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

Information Security – Audit and Accountability (AU) Procedures

1. PURPOSE

The purpose of this procedure is to facilitate the implementation of Environmental Protection Agency (EPA) security control requirements for the Audit and Accountability (AU) 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 Organizations.*

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 Audit and Accountability procedure include:

- Federal Information Security Modernization Act (FISMA) of 2014, Public Law 113-283, chapter 35 of title 44, United States Code (U.S.C.)
- OMB Circular A-130, “Managing Federal Information as a Strategic Resource,” Appendix I, “Responsibilities for Protecting and Managing Federal Information

Resources" July 2016

- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006
- OMB M-21-31, "Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents" August 2021
- 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 "AU" designator (e.g., AU-2, AU-3) identified for each procedure below corresponds to the NIST- identifier for the Audit and Accountability 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 AU 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.

AU-2 – Event Logging

For All Systems and Privacy Control Baseline:

1) Identify the types of events that the system is capable of logging in support of the audit function: all event types that are significant and relevant to the security of systems and the privacy of individuals and that provide the ability to establish, correlate, and investigate events relating to an incident or identify those responsible for one;
2) Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;
3) Specify the following event types for logging within the system: all applicable event types identified in Appendix C of OMB M-21-31;
4) Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and

5) Review and update the event types selected for logging annually or when there are significant changes in federal directives, Agency policies or procedures, or the threat environment.

AU-3 – Content of Audit Records

For All Systems:

1) Ensure that audit records contain information that establishes the following:
   a) What type of event occurred;
   b) When the event occurred;
   c) Where the event occurred;
   d) Source of the event;
   e) Outcome of the event; and
   f) Identity of any individuals, subjects, or objects/entities associated with the event.

AU-3(1) – Content of Audit Records | Additional Audit Information

For Moderate and High Systems:

1) Generate audit records containing the following additional information:
   a) Manufacturer-specific event name/type;
   b) Source and destination port and/or protocol information; and
   c) Individual identities of users that use shared/group accounts.

AU-3(3) – Content of Audit Records | Limit Personally Identifiable Information Elements

For Privacy Control Baseline:

1) Limit personally identifiable information contained in audit records to the following elements identified in the privacy risk assessment: personally identifiable information (PII) elements are not authorized to be contained within audit records.

AU-4 – Audit Log Storage Capacity

For All Systems:

1) Allocate audit log storage capacity to accommodate EPA Records Schedules retention requirements but at a minimum must comply with OMB M-21-31.

AU-5 – Response to Audit Logging Process Failures

For All Systems:

1) Alert the network, system, or application administrator within two (2) minutes in the event of an audit logging process failure; and
2) Take the following additional actions: overwrite oldest audit records for those systems

which are configured to offload audit logs to a separate system such as the Enterprise Log Management System or shut down the information system when audit records are not offloaded to a separate system. Actions taken must comply with OMB M-21-31 or subsequent revisions.

AU-5(1) – Response to Audit Logging Processing Failures | Storage Capacity Warning

For High Systems:

1) Provide a warning to the network, system, or application administrator, the ISO and the ISSO within two (2) minutes when allocated audit log storage volume reaches 70%, 80%, 90% and 100% of repository maximum audit log storage capacity.

AU-5(2) – Response to Audit Logging Processing Failures | Real-time Alerts

For High Systems:

1) Provide an alert within near real-time to the network, system, or application administrator, the ISO and the ISSO when the following audit failure events occur: the system experiences a failure to forward audit logs to a separate system such as the Enterprise Log Management System, a failure to generate audit logs, and when audit logs are overwritten.

AU-6 – Audit Record Review, Analysis, and Reporting

For All Systems:

1) Review and analyze system audit records at least weekly or as required for indications of compromise, inappropriate or unusual activity and the potential impact of the inappropriate or unusual activity;
2) Report findings to the EPA Enterprise Service Desk (EISD), the ISO, the ISSO, and the Liaison Privacy Official (LPO) as needed when privacy systems are impacted; and
3) Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible source of information.

