Information Security – Assessment, Authorization and Monitoring (CA) Procedure

Directive No: CIO 2150-P-04.3

Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19

Information Security – Assessment, Authorization and Monitoring (CA) Procedure

1. PURPOSE

The purpose of this procedure is to facilitate the implementation of Environmental Protection Agency (EPA) security control requirements for the Assessment, Authorization and Monitoring (CA) control family, as identified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organization*.

2. SCOPE

These procedures address all United States 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.

3. AUDIENCE

Senior Information Officials (SIO), Information Security Officers (ISO) and EPA System Owners (SO) or their official designees, for EPA-operated systems, and Service Managers (SM), for systems operated on behalf of the EPA, EPA employees, contractors and all other users of EPA information and systems.

4. BACKGROUND

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 security requirements by implementing the security controls defined in the NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*.

This document adopts procedures and standards for the EPA consistent with FIPS Publication 200.

5. AUTHORITY

Additional legal foundations for the Assessment, Authorization and Monitoring procedure include:

- Federal Information Security Modernization Act of 2014, Public Law 113-283, chapter 35 of title 44, United States Code (U.S.C.)
- OMB Circular A-130, "Managing Information as a Strategic Resource," Appendix I, Responsibilities for Protecting and Managing Federal Information Resources, July 2016
- EPA Information Security Policy
- EPA Roles and Responsibilities Procedures

6. PROCEDURE

SIO, ISO and EPA SO or their official designees for EPA-operated systems; and SM, for systems operated on behalf of the EPA and to the extent made applicable to their management of the system through a contract or other appropriate mechanism, are responsible for implementing the controls in this procedure. EPA is adopting this procedure agency-wide and expects these officials to develop a plan with timelines for adoption for their system(s). EPA employees, contractors and all other users of EPA information and information systems that support the operations and assets of the EPA should be aware of the content of this procedure and should follow the directions provided by SIO, ISO and EPA SO or their official designees and SM for the systems that they oversee.

The "CA" designator (e.g., CA-2, CA-3) identified for each procedure below corresponds to the NIST- identifier for the Assessment Authorization and Monitoring control family, as identified in NIST SP 800-53, Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations.

NIST defines the applicable CA security and privacy baseline controls in NIST 800-53B, Control Baselines for Information Systems and Organizations. The applicable security baseline for each impact level (Low, Moderate, High or For All Systems) as well as the Privacy Control Baseline are identified below the control name.

CA-2 – Control Assessments

For All Systems:

1) Select the appropriate assessor or assessment team for the type of assessment to be conducted;
2) Develop a control assessment plan that describes the scope of the assessment including:
   a) Controls and control enhancements under assessment;
   b) Assessment procedures to be used to determine control effectiveness; and
   c) Assessment environment, assessment team and assessment roles and responsibilities;
3) Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment;
4) Assess the security controls in the information system and its environment of operation annually or upon significant change to the system or environment 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 and privacy requirements;
5) Produce a control assessment report that document the results of the assessment; and
6) Provide the results of the control assessment to the ISO, Information System Security Officer (ISSO) and Office of Information Security and Privacy (OISP).

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

For Moderate and High Systems:

1) Employ independent assessors or assessment teams to conduct control assessments.

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

For High Systems:

1) Include as part of control assessments, annual, announced, penetration testing or other forms of testing to include but not limited to:
   a) Automated security test cases as feasible by the assessor;
   b) Vulnerability scanning;
   c) Malicious user testing;
   d) Performance and load testing;
   e) Data leakage or data loss assessment;
   f) Insider threat assessment; and
   g) System-specific requirements as identified by the Region or Program Office and must be documented in the System Security Plan (SSP) and Security Control Test Plan.

CA-3 – Information Exchange

For All Systems:

1) Approve and manage the exchange of information between the system and other systems using Interconnection Security Agreements (ISA); information exchange security agreements; Memoranda of Understanding or Agreement (MOU/A); or Service Level Agreements (SLA);
2) Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated; and
3) Review and update the agreements as agreed upon by the participating signatories but not to exceed three (3) years or whenever there is a significant change to any of the systems covered by the agreements.

CA-3(6) – Information Exchange | Transfer Authorizations

For High Systems

1) Verify that individuals or systems transferring data between interconnecting systems have the requisite authorizations (i.e., write permissions or privileges) prior to accepting such data.

CA-5 – Plan of Action and Milestones

For All Systems:

1) Develop a plan of action and milestones for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and
2) Update existing plan of action and milestones monthly based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities.

