EPA INFORMATION PROCEDURES

OFFICE OF ENVIRONMENTAL INFORMATION

EPA Classification No.:	CIO-2150.3-P-04.1	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 SECURITY ASSESSMENT AND AUTHORIZATION PROCEDURES

V2

JULY 16, 2012

1. PURPOSE

The purpose of this procedure is to facilitate the implementation of Environmental Protection Agency (EPA) security control requirements for the Security Assessment and Authorization 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 security assessment and authorization 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-02-01, "*Guidance for Preparing and Submitting Security Plans of Action and Milestones*," October 2001
- OMB Circular A-130, "*Management of Federal Information Resources,*" Appendix III, "*Security of Federal Automated 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

CA-2 – Security Assessments

a. A Security Assessment Plan that describes the scope of the assessment must be developed to include:

   i. The security controls and control enhancements under assessment.

   ii. The assessment procedures to be used to determine security control effectiveness.

   iii. The assessment environment, assessment team, and assessment roles and responsibilities.

b. At least one third of all security controls (including selected core controls) employed in the information system must be assessed annually during continuous monitoring to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome to meet the security requirements for the system. The controls subject to annual assessment are defined as "core controls."

   i. EPA shall publish the list of agency core controls.

   ii. System core controls may be defined for individual systems.

c. Criteria for the selection of core controls must take into account the following:
   i. Volatility of controls (i.e., controls most affected by ongoing changes to the information system or its environment of operation).
   ii. Criticality of the controls as deemed so by the Agency to protect agency operations and assets, individuals, other organizations, and the nation.

d. The security controls of an information system must be assessed as part of:
   i. Security authorization and reauthorization.
   ii. Meeting the FISMA requirement for annual assessments.
   iii. Continuous monitoring.
   iv. Testing/evaluation of the information system as part of the system development life cycle process.

e. A Security Assessment Report (SAR) must be developed to document the results of the assessment.
   i. The SAR must document results in sufficient detail as deemed necessary by EPA to determine:
      - The accuracy and completeness of the report.
      - Whether the controls are implemented correctly, operating as intended, and producing the desired outcome to meet the security requirements for the system.
   ii. The SAR must be updated whenever changes are made to:
      - Security controls in the information system.
      - Common controls inherited by those systems.
   iii. Updates to the SAR must be performed to ensure that the System Owner (SO) and the Authorizing Official (AO) maintain situational awareness with regard to security control effectiveness.
      - Security control effectiveness directly affects:
        - Risk mitigation activities and ultimately the security state of the information system.
        - Explicit acceptance of risk through the authorization decision and authorization to operate.

f. The results of the security control assessment must be provided, in writing, to the AO or AO designated representative.

g. Existing security assessments must still be valid and supplemented with additional assessments as needed to meet the requirement for assessing core controls annually.

h. Existing security assessment results to satisfy FISMA annual assessment requirements can be obtained from:
   i. Security assessments conducted as part of an information system authorization or reauthorization process.
   ii. Continuous monitoring activities.
   iii. Testing and evaluations of information systems conducted as part of:

- Life cycle requirements and activities.
- Application deployment requirements.
- Compliance oversight activities including vulnerability assessments and independent verification and validations.
- Assessments or tests conducted when a significant change occurs.
- Audits and/or evaluations conducted by the Inspector General (IG) or General Accountability Office (GAO).

Note: Security assessments can be used to satisfy the FISMA requirement that controls be assessed annually provided the results are current, valid, and relevant to determining security control effectiveness.

i. All security controls in the information system must be assessed at least once during the three-year authorization cycle.

j. Security control assessments must adhere to the following steps:

   i. Determine, identify, and verify information system boundaries.

   ii. Determine and understand security control inheritance from related information systems.

   iii. Prepare for the assessment by gathering documentation and supporting materials. Relevant documents and supporting materials must include, but are not limited to:

      - System Security Plan (SSP)
      - Memorandum of Understanding/Agreement (MOU/As) and Interconnection Security Agreements (ISAs)
      - Service Level Agreements (SLAs)
      - System Categorization
      - Plan of Action and Milestones (POA&Ms)
      - Contingency Plan
      - Relevant and valid test results, assessments, continuous monitoring results, audits and reviews.

   iv. Select appropriate assessment methodologies and procedures for each control.

   v. Assess each control by performing document reviews, interviews, and information system testing in accordance with selected methodologies and procedures.

   vi. Prepare the SAR, which documents the following:

      - Assessment results, i.e., the determination of the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the specified security requirements.
      - Recommendations for correcting deficiencies and reducing or eliminating vulnerabilities.

k. When planning and budgeting for security assessments, the following must be adhered to:

   i. Multi-year planning and budgeting techniques must be used.

   ii. Annual FISMA assessments must be included in information system budgets and planning.

   iii. Other significant, planned activities must be considered in budgets and planning (e.g., life cycle activities, enhancements, audits, risk assessments) to ensure cost effective use of resources.

   iv. All information systems in an organization must be considered to ensure resource efficiencies.

   v. Assessments must be coordinated between information systems with control inheritance and other relational dependencies.

