EPA INFORMATION
PROCEDURE

Information Security - Security Assessment and Authorization Procedures			
EPA Classification No.:	CIO 2150-P-04.2	CIO Approval Date:	05/27/2016
CIO Transmittal No.:	16-008	Review Date:	05/27/2019

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

INFORMATION SECURITY –
SECURITY ASSESSMENT AND AUTHORIZATION PROCEDURES

1. PURPOSE

To implement the security control requirements for the Security Assessment and Authorization (CA) control family, as identified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy 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 EPA.

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 the EPA.

3. AUDIENCE

The audience is all EPA employees, contractors, and all other users of EPA information and information systems that support the operations and assets of the EPA.

4. BACKGROUND

Based on federal requirements and mandates, the EPA is responsible for ensuring 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 shall meet the security requirements through the use of the security controls defined in the NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. This document addresses the procedures and standards set forth by the EPA, and complies with the family of Security Assessment and Authorization controls.

5. AUTHORITY

- E-Government Act of 2002, Public Law 107-347, Title III, Federal Information Security Management Act (FISMA) as amended
- Federal Information Security Modernization Act of 2014, Public Law 113-283, chapter 35 of title 44, United States Code (U.S.C.)
- 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
- Federal Information Processing Standards (FIPS) 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006
- Federal Information Processing Standards (FIPS) 201-1, Personal Identity Verification (PIV) of Federal Employees and Contractors, March 2006
- EPA Information Security Program Plan
- EPA Information Security Policy
- EPA Roles and Responsibilities Procedures
- EPA Information Security Continuous Monitoring Strategic Plan
- CIO Policy Framework and Numbering System
- Appendix I to OMB Circular No. A-130: Responsibilities for Management of Personally Identifiable Information

6. PROCEDURES

The "CA" designator identified in each procedure represents the NIST-specified identifier for the Security Assessment and Authorization control family, as identified in NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations.*

CA-2 – Security Assessments

For All Information Systems:

1) System Owners (SO), in coordination with Information Security Officers (ISO), Information Management Officers (IMO), Information Owners (IO), Information System Security Officers (ISSO), Common Control Providers (CCP) and Security Control Assessors (SCA), for EPA-operated systems shall; and Service Managers (SM), in coordination with IOs, ISOs, IMOs, ISSOs, CCPs, and SCAs, for systems operated on behalf of the EPA, shall ensure service providers:
    a) Assess security controls as early as possible and throughout the system development life cycle process.[1]
    b) Provide a security assessment plan prior to conducting assessments.
        i) The security assessment plan shall delineate:
            (1) The scope of the assessment,
            (2) The assessment procedures to be used to determine security control effectiveness,
                (a) Assessments shall be conducted in accordance with the latest final version – as determined by the EPA Senior Agency Information Security Officer (SAISO) – of NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations,*
            (3) The assessment environment, assessment team, and assessment roles and responsibilities.
        ii) ISSOs shall review each system security assessment plan to seek clarification and consensus for security requirements for each specific system under review.
        iii) For EPA-operated systems, SOs shall review and approve security assessment plans.
        iv) For systems operated on behalf of the EPA, IOs and SMs shall review and approve security assessment plans.
    c) Follow the security assessment plan and notify approvers of any changes to the plan necessary to complete the assessment once the assessment begins.

[1] *This requirement is not be applicable to systems operated on behalf of EPA where EPA is not involved with the development life cycle process. For example, when an established service is obtained from a cloud service provider the Service Manager or Information Owner need not determine and verify whether controls were assessed early and throughout the development life cycle process.*

d) Assess security controls under Continuous Monitoring guidelines supporting a frequency defined by the SAISO for on-going authorizations, or at least once every three (3) years[2], until the system is migrated to an on-going authorization; when significant changes are made after the initial ATO has been obtained; and until the system is decommissioned.

   i) Control assessments shall 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.

e) Follow the procedures below when significant changes are made to the information system.

   i) When significant changes are planned for, or made to, a system the SOs for EPA-operated systems and IOs and SMs for systems operated on behalf of the EPA shall conduct a Security Impact Analysis (SIA) to determine which controls shall be assessed for proper implementation and operation and assess those controls.

   ii) Incorporate results into the Risk Management Framework and address accordingly (e.g., residual risks are identified, mitigated, accepted etc.) plans of actions, and milestones are developed.

f) Document assessment results in a Security Assessment Report (SAR) that provides sufficient detail, to include correction or mitigation recommendations, to enable risk management, authorization decisions, and oversight activities.

g) Provide the SAR to the SIO in the authorization package and upload it to the Agency POA&M repository.

For FedRAMP[3] Low and Moderate Information Systems:

1) SMs, in coordination with IOs, ISOs, IMOs, and CCPs shall ensure service providers:

   a) Assess the security controls in the information system and its environment of operation at least annually to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements.

   b) Provide the results of the security control assessment to individuals or roles to include the FedRAMP PMO.

[2]Independent assessors or assessment teams assess portions of all controls annually. At a minimum, core controls, and any others identified by the SAISO, are assessed annually. Core controls are those controls identified by the SAISO as having greater impact on maintaining the desired security posture. Other controls may be identified by the SAISO as needing additional attention to improve their effectiveness.

[3] The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

CA-2(1) – Security Assessments | Independent Assessors

For Moderate and High Information Systems:

1) SOs, in coordination with ISOs, IMOs, IOs, ISSOs, CCPs and SCAs, for EPA-operated systems shall; and SMs, in coordination with IOs, ISOs, IMOs, ISSOs, CCPs, and SCAs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Assessors or assessment teams are independent third parties[4].

For FedRAMP[5] Low and Moderate Information Systems:

1) SMs, in coordination with IOs, ISOs, IMOs, and CCPs shall ensure service providers:
   a) Employ assessors or assessment teams for JAB Authorizations that are FedRAMP accredited third-party assessment organizations (3PAO) to conduct security control assessments.

CA-2(2) – Security Assessments | Specialized Assessments

For High Information Systems:

1) SOs, in coordination with ISOs, IMOs, IOs, ISSOs, CCPs and SCAs, for EPA-operated systems shall; and SMs, in coordination with IOs, ISOs, IMOs, ISSOs, CCPs, and SCAs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Provide detailed rules of engagement to be agreed upon by all parties before the commencement of any malicious user testing, penetration testing, or red team exercise.
   b) Include at least one of the following as part of all annual assessments, which can be conducted announced or unannounced.[6]
      i) Malicious user testing,
      ii) Penetration testing,
      iii) Red team exercise, or
      iv) Insider threat assessment.

For FedRAMP Moderate Information Systems:

1) SMs, in coordination with IOs, ISOs, IMOs, and CCPs shall ensure service providers:
   a) Employ an independent assessor or assessment teams to assess the security controls in the information system.

