SSP.

ii. Develop and maintain the NROB.

Information Management Officer (IMO)

a. The IMO has the following responsibilities with respect to security planning:

i. Review and approve the NROB as a part of the SSP.

ii. Ensure planning activities are accurately reflected in multi-year budgetary and planning documents and adequate resources are made available through the budgetary process.

iii. Ensure accurate relationships between information systems and Privacy Act System of Records are maintained and coordinated, are accurately identified in the SSP, and system categorization.

Information Owner (IO)

a. The IO has the following responsibilities with respect to security planning:

i. Provides procurement, development, integration, modification, operation, maintenance, and disposal of an information system.

ii. Provides operational interests of the user community (i.e., users who require access to the information system to satisfy mission, business, or operational requirements)

iii. Provides the development and maintenance of the security plan and ensures that the system is deployed and operated in accordance with the agreed-upon security controls.

iv. Responsible for deciding who has access to the system (and with what types of privileges or access rights) and ensures that system users and support personnel receive the requisite security training (e.g., instruction in rules of behavior)

v. Reviews security assessment results from the Security Control Assessor

Information System Management Staff

a. Information system management staff have the following responsibilities with respect to security planning:

i. Assist management in developing the SSP by identifying any shortcomings or needed improvements to security.

System Owner (SO)

b. The SO has the following responsibilities with respect to security planning:

i. Develop and approve the SSP.

ii. Ensure adequate funding and resources to carry out security planning requirements.

iii. Review the minimum baseline security controls required by the FIPS 199 categorization for the information system.

iv. Determine if additional system specific security controls are required due to the unique mission objectives, statutory requirements, and federal regulations pertaining to the system.

v. Implement the security controls.

vi. Revise the SSP to address any system/organizational, information, or privacy changes or problems identified during plan implementation or security control assessments.

vii. Review, and update if appropriate, the approved SSP at least annually or when a significant change to the information system's operating environment or security requirements.

viii. Update the SSP based on the results of the continuous monitoring process.

ix. Review the SSP prior to information system retirement and disposal to ensure controls remain in effect.

x. Document in the SSP controls pertaining to information system disposal.

xi. Plan and coordinate with stakeholders and participants security-related activities affecting the information system well in advance of conducting such activities.

xii. Train users on the NROB.

xiii. Distribute the NROB to all users.

xiv. Maintain records that users receive and acknowledge receipt of the NROB.

xv. Review the NROB annually or whenever a significant change to the information system occurs.

xvi. Develop, review, and update the PIA and PTA for the information system as applicable.

xvii. Ensure any Privacy Act System of Records supported by the information system is accurately identified in the SSP and system categorization.

Information Security Officer (ISO)

a. ISOs have the following responsibilities with respect to security planning:

i. Review and maintain the SSPs for the systems they manage or oversee.

ii. Conduct and participate in security-related planning activities and ensure they mesh appropriately with operational necessities.

iii. Identify the specific System(s) of Records supported by the information system, if appropriate, and document in the SSP and system categorization.

Information System Security Officer (ISSO)

a. The ISSO has the following responsibilities with respect to security planning:

i. Assist with developing the SSP.

ii. Ensure that SSPs adequately address federal and Agency requirements.

iii. Review and assist in maintaining the SSPs for the systems they oversee.

Users / Individuals

a. Users/individuals have the following responsibilities with respect to security planning:

i. Assist management in developing the SSP by identifying any shortcomings or needed improvements to security.

i. Provide signed acknowledgement that they have read, understand, and agree to abide by the NROB.

ii. Provide signed acknowledgement that they have read, understand, and agree to abide by the system or application level ROB.