   - Many information systems inherit controls from one or more General Support Systems (GSSs).
   - Other relational dependencies to consider include interrelated systems.

l. When the potential impact on agency operations, agency assets, individuals, other organizations, and the nation is low (e.g., low FIPS 199 security categorization), a self-assessment activity is acceptable and a cost-effective mechanism to fulfill the security assessment requirement.

m. NIST SP 800-37, Revision 1 must be used as guidance for the security assessment and authorization process.

n. NIST SP 800-53A, Revision 1 must be used as guidance for security control assessments.

o. NIST SP 800-115 must be used as guidance for conducting security assessments.

For moderate and high information systems

p. An independent assessor or assessment team shall conduct an assessment of the security controls in the information system.

Note: Refer to Section 9 for definitions on independent assessor/assessment team and impartiality.

Note: Independent security assessment services can be obtained from other elements within the organization or can be contracted to a public or private sector entity outside of the organization. Contracted assessment services are considered independent if the SO is not directly involved in the contracting process or cannot unduly influence the impartiality of the assessor or assessment team conducting the assessment of the security controls in the information system.

q. Selection of an assessor must ensure that the SO and AO can rely on the security expertise and technical judgment of the assessor to:

   i. Assess the system-specific security controls and common controls inherited by information systems using assessment procedures specified in the security assessment plan.

ii. Provide specific, unbiased recommendations on how to:
    - Correct weaknesses or deficiencies in the controls.
    - Address identified vulnerabilities.

r. When assessments must be conducted by an entity with an explicitly determined degree of independence to the organization, independence must be determined by the AO based on the security categorization of the information system and/or the risk to Agency operations and assets, and to individuals.

   i. To make an informed, risk-based decision, the selection of independent assessors must consider the following criteria to ensure credibility of the security assessment results and to receive the most objective information possible:
      - Preserving the impartial and unbiased nature of the assessment process including, but not limited to, freedom from any perceived or actual conflicts of interest with respect to:
        - The development, operation, and/or management of the information system.
        - The chain of command associated with the information system.
        - The determination of security control effectiveness.
        - A competitive relationship with any organization associated with the information system being assessed or impacts on their reputations.
        - Possibility or appearance of a *quid pro quo* situation or relationship.
        - Undue influence as a result of a contractual or other related relationship.
        - The assessor’s technical expertise and knowledge of federal requirements.

For high information systems

s. Security control assessments must include, annual, announced, and/or unannounced, in-depth monitoring; malicious user testing; penetration testing; red team exercises; and EPA or other federally defined forms of security testing.

Note: A standard method for penetration testing consists of (i) pretest analysis based on full knowledge of the target system, (ii) pretest identification of potential vulnerabilities based on pretest analysis, and (iii) testing designed to determine exploitability of identified vulnerabilities.

t. Information system monitoring, malicious user testing, penetration testing, red-team exercises, and/or other forms of security testing (e.g., independent verification and validation) must be conducted to improve the readiness of the organization by exercising organizational capabilities and indicating current performance levels as a means of focusing organizational actions to improve the security state of the system and organization.

u. Detailed rules of engagement must be agreed upon by all parties before the commencement of any penetration testing scenario.
   i. These rules of engagement must be correlated with the tools, techniques, and procedures that are anticipated to be employed by threat sources in carrying out attacks.

v. An organizational assessment of risk must guide the decision on the level of independence required for penetration agents or penetration teams conducting penetration testing.

w. Red team exercises must be conducted as a simulated adversarial attempt to compromise organizational missions and/or business processes to provide a comprehensive assessment of the security capability of the information system and organization.
   i. Vulnerabilities uncovered during red team exercises must be incorporated into the vulnerability remediation process.

Note: While penetration testing may be laboratory-based testing, red team exercises are intended to be more comprehensive in nature and reflect real-world conditions.

x. Testing must be conducted in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

y. Testing methods must be approved by AOs in coordination with the organization’s Risk Executive Function.

CA-3 – Information System Connections

Note: This control applies to dedicated connections between information systems and does not apply to transitory, user-controlled connections such as email and website browsing.

a. Connections from the information system to other information systems outside of the authorization boundary must be authorized through the use of ISAs.
   i. For connections to systems outside of EPA, an Interagency Agreement must accompany the ISA.
   ii. If the connecting systems have the same AO, an ISA is not required. Rather, the interface characteristics between the connecting information systems must be described in the SSPs for the respective systems.
   iii. If the connecting systems have different AOs but the AOs are in the same organization, EPA shall determine whether an ISA is required, or, alternatively, the interface characteristics between the connecting information systems must be described in the SSPs for the respective systems.

Note: Instead of developing an ISA, organizations may choose to incorporate this information into a formal contract, especially if the connection is to be established between a federal agency and a nonfederal (i.e., private sector) organization. In every case, documenting the interface characteristics is required, yet the formality and *approval process vary considerably even though all accomplish the same fundamental objective of managing the risk being incurred by the connection of the information systems.*

b. To establish a connection, the following activities must be adhered to:

i. Define the business case.

ii. Establish a joint planning team to examine all relevant technical, security, and administrative issues.

- Risks that may be introduced when information systems are connected to other systems with different security requirements and security controls must be carefully considered.
- The AO shall determine the risk associated with each connection and the appropriate controls to be employed.

iii. Ensure all systems to be interconnected have or will have a current Authorization to Operate (ATO) prior to establishing the interconnection.

- The aforementioned may require re-assessment and re-authorization of the information system.

iv. Plan for termination of connections.