[4] *Assessors or assessor groups are independent third parties if they are not the individual or group that develops system security plans, contingency plans, and other control documentation; do not operate or maintain system controls; do not report to system management; and are not in a relationship where reciprocity of favorable results are actual or could be perceived.*

[5] *Cloud Service Providers (CSPs) can take one of three paths to become FedRAMP compliant: JAB Provisional Authorization (P-ATO), Agency Authorization, and CSP Supplied Package.*

[6] *The applicability of announced or unannounced is limited to the systems' user and administrator groups. All such action shall be coordinated through the CIO's Office, at a minimum with the SAISO and the Director, OTOP.*

CA-2(3) – Security Assessments | External Organizations

For FedRAMP Moderate Information Systems:

1) SMs, in coordination with IOs, ISOs, IMOs, and CCPs shall ensure service providers:
   a) Accept the results of an assessment performed by any FedRAMP Accredited 3PAO when the assessment meets the conditions of a P-ATO[7] in the FedRAMP Repository.

CA-3 – Information System Connections

For All Information Systems:

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

1) SOs, in coordination with ISOs, IMOs, IOs, ISSOs, CCPs and SCAs, for EPA-operated systems shall; and SMs, in coordination with IOs, ISOs, IMOs, ISSOs, CCPs, and SCAs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Authorize connections from the information system to other information systems outside of the authorization boundary through the use of Interconnection Security Agreements (ISA),
   b) Follow the procedures below for connections to systems outside of the EPA intranet:
      (1) An approved Interagency Agreement (IA) or Memorandum of Understanding / Agreement (MOU/A) signed by a SIO is implemented with the ISA.
      (2) Route connections through the agency's Trusted Internet Connection (TIC) solution or equivalent approved by the SAISO and adhere to requirements promulgated in TIC directives.
      (3) Submit an interconnection request to the EPA's National Computer Center (NCC) Director. The request shall include the following:
         (a) Type of connection to be established,
         (b) Connection requirements,
         (c) Key personnel to help coordinate the planning efforts of the system interconnection,
         (d) Duration of the interconnection, and
         (e) Point of contact for the external organization requesting the interconnection.
      (4) The Director, NCC reviews and approves or rejects the request and sends a copy of the acceptance or rejection letter to the SO, SIO, ISO, and the point of contact for the external organization requesting the connection. If rejected, the letter shall include the rejection reason(s) and corrective actions needed for acceptance.

[7] *CSPs with a JAB Provisional Authorization (FedRAMP P-ATO) have undergone a rigorous technical review by the FedRAMP PMO, been assessed by a FedRAMP accredited 3PAO, and received a P-ATO from the DHS, DOD, and GSA CIOs. CSPs with an Agency Authorization have worked directly with a customer agency to achieve a FedRAMP compliant ATO that has been verified by the FedRAMP PMO.*

(5) In addition to the SIO of the program office or region implementing the connection, the Office of Environmental Information (OEI) SIO signs the ISA and IA or MOU/A authorizing the interconnection and accepting the associated risks for supporting OEI systems.

ii) For connecting systems that have the same SIO, an ISA is not required. Rather, the interface characteristics between the connecting information systems shall be described in the System Security Plans (SSP) for the respective systems, and

iii) For connecting systems with different SIOs, the SIOs shall come to a consensus agreement on whether an ISA is required.

(1) If one SIO determines a need for an ISA, all parties shall coordinate to develop and implement the ISA.

(2) If all SIOs agree an ISA is not required, the interface characteristics between the connecting information systems shall be described in the SSPs for the respective systems.

c) Have the SIO authorizing the system(s) for operation, whether EPA-operated or operated on behalf of the EPA, involved in the interconnection sign the ISA(s) authorizing the interconnection and accepting the associated risks,

d) Have the SIO authorizing the system(s) for operation, whether EPA-operated or operated on behalf of the EPA, involved in the interconnection sign IA(s) or MOU/A(s),

e) Have a current ATO or authorization to test for all systems to be interconnected prior to establishing the interconnection,

f) Conduct an SIA prior to connecting the systems,

g) Present SIA results to the SIO with recommendations on interconnecting the systems from the IMO and ISO,

i) SIOs shall make risk based decisions on whether to approve interconnections.

h) Fully document approved interconnections in the respective SSPs,

i) All interconnected systems’ documentation, such as contingency plans, shall be updated to reflect the impact and change.

i) Provide information system documentation to system personnel of the externally connected system upon request,

i) System personnel requesting access to EPA’s information system documentation shall review it on site at an EPA facility.

j) Review, update and reissue ISAs, as necessary, at least annually or whenever significant changes have been made to any of the interconnected systems, to ensure all security requirements are adequately addressed and that no material changes to the connection have occurred,

i) The annual review can be incorporated with the annual assessment,

ii) The SSP and other security documents addressing the interconnection shall also be reviewed and updated to ensure they accurately reflect the status of each interconnection,

k) Monitor and test information system interconnections on an ongoing basis verifying enforcement of security requirements,

l) Notify the Director, NCC in writing of the decision to terminate the system interconnection, whether the interconnection is in place or previously planned,

m) Notify the Director, NCC in writing of the decision to restore any system interconnection that was previously terminated,

n) Terminate all system interconnections under the following conditions:

   i) An ATO of an interconnected system expires or is withdrawn,

   ii) The IA or Memorandum of Understanding (MOU)/Memorandum of Agreement (MOA) associated with the interconnection expires or is withdrawn,

   iii) The ISA expires or is withdrawn, or

   iv) The business case no longer requires the system connection.

o) Accomplish the following actions upon system interconnection termination:

   i) Assess or re-assess relevant security controls (e.g., access authorizations, physical connections).

   ii) Update appropriate security documentation. The following documents at a minimum shall be updated:

      (1) SSP[8]

      (2) Risk Assessment[9]

      (3) Contingency Plan (CP)[10]

      (4) Incident Response Plan[11]

For FedRAMP Low Information Systems:

1) SMs, in coordination with IOs, ISOs, IMOs, and CCPs shall ensure service providers:

   a) Review and update Interconnection Security Agreements (ISA) every three years and on input from FedRAMP.

For FedRAMP Moderate Information Systems:

1) SMs, in coordination with IOs, ISOs, IMOs, and CCPs shall ensure service providers:

   a) Review and update Interconnection Security Agreements (ISA) annually and on input from FedRAMP.

CA-3(1) – System Interconnections | Unclassified National Security System Connections

Not selected as part of the control baseline.

CA-3(2) – System Interconnections | Classified National Security System Connections

[8] *Refer to the latest version of the EPA Information Security – Planning Procedures for update guidance.*
[9] *Refer to the latest version of the EPA Information Security – Risk Assessment Procedures for update guidance.*
[10] *Refer to the latest version of the EPA Information Security – Contingency Planning Procedures for update guidance.*
[11] *Refer to the latest version of the EPA Information Security – Incident Response Procedures for update guidance.*

Not selected as part of the control baseline.