9. DEFINITIONS

- Availability – ensuring timely and reliable access to and use of information.
- Certification – a comprehensive assessment of the management, operational and

technical security controls in an information system made in support of security accreditation to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

- Compensating Control – a management, operational, or technical control employed by an information system in lieu of a recommended security control in the low, moderate, or high baselines described in NIST SP 800-53 (as amended), which provides equivalent or comparable protection for an information system.
- Confidentiality – preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.
- General Support System (GSS) – an interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people.
- Information – an instance of an information type.
- Information Security – the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
- Information System – a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
- Information Technology (IT) – any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that (i) requires the use of such equipment or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term Information Technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.
- Integrity – guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity.
- Major Application (MA) – 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. However, certain applications, because of the information they contain, 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.
- Organization – a federal agency or, as appropriate, any of its operational elements.
- Privacy Impact Assessment (PIA) – an analysis of how information is handled (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements

regarding privacy; (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

- Scoping Guidance – provides organizations with specific policy/regulatory-related, technology-related, physical infrastructure-related, operational/environmental-related, public access-related, scalability-related, common security control-related, and security objective-related considerations on the applicability and implementation of individual security controls in the control baseline.
- Security Requirements – requirements levied on an information system that are derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, procedures, or organizational mission/business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.
- Signature (of an individual) – a mark or sign made by an individual to signify knowledge, approval, acceptance, or obligation (can be accomplished manually, sometimes referred to as a “wet signature,” or electronically).
- Significant Change – a modification that impacts the operating environment, functional design, operation, or protective controls required for a system. Changes in user audiences, owning organization, public access, and communication methods are considered significant changes. Other examples of a significant change include, but are not limited to a change in criticality and/or sensitivity level that causes a change in the controls or countermeasures required; a change in the security policy; a change in the threat of system risk; a change in the activity that requires a different mode of operation; additions or a change to the operating system or to software providing security features; additions or a change to the hardware that requires a change in the approved security countermeasures; a breach of security, a breach of system integrity, or an unusual situation that appears to; a significant change to the physical structure of the facility or to the operating procedures; a move to another location; and a significant change to the configuration of the system.
- System Security Plan (SSP) – a formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.
- User – individual or (system) process authorized to access an information system.
- Written – or “in writing” means to officially document the action or decision and includes a signature. The documentation can be accomplished manually or electronically.

10. WAIVERS

Waivers may be requested from the CIO by submitting a justification based on:

- substantive business case need(s)
- demonstration of, or a proposal for, establishment of adequate compensating

controls that provide a suitable alternative to the mandated protection

The CIO may grant a waiver for sufficient reasons exercising judgment in the best interests of the Agency.

The SAISO and Director, OTOP shall coordinate to maintain central repository of all waivers.

11. RELATED POLICY, PROCEDURES, STANDARDS AND GUIDELINES

Related policy and procedures are available on OEI's Policy Resources website.
http://intranet.epa.gov/oei/imitpolicy/policies.htm
Related standards and guidelines are available on OEI's website.

12. MATERIAL SUPERSEDED

EPA Information Security Manual, Directive 2195A1, 1999 Edition, Sections 2.6.1, and 13.0

13. ADDITIONAL INFORMATION

NA

Malcolm D. Jackson
Assistant Administrator and Chief Information Officer
Office of Environmental Information

APPENDIX A: ACRONYMS

AO	Authorizing Official
C&A	Certification and Accreditation
CIO	Chief Information Officer
EPA	Environmental Protection Agency
FIPS	Federal Information Processing Standards
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Management Act
GAO	Government Accountability Office
GSS	General Support System
IG	Inspector General
ISA	Interconnection Security Agreement
ISO	Information Security Officer
ISSO	Information System Security Officer
IT	Information Technology
JFMIP	Joint Financial Management Improvement Program
MA	Major Application
MOU/A	Memorandum of Understanding or Agreement
NROB	National Rules of Behavior
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
POA&M	Plan of Action and Milestones
PTA	Privacy Threshold Analyses
SAISO	Senior Agency Information Security Officer
SIO	Senior Information Official
SO	System Owner
SP	Special Publication
SSP	System Security Plan
USC	United States Code

APPENDIX B: RULES OF BEHAVIOR TEMPLATE

The following verbiage is provided for use for information system's baseline ROB. This ROB must also be customized to meet the needs and specific requirements of the disparate information systems. Attach a copy of the rules of behavior to the SSP as an appendix.