- Document requirements for emergency disconnections when developing any interconnection agreement.
- Plan for and develop requirements and procedures for reconnection, as appropriate.

v. Document the management requirements in the MOU/A by addressing the following:

- Contact information and topics requiring formal communication between the parties.
- Procedures and requirements for termination of agreements.

vi. Document the technical requirements in the ISA by addressing the following:

- Roles and responsibilities for each party.
- Interface characteristics.
- Security requirements.
- Nature of the information communicated.

vii. Approve or reject the interconnections.

- Obtain approval signatures of the SO, AO, and other officials as may be required by EPA for the specific type of agreement.
- Interim approval is an option, but it requires enumeration and documentation of terms, conditions, and expiration for the interim approval.

viii. Upon execution of an MOU/A, all parties must update their SSPs, Risk Assessments, Incident Response Plans, and Contingency Plans to reflect any major changes to their systems, including exposure to outside threats and vulnerabilities arising as a result of the MOU/A.

- The interconnection must be fully documented in the SSP according to the current Agency standard template format.

ix. Signed copies of the MOU/A and the ISA must be attached to all relevant security documentation.

c. For information systems housed at EPA's National Computer Center (NCC) or interconnections that impact the EPA network, the following requirements must apply as part of setting up an interconnection agreement between an EPA information system and a non-EPA information system:

i. A request for connection to the Director of NCC must be submitted in order to establish such a connection. The request must include the following:

- Type of connection to be established
- Business purpose for the connection
- Connection requirements and controls in place
- Key personnel to help coordinate the planning efforts of the system interconnection
- Duration of the interconnection
- Point of contact for the external organization requesting the interconnection

ii. NCC shall review the request and send a copy of the rejection or acceptance letter to the SO, the Senior Information Official (SIO), and the point of contact for the external organization requesting to connect.

d. Information system documentation must be made available to the system personnel of the connected system should they want to review it.

i. System personnel requesting access to EPA's information system documentation must review it on site at an EPA facility.

e. The agreement documentation must be reviewed and updated annually, in order to reaffirm that all security requirements are still being met and that no changes to the connection have occurred.

i. The annual review can be done as part of the annual FISMA assessment.

ii. The SSP and other security documents must also be reviewed to ensure that they accurately reflect the status of each interconnection.

f. The information system interconnections must be monitored and tested on an ongoing basis verifying enforcement of security requirements.

g. ISAs shall be reissued every three years or whenever any significant changes have been made to any of the interconnected systems.

h. ISAs shall be reviewed and updated as needed annually.

i. System interconnections must be terminated under the following conditions:

i. An ATO expires or is withdrawn.

ii. The MOU/A and/or the ISA expire or are withdrawn.

iii. The business case no longer requires the system connection.

j. The NCC must be notified in writing of the decision to terminate the system interconnection, whether the interconnection is in place or previously planned.

i. The NCC must also be notified in writing of the decision to restore any system interconnection that was terminated.

k. Upon terminating and disconnecting any interconnection, relevant security controls must be assessed or re-assessed (e.g., access authorizations, physical connections).

l. Upon terminating any interconnection, the appropriate security documentation supporting the security authorization must be updated:

i. SSP

- Refer to *Information Security – Interim Security Planning Procedures f*or guidance on updating the SSP.

ii. Risk Assessment

- Refer to *Information Security – Interim Risk Assessment Procedures* for guidance on updating the Risk Assessment.

iii. Contingency Plan

- Refer to *Information Security – Interim Contingency Planning Procedures* for guidance on updating the Contingency Plan.

iv. Incident Response Plan

- Refer to *Information Security – Interim Incident Response Procedures* for guidance on updating the Incident Response Plan.

m. NIST SP 800-47 must be used as guidance for connecting information systems.

<u>CA-5 – Plan of Action and Milestones</u>

a. A POA&M for the information system documenting the planned, remedial actions to correct weaknesses or deficiencies in security controls and to reduce or eliminate known vulnerabilities must be developed.

b. The existing POA&M must be updated weekly based on findings of weaknesses including, but not limited to, the following:

i. Reviews, tests, audits, or assessments

ii. Security impact analyses

iii. Independent verification and validation findings

iv. Continuous monitoring activities

v. Incidents.

c. All findings, recommendations, and their source must be tracked to the related item in the POA&M.

d. Findings must be analyzed as to their level of risk (i.e., high, medium, low) and a determination must be made for appropriate action(s) to be taken to correct or mitigate, as appropriate, the identified weaknesses to an acceptable level of risk.

e. One or more tasks to remediate a finding must be documented in the POA&M for any:

i. High-level risks that are not corrected within 30 days

ii. Medium-level risks that are not corrected within 60 days

iii. Low level risks as required by the AO

f. The status of all findings and recommendations must be documented regardless of whether or not a remediation task is created.

   i. Document the AO’s risk-based decision(s) to accept the weakness.

   ii. Document any weakness covered in an existing POA&M.

g. All findings must be entered into the Agency’s FISMA reporting and tracking tool.

   i. EPA shall rely on the Agency’s FISMA reporting and tracking tool to meet oversight reporting requirements to OMB and Congress.