CA-3(3) – System Interconnections | Unclassified Non-National Security System Connections

For FedRAMP Moderate Information Systems:

1) SMs, in coordination with IOs, ISOs, IMOs, and CCPs shall ensure service providers:
    a) Prohibit the direct connection of unclassified, non-national security systems to an external network without the use of Boundary Protections that meet the Trusted Internet Connection (TIC) requirements.[12]

CA-3(4) – System Interconnections | Connections to Public Networks

Not selected as part of the control baseline.

CA-3(5) – System Interconnections | Restrictions on External System Connections

For Moderate and High Information Systems:

1) SOs, in coordination with ISOs, IMOs, IOs, ISSOs, CCPs and SCAs, for EPA-operated systems shall; and SMs, in coordination with IOs, ISOs, IMOs, ISSOs, CCPs, and SCAs, for systems operated on behalf of the EPA, shall ensure service providers:
    a) Employ a “deny-all, permit-by-exception” policy for allowing information systems to connect to external information systems.
        i) “Allow-all, deny-by-exception” is a weak policy, known as *blacklisting*.
        ii) “Deny-all, permit-by-exception” is a strong policy, known as *whitelisting*.
2) SOs, in coordination with ISOs, IMOs, IOs, ISSOs, CCPs and SCAs, for EPA-operated systems shall; and SMs, in coordination with IOs, ISOs, IMOs, ISSOs, CCPs, and SCAs, for systems operated on behalf of the EPA shall:
    a) Determine what exceptions, if any, are acceptable.

CA-4 – Security Certification

Incorporated into CA-2

CA-5 – Plan of Action and Milestones

For All Information Systems:

1) SOs, in coordination with ISOs, IMOs, IOs, ISSOs, CCPs and SCAs, for EPA-operated systems shall; and SMs, in coordination with IOs, ISOs, IMOs, ISSOs, CCPs, and SCAs, for systems operated on behalf of the EPA, shall ensure service providers:
    a) Document and manage discovered weaknesses and planned remedial actions – Plans of Action and Milestones (POA&Ms) – in the Agency Information Security Repository.[13] All

[12] *Refer to the TIC Reference Architecture 2.0 document: http://www.dhs.gov/trusted-internet-connections.*

[13] *The Agency’s Information Security Repository is used to meet oversight reporting requirements to OMB and Congress as well as managing and tracking information security issues for systems and services involving EPA information.*

discovered weaknesses, recommendations and their sources of discovery shall be traceable to the related POA&M. ISOs shall review and validate completed POA&Ms to ensure that artifacts are in place for closure, those POA&Ms not meeting criteria to close shall be returned to the SO for remediation and resubmission for closure.

i) POA&Ms shall be developed for discovered weaknesses from any source including, but not limited to, the following:

(1) Reviews, tests, audits or assessments;

(2) SIA;

(3) Independent verification and validation (IV&V) findings;

(4) Continuous monitoring activities;

(5) Incidents; and

(6) Routine maintenance and administration.

b) Identify POA&Ms as either Program or System level.

i) Program level POA&Ms address weaknesses that affect multiple systems within a program office or region, enterprise wide or the entire information security program. Examples include outdated regional level procedures, a lack of a patch management process, and a lack of an Information Security Program Plan.

ii) System level POA&Ms address weaknesses that pertain to a single system. Examples include an outdated SSP, controls improperly configured, and controls not assessed according to policy.

c) Analyze identified weaknesses to determine their level of risk (i.e., high, medium, low) and identify appropriate action(s) necessary to remediate or mitigate, as appropriate, the identified weaknesses to an acceptable level of risk.

i) Document discovered weaknesses in POA&Ms:

(1) Within 30 days of discovery when the risk is determined to be High and the weakness cannot be or is not remediated or mitigated within 30 days of discovery.

(2) Within 60 days of discovery when the risk is determined to be Medium and the weakness cannot be or is not corrected within 60 days of discovery.

(3) Within 90 days of discovery when the risk is determined to be Low and the weakness cannot be or is not corrected within 90 days of discovery.

(4) Document results of actions taken to remediate or mitigate all weaknesses with appropriate artifacts, such as screen shots, verifying scans or testing results.

d) Document the following information in each POA&M:[14,15]

i) Type of weakness;

ii) Identity of the office, SO or IO responsible for resolving the weakness;

iii) Estimated funding required for resolving the weakness;

[14] *In accordance with OMB memo M 02-01 Guidance for Preparing and Submitting Security Plans of Action and Milestones.*

[15] *For non-EPA-operated systems and services sufficient information shall be obtained to enable informed risk based decisions by SIOs, such as type of weakness with identified risk, scheduled completion dates, and status.*

iv) Scheduled completion date for weakness remediation or mitigation;

(1) The start date and completion date may be revised, but the baseline dates shall not be changed.

(2) Any revision to the completion date shall include documented justification for the schedule change.

v) Key milestones with completion dates;

(1) Each POA&M should normally have multiple milestones.

(2) Each milestone shall have a baseline start and baseline end date.

vi) Source of weakness discovery; and

vii) Status of the corrective action using one of the following terms:

(1) Ongoing

(2) Completed

(a) The term *completed* should only be used when corrective actions have been completed and verified to obtain the desired level of remediation or mitigation.[16]

e) Document an SIO's or Risk Executive's decision to accept a weakness in a POA&M.

i) The completion date is the date the decision is made to accept the risk.

ii) A key milestone will be the risk acceptance decision.

f) Review and update POA&Ms monthly.

i) Review POA&M statuses identifying outstanding risks quarterly with the applicable SIO, ISO, IMO, and others, as necessary, to facilitate the risk management process.

g) Coordinate with the SAISO in monitoring and validating discovered weaknesses.

i) For additional information concerning the POA&M monitoring and validation process, refer to Appendix B.

h) Include applicable POA&Ms in systems' security accreditation packages for SIO review.

CA-5(1) – Plan of Action and Milestones | Automation Support For Accuracy/Currency

Not selected as part of the control baseline.