As a user of the **{System Name}**, I understand that I am personally responsible for my use and any misuse of my user account and password. I understand that by accessing a U.S. Government information system that I must comply with the following requirements:

1. Users must safeguard the information to which they have access at all times.

2. The information system is a government system and intended for authorized use only.

3. The information system may not be used for commercial purposes, for financial gain, or in support of "for profit" non-government activities.

4. The government reserves the right to monitor the activities of any user and/or any machine connected to {System Name}.

5. The {System Name} and the information contained within are the property of the federal government. EPA owns the data stored on these systems, including all messages and information, even those deemed personal.

6. No data may be transmitted on the system that is more sensitive than the level for which that information system has been approved.

7. Information that was obtained via {System Name} may not be divulged outside of government channels without the express, written permission of the System Owner.

8. Any activity that would discredit the Agency, including, but not limited to, seeking, transmitting, collecting, or storing defamatory, discriminatory, sexually explicit, obscene, harassing, or intimidating messages or material, is prohibited.

9. Any activity that violates federal laws for information protection (e.g., hacking, phishing, spamming) is prohibited. Violations will be turned over to the appropriate federal law enforcement organization for prosecution.

10. {System Name} user accounts are provided solely for the use of the individual for whom they were created. Passwords or any other authentication mechanism must never be shared or stored any place easily accessible by any other than the authorized individual. If stored, a password must not be in a clear-text or readable format. Sharing of user accounts may be grounds for terminating system access.

11. Passwords must adhere to the following requirements: [insert system password requirements or the standards found in Information Security – Interim Identification and Authentication Procedures as a minimum].

12. Authorized users do not have a right, nor should they have an expectation, of privacy while using any government office equipment at any time except as required pursuant to information or an information system covered by the Privacy Act of 1974.

13. At no time should non-government furnished equipment (e.g., personally-owned equipment) be connected to the system without prior authorization.

14. Auto-forwarding or redirecting of EPA email outside of the .gov domain is prohibited and shall not be used. An automatic forward may not be placed on an EPA mailbox to send to a personal or non-EPA business email account. Users may manually forward individual messages after determining that the risk or consequences are low.

    - When sending email to an address outside of the .gov domain, users shall ensure that any sensitive information, particularly PII, is appropriately protected, i.e., encrypted.

15. Any security problems or password compromises must be reported immediately to the Information Security Officer and EPA Call Center.

16. I understand that federal law provides for punishment under Title 18, U.S. Code, including a fine and up to 10 years in jail for the first offense for anyone who commits any of the following violations:

    - Knowingly accesses an information system without authorization, or exceeds authorized access, and obtains information that requires protection against unauthorized disclosure.
    - Intentionally, without authorization, accesses a government information system and impacts the government’s operation, including availability of that system.
    - Intentionally accesses a government information system without authorization, and alters, damages, or destroys information therein.
    - Prevents authorized use of the system or accesses a government information system without authorization, or exceeds authorized access, and obtains anything of value.

17. When the user no longer has a legitimate need to access the system, the user must notify the System Owner immediately so that access can be terminated.

18. Any suspected loss of confidentially sensitive information, including personally identifiable information, must be reported to the EPA Call Center and the information security officer within one hour of discovery.

DOCUMENT CHANGE HISTORY

Version	Release Date	Summary of Changes	Author of Changes	DCN
0.6	1/8/09	Initial draft	Heather Flager	Procedures-PL-Draft_TO62_020_1
1.4	3/26/09	Incorporated EPA comments, incorporated metrics	Heather Flager	Procedures-PL-Final_TO62_020_2
2.0	4/20/09	Incorporated EPA comments	Heather Flager	Procedures-PL-Final_TO62_020_3
3.3	5/24/10	Updated per NIST SP 800-53 Rev 3	Heather Flager	Procedures_PL_Draft.TO-062_050_1.0
3.4	7/15/10	TISS Final Draft Review	Charleen Johnson	Procedures_PL_Draft.TO-062_050_1.0
3.5	5/4/12	SAISO Final Review	Abe Getchell	Procedures_PL_Draft.TO-062_050_1.0
3.6	7/17/12	Document Review	LaToya Gordon	Procedures_PL_Draft.TO-062_-52_1.0