Note: The plan of action and milestones is a key document in the security authorization package and is subject to federal reporting requirements established by OMB. OMB’s annual FISMA reporting guidance contains instructions regarding POA&Ms.

h. All OMB-reportable tasks in the Agency’s FISMA reporting and tracking tool must have one or more milestones and each milestone must have a baseline start date and a baseline completion date.

   i. The start date and completion date may be revised, but the baseline dates must never be changed.

   ii. Any revision to the completion date must include documented justification for the schedule change.

i. All waiver requests shall identify the POA&M for bringing the system or program into compliance.

j. Any task in the POA&M that has been reported to OMB but will not be completed must be closed administratively.

   i. The reason for administratively closing a task must be justified and documented.

   ii. Tasks reported to OMB cannot be deleted from the Agency’s FISMA reporting and tracking tool.

k. The information system’s POA&M data must be reviewed at least monthly to ensure that there is an accurate record of all planned, implemented, and evaluated remedial actions to correct or reduce any deficiencies.

   i. The SO may delegate responsibility for the review of tasks and milestones and the mitigation of weaknesses to key personnel.

   ii. Final responsibility for the POA&M must remain with the SO.

l. POA&M data must also be reviewed quarterly with respect to the risk management strategy for the information system, thereby providing the opportunity to identify recommendations for improvement or issues that need to be addressed.

   i. Personnel participating in the quarterly review include, as appropriate, the Information Security Officer (ISO), the SO, the Information System Security Officer (ISSO), the Agency’s FISMA reporting and tracking tool point of contact, the Information Management Officer (IMO) and the SIO.

m. The information system’s POA&M must be included in the security authorization package.

n. Requests submitted without sufficient information shall be returned for clarification prior to making a decision.

<u>CA-6 – Security Authorization</u>

a. Information systems must receive an ATO before commencing operations.

   i. Per OMB policy, the security authorization must be updated at least every three years or when there is a significant change to the information system.

   - Refer to *Information Security – Interim Risk Assessment Procedures* for guidance on what constitutes a significant change.

b. The AO shall determine if risks are acceptable and the information system is authorized to operate.

   i. The AO documents the security authorization decision in an authorization decision document. The decision will result in

   - an authorization to operate (ATO) signed by the AO if residual risks are acceptable, or
   - a denial of authorization to operate signed by the AO if residual risks are unacceptable.

c. An AO for each information system must be identified and documented.

   i. The SSP must identify the AO and provide full information, including title and contact information.

   ii. When mission or risk accountability for an information system spans EPA organizational boundaries (e.g., region, program, or agency), clear and enforceable documentation detailing responsibilities and accountability must be established.

   - Documentation includes, but is not limited to, an information system charter, MOU/A, etc.

Note: OMB Circular A-130, Appendix III, establishes policy for security authorizations of federal information systems.

d. The following authorization process must be followed:

   i. The security authorization package, consisting of the updated SSP, the SAR, and the POA&M, must be delivered to the AO for review. The ISO and the AO's designated representative (AODR), if assigned, shall present the package, detail risks, and provide authorization recommendations to the AO.

   - The security authorization package provides the AO with essential information to make a credible, informed, risk-based decision on whether to allow the system to operate or not.
   - The ISO and AODR support the AO in reviewing and understanding controls implemented, testing results, residual risks to the system and information and risks to operations and other systems and information.

   ii. The AO shall decide whether risks are acceptable.

   iii. The AO documents the authorization decision and associated risks and signs a statement acknowledging accountability and the authorization decision. The AO may add any additional requirements deemed necessary for security.

iv. The final authorization package, including the authorization decision document and any additional AO determined security requirements, must be returned to the SO.

v. All documents and information shall be entered into the Agency FISMA reporting and tracking tool.

e. The decision to deny or authorize operation of an information system must be documented in the authorization decision document and must include the following:

i. Authorization decision

ii. Terms and conditions to limit or restrict operations, as appropriate

iii. An authorization termination date

iv. Risk executive function input (if provided)

f. The decision to deny an ATO must be documented in the authorization decision document and based on the following:

i. Rationale for not accepting the risks

ii. Required corrective actions, if applicable

g. For short term authorizations either to test or operate the CIO and Senior Agency Information Security Official (SAISO) must be notified in writing, which may be accomplished through the Agency FISMA reporting and tracking tool, the authorization decision with any terms and conditions that place limitations or restrictions on the operation of the information system. The following must be addressed:

i. A defined, short period of time for testing or operations

- The duration established for an ATO must be commensurate with the risk to agency operations, agency assets, or individuals associated with the operation of the information system not to exceed one year.
- The information system must be authorized to operate, testing completed or halted, or taken out of operations by the end of the one year period.

ii. Tasks in the POA&M to address identified weakness in the information system resulting from deficiencies in the planned or implemented security controls.

iii. The specific terms and conditions established by the AO that convey limitations on the information system's use and acknowledge greater risk to the Agency for a specified period of time.

h. The authorization status of information systems must be monitored by the SAISO and reported periodically to the SIO.

i. Within 30 days before the ATO expires, the SIO and SO must be notified by the SAISO that a disconnection from the network will be recommended for non-compliance.

ii. Within two weeks before the ATO expires, a disconnection notice must be developed and submitted by the SAISO to the CIO for signature.

i. The SO shall update and maintain the authorization package including SSP, SAR, POA&M, and Contingency Plan for each information system.

j. Security reauthorization must occur in accordance with federal and agency policy or at the discretion of the AO.

    i. To reduce the administrative cost of security reauthorization, the AO shall use the results of the continuous monitoring process to the maximum extent possible as the basis for rendering a reauthorization decision.

    ii. The following questions must be answered when reinitiating the security authorization process:

        - Have any changes to the information system affected the security controls in the system or introduced new vulnerabilities into the system?
        - If so, has the agency-level risk (i.e., the risk to agency operations, agency assets, or individuals) been affected?
        - Has a specified time period passed requiring the information system to be reauthorized in accordance with federal or agency policy?

    iii. Security controls assessment and reauthorization are required when there is a significant change in risk or risk exposure.

    iv. Security controls assessment and reauthorization must be completed prior to the expiration of the existing ATO.