CA-6 – Security Authorization

For All Information Systems:

1) SOs, in coordination with ISOs, IMOs, IOs, ISSOs, CCPs and SCAs, for EPA-operated systems shall; and SMs, in coordination with IOs, ISOs, IMOs, ISSOs, CCPs, and SCAs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Produce and submit a security authorization package, consisting of the SSP, SAR, CP, POA&Ms and all associated IAs or MOU/MOAs and ISAs to the appropriate SIO for review and adjudication. At a minimum, the ISO, IMO and the AODR, if assigned, shall

[16] *Also used when documenting decisions to accept risks posed by discovered weaknesses.*

present the security authorization package, detail risks, and provide authorization recommendations to the SIO. The SO, IO, SM, and/or the ISSO are also highly encouraged to attend the presentation to provide additional details in regards to the authorization package.

i) The SIO for the program office or region that implements a system or obtains a service to meet their mission needs is normally the appropriate SIO. Multiple SIOs may coordinate to make the authorization decision when a system supports crosscutting or multiple missions.[17] However, multiple SIOs are not required in such situations. A single program office or region may take ownership of the system and that program office's or region's SIO will make the authorization decision.

ii) The security authorization package provides the SIO with essential information to make a credible, informed, risk-based decision on whether to allow the system to operate or not.

iii) The ISO, IMO, and AODR support the SIO in reviewing and understanding control implementations, testing results, residual risks to the system and information and risks to operations and other systems and information.

b) Obtain an Authorization to Operate (ATO) from the appropriate SIO(s) and the CIO before commencing system operations and periodically thereafter.

c) Obtain approval of the implementation of the NIST 800-53 Appendix J controls from the Senior Agency Official for Privacy (SAOP).[18] This approval is a precondition to the issuance of an ATO.

i) Forward draft authorization packages to the Agency Privacy Officer (APO) for review.

ii) The APO shall review authorization packages, follow up with SIO/ISO/ISSOs and Privacy Liaison Officers (PLOs) as needed and review with and make recommendations to the SAOP on whether to approve the controls.

iii) The APO shall inform SIOs, ISOs, SOs and PLOs of SAOP decisions and any remedial actions needed.

d) Maintain an ATO through a robust continuous monitoring program.

e) Obtain an ATO at least every three (3) years unless approved by the SAISO for an ongoing ATO.

i) If a robust continuous monitoring program approved by the SAISO is in place for the program office or region, ongoing ATOs can be used.

f) Obtain a new ATO when there is a significant change[19] to the information system.

[17] *Where multiple SIO's authorize a system for operation, one SIO – and their program office or region – shall be identified as the "lead." Reporting and tracking of the system in the Agency's Information Security Repository shall be accomplished by the lead program office and region personnel. Non-lead SIOs and as necessary personnel from their program office or region involved with the system maintenance, management, and security (e.g., ISO, IMO, ISSO, SO, IO) shall be provided access to the system information in the tool.*

[18] *For EPA, the Chief Information Officer (CIO) serves as the Senior Agency Official for Privacy (SAOP).*

[19] *Refer to Risk Assessment Procedures for guidance on what constitutes a significant change.*

i) If approved for an ongoing ATO by the SAISO, coordinate with the SAISO to determine whether a new ATO is required.

g) Notify, using the Agency Information Security Repository, the SAISO of authorizations for periods less than three years.

i) The following shall be addressed in the notification:

(1) Any terms and conditions that place limitations or restrictions on the operation of the information system during the abbreviated term.

(2) POA&Ms to address identified weakness.

ii) Interim ATOs are not authorized for use in the EPA.[20]

iii) Authorization to Test (ATT) can be granted by an SIO if:

(1) An operational environment or live data is required to complete specific test objectives (e.g., replicating certain operating conditions in the test environment is impractical) and

(2) All applicable controls are tested and validated to ensure they are operating properly prior to testing in an operational environment or with live data except for those that can only be tested in an operational environment or with live data.

iv) ATTs shall not be used to avoid ATO assessment and authorization activity.

(1) Systems with an ATT shall only be operated for testing purposes (i.e., the system shall not be used for operational purposes during the ATT period).

v) Only authorize ATTs for use for the time required to conduct the testing.

(1) The authorized time period shall not exceed 30 days without SAISO approval.

(a) A waiver request that includes the desired time period, operational impact, risks, and justification for the extension shall be submitted to the SAISO for approval if greater than 30 days is desired.

h) Update and maintain the authorization package documents for each information system for which they are responsible.

i) Use results of all assessments and continuous monitoring processes to the maximum extent possible for developing and maintaining authorization package documents and authorization decisions.

2) SIOs and the CIO shall:

a) Review the authorization package to determine whether to authorize the system to operate with EPA information.

i) The SIO documents the authorization decision and associated risks, and signs a statement acknowledging accountability and the authorization decision. The SIO may add any additional requirements deemed necessary for security.

(1) The signed approval to operate also indicates the SIOs approval of the security authorization package and enclosed documents.

[20] *ATO's are required to document the AO's decision to allow a system to operate with EPA information. An ATO may be issued for periods less than three years. ATOs for testing purposes are also acceptable for use.*

ii) The authorization document shall include:

(1) The authorization decision,

(a) If the decision is to deny authorization, the following shall be included:

(i) Rationale for not accepting the risks.

(ii) Required corrective actions, if applicable.

(2) Terms and conditions for the authorization,

(a) Any special circumstances or restrictions under which the system shall operate.

(3) Date system authorized for operation,

(4) Authorization termination date, if using an ongoing ATO state ‘ongoing’ rather than providing a termination date, and

(5) Risk Executive function input (if provided).

b) Forward final authorization packages, including the authorization decision document and any additional SIO determined security requirements, to the SAISO.

i) The SAISO shall review authorization packages, follow up with SIO/ISO/ISSOs as needed and review with and make recommendations to the CIO on whether to authorize systems to operate.

ii) The SAISO shall inform SIOs, ISOs and SOs of CIO decisions and any remedial actions needed.

iii) The SO shall enter authorization package documents and information into the Agency Information Security Repository if not already entered.

3) The ISSO shall:

a) Verify that all required documents and information are entered into the Agency Information Security Repository. The ISO shall coordinate with the SO to correct any deficiencies.

4) ISOs shall:

a) Track authorization statuses of systems for which they are responsible and apprise the appropriate SIO of when and what actions are required with sufficient lead-time to take actions to maintain authorizations.

i) The time period for reauthorization shall be calculated from the date the CIO approves the system for operation.

5) Users shall:

a) Only use EPA information in systems authorized for use by an SIO and the CIO.

CA-7 – Continuous Monitoring

For All Information Systems:

1) The SAISO shall:

a) Develop the EPA continuous monitoring strategy. The strategy shall establish the following at a minimum to assist SIOs with determining risks:

i) Monitoring metrics,

ii) Monitoring and assessment frequencies, and

iii) Security status reporting frequency and recipients.

2) The Director, OTOP shall:

a) Implement the continuous monitoring strategy for enterprise level continuous monitoring tools, processes and configurations, and

b) Coordinate development and integration of region, program office, and system level tools, processes, and configurations into enterprise level tools, processes, and configurations.