CA-6 – Authorization

For All Systems:

1) Assign a senior official as the authorizing official for the system;
2) Assign a senior official as the authorizing official for common controls available for inheritance by organizational systems;
3) Ensure that the authorizing official for the system, before commencing operations:
   a) Accepts the use of common controls inherited by the system; and
   b) Authorizes the system to operate;
4) Ensure that the authorizing official for common controls authorizes the use of those controls for inheritance by organizational systems;
5) Update the authorizations at least every three (3) years or upon a significant change to the system or operating environment.

CA-7 – Continuous Monitoring

For All Systems:

1) Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy that includes:
   a) Establishing the following system-level metrics to be monitored:
      i) Number of open or unremediated vulnerabilities;
      ii) Number of unremediated findings;
      iii) Number of open plan of action and milestones;
      iv) Number of past due vulnerability remediations;
      v) Number of past due plan of action and milestones; and
      vi) Date of last contingency plan test, SSP review, incident response plan testing, and configuration management plan review;
   b) Establishing monthly for monitoring and annually for assessment of control effectiveness;

c) Ongoing control assessments in accordance with the continuous monitoring strategy;
d) Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy;
e) Correlation and analysis of information generated by control assessments and monitoring;
f) Response actions to address results of the analysis of control assessment and monitoring information; and
g) Reporting the security and privacy status of the system to the EPA CISO annually, after a significant change to the system or operating environment, or a reported significant cybersecurity incident.

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

For Moderate and High Systems:

1) Employ independent assessors or assessment teams to monitor the controls in the system on an ongoing basis.

CA-7(4) – Continuous Monitoring | Risk Monitoring

For All Systems:

1) Ensure risk monitoring is an integral part of the continuous monitoring strategy that includes the following:
   a) Effectiveness monitoring;
   b) Compliance monitoring; and
   c) Change monitoring.

CA-8 – Penetration Testing

For High Systems:

1) Conduct penetration testing annually on FIPS 199 categorized 'High' systems and High Value Assets (HVA).

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

For High Systems:

1) Employ an independent penetration testing agent or team to perform penetration testing on the system or system components.

CA-9 – Internal System Connections

For All Systems:

1) Authorize internal connections of devices or system components (examples include mobile devices, laptops and desktop computers, tablets, printers, card readers, scanners, sensors, or other IT related components) to the system;
2) Document, for each internal connection, the interface characteristics, security and privacy requirements and the nature of the information communicated;

3) Terminate internal system connections after exposure to certain security events or when no longer needed to meet mission or business requirements; and
4) Review annually the continued need for each internal connection.

7. ROLES AND RESPONSIBILITIES

The Information Security – Roles and Responsibilities procedure provides roles and responsibilities for personnel who have IT security or related governance responsibility for protecting the information and information systems they operate, manage and support.

8. RELATED INFORMATION

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

9. DEFINITIONS

- **Authorizing Official (AO)** – defined in the EPA as the Senior Information Official; (i) a senior agency official or executive 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 is 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) in a management position 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.
- **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.
- **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, 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).
- **Significant Change** – a change that is likely to substantively affect the security or privacy posture of a system.
- **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 the 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 or deviations may be requested through the EPA Risk Determination Process based on a substantive business need and the implementation of compensating controls that provide a suitable alternative to the mandated protection.

Only EPA's Chief Information Officer may authorize Agency-wide waivers or deviations from the standards herein.

11. MATERIAL SUPERSEDED

Information Directive: CIO 2150-P-04.2, Information Security – Security Assessment and Authorization Procedures.

12. CONTACTS

For further information, please contact the Office of Mission Support (OMS), Office of Information Security and Privacy (OISP).

VAUGHN NOGA

Digitally signed by VAUGHN NOGA
Date: 2023.06.08 08:03:36 -04'00'

Vaughn Noga
Deputy Assistant Administrator for Environmental Information and Chief Information Officer
U.S. Environmental Protection Agency

APPENDIX A: ACRONYMS & ABBREVIATIONS

AO	Authorizing Official
CIO	Chief Information Officer
CISO	Chief Information Security Official
EPA	Environmental Protection Agency
FIPS	Federal Information Processing Standards
ISA	Interconnection Security Agreement
ISO	Information Security Officer
MOU/A	Memorandum of Understanding or Agreement
NIST	National Institute of Standards and Technology
OISP	Office of Information Security and Privacy
OMB	Office of Management and Budget
OMS	Office of Mission Support
POA&M	Plan of Action and Milestones
REG	Risk Executive Group
SIO	Senior Information Official
SO	System Owner
SP	Special Publication
U.S.C.	United States Code