        - The time period for reauthorization must be calculated from the date the information system receives its ATO.

k. NIST SP 800-37, Revision 1 must be used as guidance on security assessment and authorization.

<u>CA-7 – Continuous Monitoring</u>

a. A continuous monitoring strategy must be established.

b. A continuous monitoring program must be implemented that includes the following:

    i. A configuration management process for the information system and its constituent components.

    ii. A determination of the security impact of changes to the information system and environment of operation. The security state of the information system shall be assessed as the result of events that affect residual risks or indicate controls may not be adequate.

        1. These events include but are not limited to the following:

            a. An incident that results in a breach to the information system, producing a loss of confidence by the organization in the confidentiality, integrity, or availability of information processed, stored, or transmitted by the system;

            b. A newly identified, credible, information system-related threat to organizational operations and assets, individuals, other organizations, or the Nation is identified based on intelligence information, law enforcement information, or other credible sources of information;

c. Significant changes to the configuration of the information system through the removal or addition of new or upgraded hardware, software, or firmware or changes in the operational environment potentially degrade the security state of the system; or

d. Significant changes to the organizational risk management strategy, information security policy, supported missions and/or business functions, or information being processed, stored, or transmitted by the information system.

2. Actions required for assessing the information system's security state:

a. The SO and IO shall reconfirm the security category and impact level of the information system.

b. The SO shall assess the current security state of the information system and the risk to organizational operations and assets, individuals, other organizations, and the Nation.

i. The SO shall investigate the information system vulnerability (or vulnerabilities) exploited by the threat source (or potentially exploitable by a threat source) and the security controls currently implemented within the system as described in the security plan.

c. The SO shall plan for and initiate any necessary corrective actions based on the results of an updated risk assessment.

d. The AO shall determine and document if reauthorizing of the information system is required based on the severity of the event, the adverse impact on organizational operations and assets, individuals, other organizations, and the Nation, and the extent of the corrective actions required to fix the identified weaknesses or deficiencies in the information system.

iii. Ongoing security control assessments in accordance with EPA's continuous monitoring strategy.

iv. Monthly, quarterly, and annual reports on the security state of the information system to will be made available to the SIO in accordance with continuous monitoring strategic and implementation plans.

- The SIO will review monthly, quarterly, and annual reports as provided and ensure corrective actions are implemented accordingly.

Note: A continuous monitoring program allows an organization to maintain the security authorization of an information system over time in a highly dynamic environment of operation with changing threats, vulnerabilities, technologies, and mission/business processes.

Note: Continuous monitoring of security controls using automated support tools *facilitates near real-time risk management and promotes organizational situational awareness with regard to the security state of the information system.*

c. The implementation of a continuous monitoring program must result in ongoing updates to the SSP, SAR, and POA&M.

d. Continuous monitoring activities must be scaled in accordance with the security categorization of the information system.

Note: A rigorous and well executed continuous monitoring program significantly reduces the level of effort required for the reauthorization of the information system.

e. NIST SP 800-53A, Revision 1 must be used as guidance on security control assessments.

f. NIST SP 800-37, Revision 1 must be used as guidance on security authorization and continuous monitoring.

For moderate and high information systems

g. An independent assessor or assessment team must be employed to monitor the security controls in the information system on an ongoing basis.

7. RELATED DOCUMENTS

- NIST SP 800-30*, Risk Management Guide for Information Technology Systems,* July 2002
- NIST SP 800-37, Revision 1*, Guide for Applying the Risk Management Framework to Federal Information Systems,* July 2010
- NIST SP 800-47*, Security Guide for Interconnecting Information Technology Systems,* August 2002
- NIST SP 800-53, Revision 3*, Recommended Security Controls for Federal Information Systems and Organizations,* August 2009
- NIST SP 800-53A, Revision 1*, Guide for Assessing the Security Controls in Federal Information Systems and Organizations,* June 2010
- NIST SP 800-115*, Technical Guide to Information Security Testing and Assessment,* September 2008

8. ROLES AND RESPONSIBILITIES

Senior Information Official (SIO)

a. The SIO has the following responsibilities with respect to security assessment and authorization:

   i. Authorizing Official.

   ii. Attend and receive briefings on the information system within his organization and provides input into POA&Ms.

   iii. Assist in acquiring funding and resources to address POA&Ms.

   iv. May assign a designated representative to perform AO functions, with the exception of accepting risk and signing authorization decision documents.