3) SOs, in coordination with ISOs, IMOs, IOs, ISSOs, and CCPs, for EPA-operated systems shall; and SMs, in coordination with IOs, ISOs, IMOs, and CCPs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Coordinate with the Director, OTOP to develop and integrate region, program office and system level continuous monitoring tools, processes and configurations into enterprise level tools, processes and configurations;

b) Implement the continuous monitoring strategy;

c) Correlate and analyze system level security-related information generated by assessments and monitoring to identify weaknesses and develop corrective actions; and

d) Report system level security statuses to the SAISO monthly in the Agency Information Security Repository and other identified monitoring and reporting tools.

4) IMOs and ISOs shall:

a) Coordinate with the Director, OTOP to develop and integrate region, program office and system level continuous monitoring tools, processes and configurations into enterprise level tools, processes and configurations;

b) Report program offices’ and regions’ security statuses to the SAISO monthly in the Agency Information Security Repository and other identified monitoring and reporting tools;

c) Ensure system level security statuses are reported to the SAISO monthly in the Agency Information Security Repository or other pre-approved and identified monitoring and reporting tools;

d) Correlate and analyze program offices, regions and system level security-related information generated by assessments and monitoring to identify program offices’ and regions’ level weaknesses and develop corrective actions; and

e) Implement and enforce the continuous monitoring strategy.

5) SOs, in coordination with IOs, ISOs, ISSOs, and CCPs, for EPA-operated systems shall; and SMs, in coordination with IOs, ISOs, ISSOs, and CCPs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Adhere to the latest NIST guidance[21] to conduct self and independent control assessments.

[21] *NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems and Organizations*

For FedRAMP Low and Moderate Information Systems:

1) SMs, in coordination with IOs, ISOs, IMOs, and CCPs shall ensure service providers:
   a) Ensure ongoing security status monitoring of EPA-defined metrics in accordance with the organizational continuous monitoring strategy to meet Federal and FedRAMP requirements.

CA-7(1) – Continuous Monitoring | Independent Assessment

For Moderate and High Information Systems:

1) SOs, in coordination with ISOs, IMOs, IOs, ISSOs, CCPs and SCAs, for EPA-operated systems shall; and SMs, in coordination with IOs, ISOs, IMOs, ISSOs, CCPs, and SCAs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Employ assessors or assessment teams with an adequate level of independence[22] to monitor the security controls in the information system on an ongoing basis.

CA-7(2) – Continuous Monitoring | Types of Assessments

Not selected as part of the control baseline.

CA-7(3) – Continuous Monitoring | Trend Analysis

Not selected as part of the control baseline.

CA-8 – Penetration Testing

For High Systems:

1) SOs, in coordination with ISOs, ISSOs, CCPs, and IOs, for EPA-operated systems shall: and SMs, in coordination with IOs, ISOs and CCPs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Conduct penetration testing annually and obtain results from providers. Conducting of penetration testing for C-8 can be applied to satisfy the CA-2 requirement.

CA-8(1) – Penetration Testing | Independent Penetration Agent or Team

For FedRAMP Moderate Information Systems:

1) SMs, in coordination with IOs, ISOs, IMOs, and CCPs shall ensure service providers:
   a) Employ an independent penetration agent or penetration team to perform penetration testing on the information system or system components.

CA-8(2) – Penetration Testing | Red Team Exercises

Not selected as part of the control baseline.

[22] *Assessor independence provides a degree of impartiality to the continuous monitoring process. To achieve such impartiality, assessors should not: (i) create a mutual or conflicting interest within EPA where the assessments are being conducted; (ii) assess their own work; (iii) act as management or employees of the EPA organizations they are serving; or (iv) place themselves in advocacy positions for the EPA organizations acquiring their services.*

CA-9 – Internal System Connections

For All Information Systems:

1) The SAISO and the Director, OTOP in the Enterprise Architecture shall:
   a) Establish classes and subclasses of components permitted for internal system connections;
   b) Develop baseline configurations for each component class and subclass; and
   c) Define interface characteristics and security standards for each component class and subclass connection type by FIPS-199 categorization – High, Moderate or Low.
2) SOs, in coordination with ISOs, IMOs, CCPs and IOs, for EPA-operated systems shall; and SMs, in coordination with IOs, ISOs, and CCPs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Only implement the established classes and subclasses of components;
   b) Implement the components according to the baseline configurations, interface characteristics and security requirements; and
   c) Document, in SSPs, classes and subclasses implemented and any deviations from the standards.

CA-9(1) – Internal System Connections | Security Compliance Checks

Not selected as part of the control baseline.

7. RELATED DOCUMENTS

- NIST Special Publications, 800 series
- Federal Identity, Credential and Access Management (FICAM)

8. ROLES AND RESPONSIBILITIES

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

1) The CIO has the following responsibilities with respect to security assessment and authorization:
   a) Serve as the Senior Agency Official for Privacy (SAOP).
      i) Adjudicate privacy controls.
   b) Adjudicate authorization packages.
   c) Collect, review and take action as necessary on summary information from the POA&M and authorization statuses.
   d) Instruct the Director, OTOP to disconnect systems as necessary.

Senior Agency Information Security Officer (SAISO)

1) The SAISO has the following responsibilities with respect to security assessment and authorization:
   a) Provide oversight to the Agency’s security assessment and authorization process and status.
   b) Notify SIO, IMO, ISO, SO, SM, and ISSO of compliance issues.
   c) Prepare disconnection notices for non-compliant information systems.
   d) Determine and publish core controls in consultation with appropriate officials.
   e) Determine and publish control assessment frequencies.
   f) Review authorization packages for and brief with and make authorization decision recommendations to the CIO.

   Agency Privacy Officer

   g) Review privacy controls for and brief with and make approval recommendations to the CIO.

Director, Office of Technology Operations and Planning (OTOP)

1) Director, OTOP has the following responsibilities with respect to security assessment and authorization:
   a) 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.
   b) Disconnect information systems from the network as instructed by the CIO.

Director, National Computer Center (NCC)

1) The Director, NCC has the following responsibilities with respect to security assessment and authorization:
   a) Review and approve or reject external interconnection requests.
   b) Notify SIO, SO, ISO, SM, and the point of contact for the external organization of the approval or rejection of interconnection request.

Senior Information Official (SIO)

1) The SIO has the following responsibilities with respect to Security Assessment and Authorization:
   a) Carry out the duties of AO.
   b) Attend and provide briefings on the information system within assigned organizational component and provide input into POA&Ms.
   c) Assist in acquiring funding and resources to address POA&Ms.
   d) Assign a designated representative to perform AO functions, with the exception of accepting risk, and sign authorization decision documents as needed.
   e) Adjudicate Interagency interconnect requests.

Authorizing Official (AO)

1) The AO has the following responsibilities with respect to security assessment and authorization:
    a) Review and adjudicate authorization packages and related assessment documentation as required.
    b) Determine whether significant changes in the information systems or environments of operation require reauthorization.
    c) 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, EPA's assets, and individuals in accordance with criteria in this procedure.
    d) Coordinate with the OIG, CIO, SAISO, and Risk Executive function to determine the implications of any decisions on assessor independence in the types of special circumstances as aforementioned.
    e) Determine the risk associated with each information system connection and the appropriate controls employed.
    f) Coordinate with the SAOP for review of privacy controls prior to adjudicating authorization packages.

Authorizing Official Designated Representatives (AODR)

1) The AODR has the following responsibilities with respect to security assessment and authorization:
    a) Carry out the duties of the AO as assigned.
    b) Coordinate and conduct the required day-to-day activities associated with the authorization process, ensuring proper management of risks and adequate protection of systems and information.

System Owner (SO)

1) The SO has the following responsibilities with respect to security assessment and authorization:
    a) Assess the information security controls at least 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.
    b) Provide the results of the security control assessment to the AO, in writing.
    c) 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.
    d) Ensure that the security assessment is conducted in support of OMB Circular A-130, Appendix III and NIST requirements for authorizing the information system.
    e) Conduct penetration testing and auditing as required to ensure compliance with all EPA security and continuous monitoring requirements.
    f) Establish a connection to an EPA or non-EPA information system; submit a request to the NCC Director.

g) Review and update the ISA or MOU/MOA annually to reaffirm the meeting of all security requirements and that no changes to the connection have occurred.

h) 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.

  i) Ensure POA&Ms are properly tracked, reviewed, and managed in accordance with the Agency's FISMA reporting and tracking requirements.

i) Ensure all information system continuous monitoring activities are completed in accordance with the EPA Continuous Monitoring Strategic Plan efforts.

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

k) Update and maintain the authorization packets including SSP, SAR, POA&M, and CP for each information system.

l) Review and manage POA&Ms in the Agency's Information Security Repository.

Information Security Officer (ISO)

1) ISOs have the following responsibilities with respect to security assessment and authorization:

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

  b) Monitor the status of information system annual assessments and authorization efforts.

  c) Provide advice to the AO and assist on potential issues related to security assessments and, results, and authorization requirements.

  d) Provide advice to the AO on compliance status and issues for information systems in the organization.

  e) Manage POA&Ms in the Agency's Information Security Repository.

Information System Security Officer (ISSO)

1) ISSOs have the following responsibilities with respect to security assessment and authorization:

  a) Support the SIO, SO, SM, IO and ISO with managing and implementing the information security control and assessment and authorization activities, processes, policies, procedures and other countermeasures identified under the EPA Information Security Program.

  b) Ensure the day-to-day security operations of an information system.

  c) Ensure the information security controls are implemented correctly, continuously verified, and functioning as intended.

  d) Develop and maintain, in coordination with system administrators and others involved with implementing and maintaining controls, the system security plan, including appendices, the contingency plan, and other documents required for information system authorization packages.

e) Ensure systems have an authorization to operate or authorization to test from the appropriate SIO prior to use or testing in an operational environment.

f) Enter POA&Ms, security controls, SSP, SAR and scan results, ATO status, and all other required information into the Agency Information Security Repository and maintain current and accurate information.

g) Coordinate with the CIO, Risk Executive, Risk Executive Group (REG), SAISO, and others involved with securing Agency information and systems to ensure risks are managed to an acceptable level.

h) Enter security compliance information for the system for which they have responsibility into the Agency POA&M repository.

Service Managers (SM)

1) SMs have the following responsibilities with respect to security assessment and authorization:

a) Implement policies, procedures and control techniques identified in the Agency information security program.

b) Ensure procedures, control techniques and other countermeasures as necessary to support and implement agency information security program requirements are developed and implemented for enterprise services.

c) Coordinate with key information security personnel such as the SOs, IOs, ISSO, CCP, SCAs, and other service managers to determine the information system’s security control requirements (common, hybrid, and core), implementation, assessments and authorization documentation and continuing monitoring activities.

d) Ensure systems supporting non-enterprise services are configured, monitored, and maintained to adequately protect supported information stored, processed, or transmitted within acceptable risks in accordance with the Agency’s requirements.

e) Ensure all information security controls are assessed prior to systems becoming operational and at a minimum, one third of the security controls are assessed at least once every three (3) years or when significant changes are made after the initial ATO has been obtained and until the system is decommissioned.

f) Ensure defined core controls are assessed annually as part of the subset (one-third) of the security controls required for annual assessments.

g) Ensure independent assessors or assessment teams conduct control assessments for moderate and high-categorized systems, and obtain SARs from assessors.

h) Ensure service providers develop and manage POA&Ms for discovered weaknesses for enterprise services.

i) Coordinate with the Agency’s ISOs and SOs to enter and manage POA&Ms in the Agency’s Information Security Repository.

Information Owners (IO)

1) IOs have the following responsibilities with respect to security assessment and authorization:
   a) Ensure all controls are assessed for systems supporting non-enterprise services obtained prior to deployment of the service to include the minimum subset of all security controls required to be assessed annually.
   b) Ensure independent assessors or assessment teams conduct control assessments for moderate and high-categorized information and obtain security assessment reports from the assessors.
   c) Coordinate with key information security personnel such as the SOs, IOs, ISSO, CCP, SCAs, and other service managers to determine the information system’s security control requirements (common, hybrid, and core), implementation, assessments and authorization documentation and continuing monitoring activities.
   d) Ensure identified security controls that are required to adequately protect stored, processed, or transmitted information by supporting systems are implemented.
   e) Identify and provide information to SOs, ISOs, IMOs, CCPs, SMs and service providers for additional or more stringent controls other than those identified in the baseline controls according to risk analyses.

Common Control Provider (CCP)

1) CCPs have the following responsibilities with respect to security assessment and authorization:
   a) Coordinate with the CIO, SAISO, IOs, SOs, ISOs, IMOs, and SMs regarding information security requirements, and determine and carry out responsibilities for defining, developing, documenting, implementing, assessing, and monitoring all controls to include common and hybrid controls.
   b) Assist the SOs and IOs with developing, implementing, assessing, configuring, continuously monitoring and determining common controls to adequately protect information stored, processed or transmitted within acceptable risks.
   c) Coordinate with SOs and IOs to ensure the proper categorization of systems according to information categorizations.
   d) Coordinate with SOs and IOs to identify controls required to adequately protect information stored, processed, or transmitted by assigned systems.
   e) Assist SOs and IOs with determining information systems security controls in accordance with the Agency’s security requirements.

Information Management Officer (IMO)

1) IMOs have the following responsibilities with respect to security assessment and authorization:
   a) Ensure independent assessors and/or assessment teams conduct assessments.
   b) Ensure testing and exercises are conducted in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

c) Ensure discovered weaknesses and planned remedial actions are documented and managed within the Agency's Information Security Repository.

d) Produce and submit a security authorization package, consisting of the SSP, SAR, CP, POA&Ms, and all associated IAs or MOU/MOAs and ISAs to the appropriate SIO for review and adjudication.

e) Obtain an ATO from the appropriate SIO before commencing system operations and periodically thereafter.

f) Coordinate with the Director, Office of Technology Operations and Planning (OTOP) to develop and integrate regions, program offices and system level continuous monitoring tools, processes and configurations into enterprise level tools, processes and configurations.

g) Provide SIOs with SIA results and recommendations on interconnecting systems.