Authorizing Official (AO)

b. The AO is the accountable official for information system authorization (i.e., ATO) and has the following responsibilities with respect to security assessment and authorization:
   i. Decide on the required level of assessor independence based on the criticality and sensitivity of the information system and the ultimate risk to EPA operations and EPA's assets and to individuals in accordance with criteria in this procedure.
   ii. Determine if the level of assessor independence is sufficient to provide confidence that the assessment results produced are sound and can be used to make a credible, risk-based decision.
   iii. Consult with the OIG, the CIO, SAISO, and Risk Executive Function to fully discuss the implications of any decisions on assessor independence in the types of special circumstances as aforementioned.
   iv. Review the security authorization package and issue an authorization decision document.
   v. Use the results of the continuous monitoring process as input into the reauthorization decision.
   vi. Ensure ATOs for systems remain current and in compliance.
   vii. Approve the SSP.
   viii. Determine the risk associated with each information system connection and the appropriate controls employed.

Senior Agency Information Security Officer (SAISO)

c. The SAISO has the following responsibilities with respect to security assessment and authorization:
   i. Provide oversight to the Agency's security assessment and authorization process and status.
   ii. Notify SIO, IMO, ISO, SO, and ISSO of compliance issues.
   iii. Prepare disconnection notices for non-compliant information systems.
   iv. Determine and publish core controls in consultation with appropriate officials.

System Owner (SO)

d. The SO has the following responsibilities with respect to security assessment and authorization:
   i. Conduct an assessment of the security controls in the information system annually to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome to meet the security requirements for the system.
   ii. Provide the results of the security control assessment to the AO, in writing.
   iii. Assess all of the security controls in the information system during the initial

security authorization and within the three-year authorization cycle for re-authorization.

iv. Conduct penetration testing and auditing as required to ensure compliance with all EPA security requirements.

v. To establish a connection to an EPA or a non-EPA information system, submit a request to the NCC director.

vi. Review and update the ISA or MOU/A annually to reaffirm that all security requirements are still being met and that no changes to the connection have occurred.

vii. Notify the NCC in writing of the decision to terminate the system interconnection that was previously planned and/or restoration of the connection that was terminated.

viii. Ensure that the security assessment is conducted in support of OMB Circular A-130, Appendix III and NIST requirements for authorizing the information system.

ix. Develop POA&Ms and maintain and update the POA&Ms at least monthly to ensure that the system has an accurate record of all planned, in progress, and completed remedial actions to correct or reduce any deficiencies.

x. Ensure that actions to address weaknesses are created, tracked and managed as part of the system's POA&M and that they are:

1. prioritized and assessed for risk correctly
2. supported by documentation in writing, approved at the appropriate level, and retained for later audits and reviews
3. created in the Agency's FISMA reporting and tracking tool to for all weaknesses and actions in the POA&M
4. reviewed to ensure that they are in compliance with federal and Agency requirements

xi. Integrate continuous monitoring into the information system's operations.

xii. Establish the schedule for continuous monitoring to ensure adequate coverage of all controls is achieved.

xiii. Manage the information system's configuration according to established processes, monitor security controls, and provide status reports and documentation to the AO regularly.

xiv. Update and maintain the authorization package including SSP, SAR, POA&M, and Contingency Plan for each information system.

Information Security Officer (ISO)

a. The ISO has the following responsibilities with respect to security assessment and authorization:

i. Coordinate with the AO, SO, ISSO, and senior budget officials to ensure that resources will be considered in multi-year planning activities.

ii. Monitor the status of information system annual assessments.

iii. Monitor the timing constraints for final or renewal of security assessment and authorization actions.

iv. Advise the AO on potential issues related to assessments, results, and authorization requirements.

v. Assist in identifying and resolving any authorization accountability issues between organizations.

vi. Advise the AO of compliance status and issues for information systems in the organization.

Information System Security Officer (ISSO)

a. The ISSO has the following responsibilities with respect to security assessment and authorization:

i. Periodically review and verify that security controls specified in the SSP are in place and operating correctly.

ii. Assist the SO and ISO in their security responsibilities.

iii. Monitor the status of the ATO and advise the SO.

iv. Assist the ISO in coordination, status monitoring and oversight of authorization.

v. Advise the SO on security requirements and risk.

vi. Monitor the ATO statuses of the organization’s information systems and apprise the ISO and SO of compliance issues.

Chief Information Officer (CIO), Office of Environmental Information (OEI)

b. The CIO has the following responsibilities with respect to security assessment and authorization:

i. Collect and review the POA&M quarterly. Based on established criteria and an analysis of the risk mitigation strategy, the CIO provides recommendations for improvements as necessary to the SIO, ISO, SO, and ISSO as appropriate.

ii. Collect summary information from the POA&M and authorization status to meet EPA oversight reporting requirements to OMB and Congress.

iii. Provide quarterly reports to OMB as required.

iv. Instruct Office of Technology Operations and Planning (OTOP) to disconnect systems as necessary.

Office of Technology Operations and Planning (OTOP)

c. OTOP has the following responsibilities with respect to security assessment and authorization:

i. Review and disseminate a copy of the rejection or acceptance letter to the SO and the point of contact for the proposed organization requesting to interconnect with or through the Agency network and central processing resources.

ii. Disconnect information systems from the network as instructed.

<u>Office of Grants and Debarment (OGD)</u>

d. OGD has the following responsibilities with respect to security assessment and authorization:

   i. Assist EPA offices in establishing appropriate connection agreements on behalf of the Agency.

9. DEFINITIONS

- Administrative Closure – actions taken to close a task for a reason other than completion of the milestones enunciated in the task; reasons can include system retirement, deletion of a duplicate task, error in creation of a task, etc.
- Authorizing Official (AO) – (i) a senior agency official or executives with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to EPA mission operations and assets, individuals, other organizations, and the nation; (ii) has budgetary oversight for information systems or are responsible for the mission or business operations supported by the systems; (iii) a federal employee due to the inherently federal responsibilities of the function; and (iv) be in management positions with a level of authority commensurate with understanding and acceptance of information system-related security risks.
- Continuous Monitoring – a program that allows an organization to maintain the security authorization of an information system over time in a highly dynamic environment of operation with changing threats, vulnerabilities, technologies, and missions/business processes.
- Core Controls – controls that must be reviewed every year in order to be considered current. Non-core controls must be reviewed at least once every three years and must be scheduled to be reviewed within a three year period.
- Impartiality – free from any perceived or actual conflicts of interest with respect to the developmental, operational, and/or management chain associated with the information system or to the determination of security control effectiveness.
- Independent Assessor or Assessment Team – any individual or group capable of conducting an impartial assessment of an EPA information system.
- Information System Interconnection – the direct connection of two or more IT systems for the purpose of sharing data and other information resources.
- Plan of Action & Milestones (POA&M) – a document that identifies tasks that need to be accomplished to remediate identified weaknesses in an information system or program. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.
- Security Assessment – a process employed to review the management, operational, and technical security controls in an information system. This assessment determines 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. Security control assessments can include a variety of assessment methods (e.g., interviewing, examining, testing) and associated assessment procedures depending on the depth and breadth of the assessment. Security assessment results in the form of findings describe weaknesses or

deficiencies in the security controls employed in an information system and are used to provide an authorizing official with critical information needed to support a credible, risk-based decision on whether to place the system into operation or continue its operation.

- Security Authorization – the official management decision, conveyed through the authorization decision document, given by a senior organizational official or executive (i.e., authorizing official) to authorize operation of an information system and to explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.
- 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).
- 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, Section 5
- *Information Security – Interim Security Assessment and Authorization Procedures, June 2011*

13. ADDITIONAL INFORMATION

NA

EPA Classification No.:	CIO-2150.3-P-04.1	CIO Approval Date:	08/06/2012
CIO Transmittal No.:	12-003	Review Date:	08/06/2015

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

APPENDIX A: ACRONYMS

AO	Authorizing Official
ATO	Authorization to Operate
CIO	Chief Information Officer
EPA	Environmental Protection Agency
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
IG	Inspector General
ISA	Interconnection Security Agreement
ISO	Information Security Officer
ISSO	Information System Security Officer
IT	Information Technology
GAO	Government Accountability Office
GSS	General Support System
MOU/A	Memorandum of Understanding or Agreement
NCC	National Computer Center
NIST	National Institute of Standards and Technology
OEI	Office of Environmental Information
OIG	Office of Inspector General
OGD	Office of Grants and Debarment
OMB	Office of Management and Budget
OTOP	Office of Technology and Operations Planning
PII	Personally Identifiable Information
POA&M	Plan of Action and Milestones
SAISO	Senior Agency Information Security Official
SAR	Security Assessment Report
SIO	Senior Information Official
SLA	Service Level Agreement
SO	System Owner
SP	Special Publication
SSP	System Security Plan
SYSCAT	System Categorization
USC	United States Code

APPENDIX C: EPA SECURITY AUTHORIZATION PACKAGE TRANSMITTAL MEMO

Sample verbiage is provided below. However, when needed, please reference the *EPA System Security Assessment Memo* template found at http://intranet.epa.gov/itsecurity/Template%20-%20C&A%20Security%20Certification%20Memo.doc.

DATE: [Month DD, YYYY]

MEMORANDUM

SUBJECT: Security Controls Assessment for the **[Insert Information System Name]** Security Authorization Package

FROM: **[System Owner's Name and Title]**
[Office/Division]
[Program Office/Region Name]

TO: **[Authorizing Official's Name and Title]**
[Office/Division]
[Program Office/Region Name]

A security controls assessment of the [**Insert Information System Name**] located at **[Location]** has been conducted in accordance with OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*; NIST Special Publication 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*; and the EPA Agency Network Security Policy. The attached Security Authorization Package contains: (i) current System Security Plan (SSP), (ii) Security Assessment Report (SAR), and (iii) Plan of Action and Milestones (POAMs).

The security controls listed in the System Security Plan have been assessed by **[Assessor's Name]** and the results are documented in the SAR. The assessment provides information on 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. The POAMs describe the corrective measures that have been implemented or are planned, to address any weaknesses or deficiencies in the security controls for the information system and to reduce or eliminate known vulnerabilities.