Security Control Assessors (SCA)

1) SCAs have the following responsibilities with respect to security assessment and authorization.

a) Provide security assessment plans to the SOs prior to conducting security assessments.

b) Test security controls according to the security assessment plan in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

c) Provide SO and IO with documented information system security assessment results (i.e., SAR).

9. DEFINITIONS

- *Administrative Closure* – actions taken to close a task for a reason other than completion of the milestones stated in the task; reasons can include system retirement, deletion of a duplicate task, error in creation of a task, etc.
- *Authorizing Official (AO)* – defined in the EPA as the Senior Information Official; (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 shall be reviewed every year in order to be considered current. Non-core controls shall be reviewed at least once every three years and shall be scheduled to be reviewed within a three-year period.
- *EPA-operated System* – a system where EPA personnel have sole, direct system management responsibilities. System administration is directed by EPA personnel and may be accomplished by EPA federal employees or contractors. The system may be operated internally or externally to the EPA's intranet boundary.
- *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.
- *Ongoing Authorization* – the SIOs continued authorization to operate a system based on risk identified through use of a robust continuous monitoring program.
- *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, or findings, describe weaknesses or deficiencies in the security controls of an information system and 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).
- *System Operated on Behalf of the EPA* – a system where EPA personnel do not have sole or direct system management responsibilities. System administration is directed and

performed by service provider personnel. The system may be operated within or external to EPA's intranet boundary.

- *Written* (or in writing) – to officially document the action or decision, either manually or electronically, and includes a signature.

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 a 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 – Interim Security Assessment and Authorization Procedures, Version 2.0, July 16, 2012

13. ADDITIONAL INFORMATION

N/A

Ann Dunkin
Chief Information Officer
U.S. Environmental Protection Agency

APPENDIX A: ACRONYMS AND ABBREVIATIONS

AO	Authorizing Official
AODR	Authorizing Official Designated Representative
ATO	Authorization to Operate
ATT	Authorization to Test
CIO	Chief Information Officer
EPA	Environmental Protection Agency
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
GAO	Government Accountability Office
IA	Interconnection Agreement
IG	Inspector General
ISA	Interconnection Security Agreement
ISO	Information Security Officer
ISSO	Information System Security Officer
IT	Information Technology
MOU/MOA	Memorandum of Understanding/Memorandum of 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
REG	Risk Executive Group
SAISO	Senior Agency Information Security Official
SAOP	Senior Agency Official for Privacy
SAR	Security Assessment Report
SIA	Security Impact Analysis
SIO	Senior Information Official
SLA	Service Level Agreement
SO	System Owner
SP	Special Publication
SSP	System Security Plan
USC	United States Code