____
[Print] Name, Title

____
Signature

Conditions:

[Conditions Placed Here. These Conditions Will Be Used To Establish POAMS Within Xacta To Address Any Concern(s) The Authorizing Official Has To Approve The System.]

cc: Robert McKinney Senior Agency
Information Security Officer (SAISO)
Office of Environmental Information

[Name]
Information Security Officer
[Office/Division]
[Program Office/Region Name]

Enclosures:

APPENDIX D: EPA SECURITY AUTHORIZATION DECISION DOCUMENT

Sample verbiage is provided below. However, when needed, please reference the *EPA Information Systems Authorization Decision Document* template found at http://intranet.epa.gov/itsecurity/Template%20-%20C&A%20System%20Security%20Plan%20Template.doc.

DATE [Month DD, YYYY]

MEMORANDUM

SUBJECT: Security Authorization, and Authorization to Operate, for the **[Insert Information System Name]** Security Authorization Package

FROM: **[Authorizing Official's Name and Title]**
[Office/Division]
[Program Office/Region Name]

TO: **[System Owner's Name and Title]**
[Certification Official's Name and Title]
[Information Security Officer's Name and Title]

After reviewing the results of the security controls assessment of the **[Insert Information System Name]** and its constituent system-level components **(**if applicable) located at **[Location]**, and the supporting evidence provided in the associated Security Authorization Package [including the current System Security Plan (SSP), the Security Assessment Report (SAR), and the Plan of Action and Milestones (POA&Ms)], I have determined that the risk to Agency operations, assets, individuals, other organizations, and the Nation resulting from the operation of the information system is **[Select: [acceptable]; [acceptable but only because an overarching mission necessity requires placing the system into operation or continuing its operation].**

Accordingly, I am issuing an Authorization to Operate the information system in its existing operating environment. The information system is authorized **[Select: [without any significant restrictions or limitations]; [Insert terms and conditions: provide a description of any specific limitations or restrictions placed on the operation of the information system or inherited controls that must be followed by the System Owner or common control provider]]**. This security authorization is my formal declaration that adequate security controls have been implemented in the information system and that a satisfactory level of security is present in the system. [The previous sentence should be deleted for those systems with significant terms and conditions and authorized solely because of overarching mission necessity.]

This Authorization to Operate will expire on **[Insert authorization termination date]** and reauthorization will be required.

The Security Authorization of the information system will remain in effect as long as the conditions exist as follows:

1. The vulnerabilities reported during the continuous monitoring process do not increase Agency-level risk to levels deemed unacceptable.
2. The system has not undergone any major changes requiring the System Security Plan to be updated.
3. The System's Owner commits to complete any POA&Ms that are established now or in the future to ensure the continued effectiveness of this System Security Plan and the security controls specified.

A copy of this letter with all supporting Security Authorization documentation should be retained in accordance with the Agency's record retention schedule.

____
[Print] Name, Title

____
Signature

cc: Robert McKinney
Senior Agency Information Security Officer (SAISO)
Office of Environmental Information

Enclosures:

APPENDIX E: SYSTEM THRESHOLD QUESTIONNAIRE

Sample verbiage is provided below. However, when needed, please reference the *System Threshold Questionnaire* template attached to this document.

1. Is the system a Local Area Network (LAN) or a Wide Area Network (WAN)?

__ Yes __No

2. Does the system support applications on desktop computers, file servers, mail servers, or Internet connections? A General Support System (GSS) can also be a mainframe or a group of servers that support multiple applications.

__ Yes __No

3. Is the system critical to EPA's mission?

__ Yes __No

4. Is the system reviewed under the Capital Planning and Investment Control (CPIC) process and required to complete an Exhibit 300?

__ Yes __No

5. Does the system contain sensitive Personally Identifiable Information (PII); i.e. social security number, medical information about an individual or financial information about an individual?

__ Yes __No

6. Does the system require special attention to security as a result of the information the system processes, stores, or transmits?

__ Yes __No

7. Does the system require special attention to security because of its significant role in the administration of Agency programs, finances, property or other resources?

__ Yes __No

8. Does the system require special attention to security as a result of the risk, including the likelihood and magnitude of harm if the information system and the information it processes, stores, or transmits were lost, misused, accessed by unauthorized individuals, disclosed, destroyed, or modified?

__ Yes __No

DOCUMENT CHANGE HISTORY

Version	Release Date	Summary of Changes	Author of Changes	DCN
0.8	10/20/2008	Initial draft	Heather Flager	Procedures-CA-Draft_TO62_020_1
2.0	6/17/2009	Incorporated EPA comments Final	Heather Flager	Procedures-CA-Final_TO62_020_2
2.1	9/22/2009	Modified CA-6 and responsibilities of ISO, SIO and added senior Agency official	William Gill	Procedures_CA_Final_v 2.1.doc
2.2	11/3/2009	Modified Responsibility of Senior Official (AO) to comply with NIST 800-53	William Gill	Procedures_CA_Final_v 2.2.doc
2.9	8/16/2010	Updated per NIST SP 800-53 Rev 3	Heather Flager	Procedures_CA_Draft.TO-062_050_1.0
2.9	8/19/2010	TISS Initial review	Charleen Johnson	Procedures_CA_Draft.TO-062_050_1.0
3.0	12/27/2010	TISS Final Draft Review	Charleen Johnson & Mark Hubbard	Procedures_CA_Draft.TO-062_050_1.0
3.1	5/4/2012	SAISO Final Review	Abe Getchell	Procedures_CA_Draft.TO-062_050_1.0
3.2	7/16/2012	Document Review	LaToya Gordon	Procedures_CA_Draft.TO-062_050_1.0