APPENDIX B: POA&M MONITORING AND VALIDATION PROCESS DIAGRAM AND OUTLINE

Figure 1: Process Flow Diagram

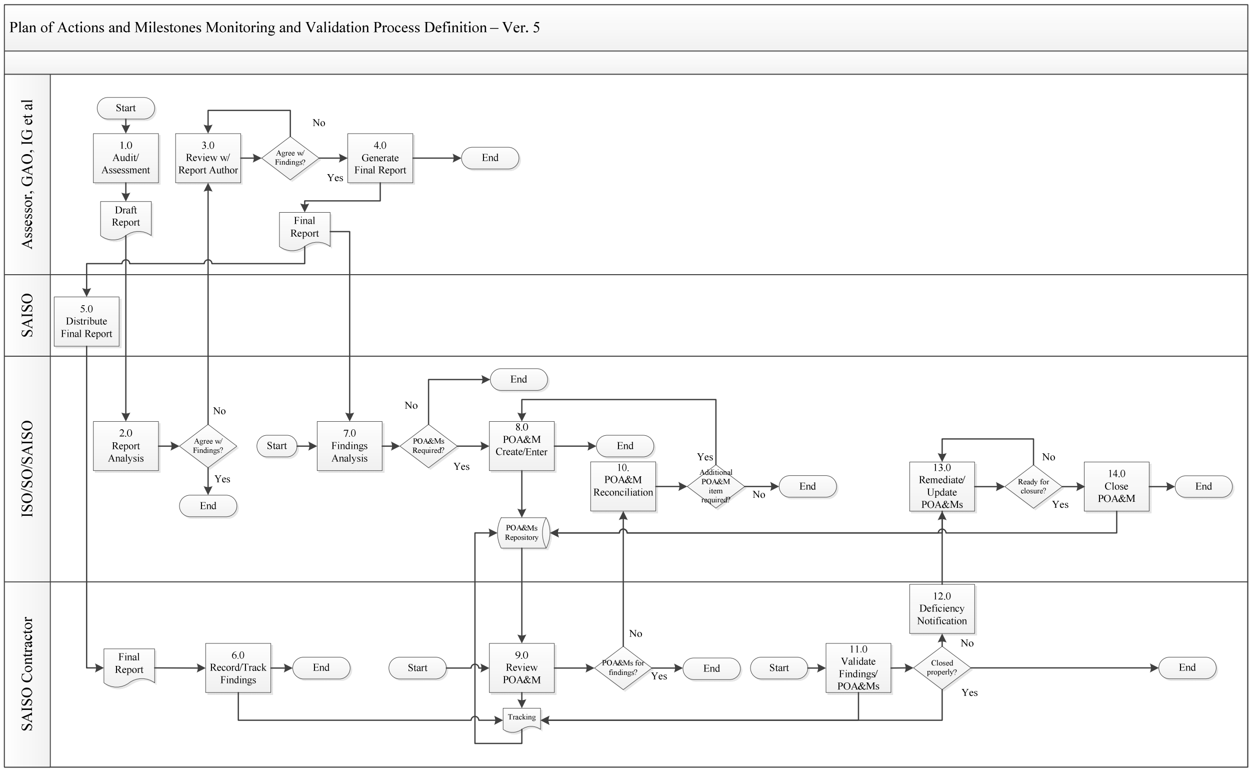

Table 1: Process Outline

1.0		**AUDIT/ASSESSMENT PROCESS**
	Input	Audit/Assessment target and objectives
	Process	Organization performs review of EPA program or regional office.
	Output	Draft report
2.0		**REPORT ANALYSIS**
	Input	Draft report
	Process	ISO/SO conducts analysis of audit/assessment findings and prepares a response.
	No	ISO/SO disagree with findings. Proceed to *Step 3.0, Review with Report Author*.
	Yes	ISO/SO agree with findings. Proceed to *Step 7.0, Findings Analysis.*
	Output	Decision on findings
3.0		**REVIEW WITH REPORT AUTHOR PROCESS**
	Input	ISO/SO initial decision on findings
	Process	ISO/SO and report authors review findings, iterative process until parties reach agreement.
	No	Disagree with findings. Repeat Step 3.0.
	Yes	Agree with findings. Proceed to *Step 4.0, Generate Final Report.*
	Output	Agreement on findings
4.0		**GENERATE FINAL REPORT**
	Input	Agreement on findings
	Process	Auditor/Assessor generates final report.
	Output	Final report
5.0		**DISTRIBUTION FINAL REPORT PROCESS**
	Input	Final report
	Process	SAISO determines destination of report received from auditor/assessor (SAISO Contractor or ISO/SO).
	Output	Audit/Assessment report
6.0		**RECORD/TRACK FINDINGS**
	Input	Final report
	Process	SAISO Contractor records final report findings for the purpose of tracking through resolution. [End]
	Output	Tracking list of findings
7.0		**FINDINGS ANALYSIS**
	Input	Final report

	Process	ISO/SO conducts analysis of findings and determines a disposition strategy.
	Yes	POA&M item is required. Proceed to *Step 8.0, POA&M Entry.*
	No	POA&M item is not required. [End]
	Output	Decision on requirement for a POA&M item
8.0		**POA&M Entry Process**
	Input	Decision from Step 7.0 and final report
	Process	ISO/SO enter findings in Agency POA&M repository to reflect decisions, final report findings, and outcome of reconciliation process. [End]
	Output	POA&M items
9.0		**Review POA&M Items**
	Input	POA&M items
	Process	SAISO Contractor conducts a review of the POA&M items to reconcile with outstanding audit/assessment findings.
	Yes	POA&M items found for audit/assessment findings. [End]
	No	POA&M items are absent for audit/assessment findings. Proceed to *Step 10.0, POA&M Reconciliation Process.*
	Output	Updates to tracking list
10.0		**POA&M Reconciliation Process**
	Input	Findings tracking list and POA&M items
	Process	ISO/SO and SAISO Contractor reconcile discrepancies between the number of audit/assessment findings and POA&M items.
	Yes	Additional POA&M items are required, repeat *Step 8.0, POA&M Entry.*
	No	Additional POA&M items are not required. [End]
	Output	Audit/Assessment findings are reconciled with POA&M items.
11.0		**Validate Findings/POA&M Process**
	Input	Audit/Assessment findings and POA&Ms
	Process	SAISO Contractor reviews audit/assessment findings and POA&Ms to determine if the all requirements have been adequately addressed.
	Yes	Items adequately addressed and can be closed. Tracking list updated accordingly.
	No	Items not adequately addressed. Proceed to *Step 12.0, Deficiency Notification.*
	Output	Deficiency notice of updates to tracking list
	Output	Training report
12.0		**Deficiency notification Process**
	Input	Findings from *Step 11.0, Validate Findings/POA&M Process*

	Process	SAISO Contractor notifies SAISO and respective ISO/SO of deficiency, with suggested plan of action for resolution. Proceed to *Step 13.0 Remediate Update POA&Ms.*
	Output	Plan of action
13.0		**Remediate/Update POA&Ms Process**
	Input	Plan of action
	Process	ISO/SO review plan of action provided by SAISO contractor's validation of findings/POA&Ms.
	Yes	Item ready for closure. Proceed to *Step 14.0, Close POA&M*.
	No	Item is not ready for closure. Repeat *Step 13.0, Remediate/Update POA&Ms Process.*
	Output	Updated POA&Ms
14.0		**Close POA&M Process**
	Input	Updated POA&Ms
	Process	ISO/SO ensures all required elements of POA&M items are complete and subsequently closes POA&M item. [End]
	Output	Closed POA&M items

APPENDIX C: SAOP ROLE AND NIST RISK MANAGEMENT FRAMEWORK

SAOP Responsibilities in the Risk Management Framework for Federal Information Systems

SAOP Responsibility	Description	Citation
Overall agency-wide responsibility for privacy	The SAOP has overall agency-wide responsibility and accountability for developing, implementing, and maintaining an organization-wide governance and privacy program to ensure compliance with all applicable laws, regulations, and policies regarding the collection, use, maintenance, dissemination, and disposal of PII by programs and information systems.	Appendix III, § 5(e)
Develop and maintain a privacy continuous monitoring strategy	The SAOP shall develop and maintain a privacy continuous monitoring strategy to address privacy risks and requirements across the organizational risk management tiers.	Appendix III, § 5(e)(1)
Establish and maintain a privacy continuous monitoring program	The SAOP shall establish and maintain a privacy continuous monitoring program to maintain ongoing awareness of privacy risks and assess privacy controls at a frequency sufficient to ensure compliance with applicable requirements and to adequately protect PII.	Appendix III, § 5(e)(2)
Review IT capital investment plans and budgetary requests	The SAOP shall review IT capital investment plans and budgetary requests to ensure that privacy requirements (and associated privacy controls), as well as any associated costs, are explicitly identified and included.	Appendix III, § 5(e)(3)

SAOP Responsibility	Description	Citation
Review and approve the categorization of systems	The SAOP shall review and approve, in accordance with NIST FIPS Publication 199 and Special Publication 800-60, the categorization of information systems that collect, process, store, maintain, or disseminate PII.	Appendix III, § 5(e)(4)
Designate privacy controls for systems	The SAOP shall designate system-specific, hybrid, and common privacy controls.	Appendix III, § 5(e)(5)
Review and approve the privacy plans for systems	The SAOP shall review and approve the privacy plans for organizational information systems prior to authorization, reauthorization, or ongoing authorization.	Appendix III, § 5(e)(6)
Conduct assessments of privacy controls for systems	The SAOP shall conduct privacy control assessments to ensure that privacy controls are implemented correctly, operating as intended, and effective in satisfying privacy requirements.	Appendix III, § 5(e)(7)
Review authorization packages for systems	The SAOP shall review authorization packages and determine that all applicable privacy requirements are met and the risk to PII is sufficiently addressed prior to authorizing officials making risk determination and acceptance decisions.	Appendix III, § 5(e)(8)
Maintain formal incident response capabilities	The SAOP shall maintain formal privacy incident response capabilities to include breach notification, shall implement formal privacy incident policies, and shall provide adequate training and awareness for	Appendix III, § 5(f)(1)-(3)

SAOP Responsibility	**Description**	**Citation**
	employees and contractors on how to report and respond to privacy incidents.	
Develop and maintain agency-wide privacy training	The SAOP shall develop and maintain mandatory agency-wide privacy training for all employees and contractors, including role-based training, and shall establish enforceable rules of behavior.	Appendix III, § 5(g)(1)-(8)