AU-6(1) – Audit Record Review, Analysis, and Reporting | Automated Process Integration

For Moderate and High Systems:

1) Integrate audit record review, analysis, and reporting processes using automated mechanisms.

AU-6(3) – Audit Record Review, Analysis, and Reporting | Correlate Audit Repositories

For Moderate and High Systems:

1) Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.

AU-6(5) – Audit Record Review, Analysis, and Reporting | Integrated Analysis of Audit Records

For High Systems:

1) Integrate analysis of audit records with analysis of vulnerability scanning information; performance data; system monitoring information; maintenance logs; intrusion prevention systems; and appropriate network infrastructure logs to further enhance the ability to identify inappropriate or unusual activity.

AU-6(6) – Audit Record Review, Analysis, and Reporting | Correlation with Physical Monitoring

For High Systems:

1) Correlate information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.

AU-7 – Audit Record Reduction and Report Generation

For Moderate and High Systems:

1) Provide and implement an audit record reduction and report generation capability that:
   a) Supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations of incidents; and
   b) Does not alter the original content or time ordering of audit records.

AU-7(1) – Audit Record Reduction and Report Generation | Automatic Processing

For Moderate and High Systems:

1) Provide and implement the capability to process, sort, and search audit records for events of interest based on the following content: system resources involved, objects or information accessed, identities of individuals, event types, event locations, event dates and times, Internet Protocol (IP) addresses involved, or event success or failure.

AU-8 – Time Stamps

For All Systems:

1) Use internal system clocks to generate time stamps for audit records; and

2) Record time stamps for audit records that meet OMB M-21-31 requirements and that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.

AU-9 – Protection of Audit Information

For All Systems:

1) Protect audit information and audit logging tools from unauthorized access, modification, and deletion; and
2) Alert the ISO, ISSO and the EISD upon detection of unauthorized access, modification, or deletion of audit information.

AU-9(2) – Protection of Audit Information | Store on Separate Physical Systems or Components

For High Systems:

1) Store audit records in near real-time in a repository that is part of a physically different system or system component than the system or component being audited.

AU-9(3) – Protection of Audit Information | Cryptographic Protection

For High Systems:

1) Implement cryptographic mechanisms to protect the integrity of audit information and audit tools.

AU-9(4) – Protection of Audit Information | Access by Subset of Privileged Users

For Moderate and High Systems:

1) Authorize access to management of audit logging functionality to only personnel assigned with audit-related privileges by the SO.

AU-10 – Non-repudiation

For High Systems:

1) Provide irrefutable evidence that an individual (or process acting on behalf of an individual) has performed all actions associated with that user or process.

AU-11 – Audit Record Retention

For All Systems and Privacy Control Baseline:

1) Retain audit records in accordance with EPA Records Schedules but at a minimum to meet the requirements of OMB M-21-31 or subsequent revisions to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements.

AU-12 – Audit Record Generation

For All Systems:

1) Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2(1) on: system, device, and application components defined in OMB M-21-31;
2) Allow ISO, ISSO or personnel assigned by the SO to select the event types that are to be logged by specific components of the system; and
3) Generate audit records for the event types defined in AU-2 3) that include the audit record content defined in AU-3.

AU-12(1) – Audit Record Generation | System-wide and Time-correlated Audit Trail

For High Systems:

1) Compile audit records from system components into a system-wide (logical or physical) audit trail that is time-correlated to comply with OMB M-21-31.

AU-12(3) – Audit Record Generation | Changes by Authorized Individuals

For High Systems:

1) Provide and implement the capability for network, system, or application administrators or personnel assigned by the SO to change the logging to be performed on system components based on security, threat, or business requirements within thirty (30) minutes.

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

The information listed below relates to the Audit and Accountability Procedure:

- NIST Special Publications, 800 Series
- Related standards and guidelines are available on the OMS website

9. DEFINITIONS

- **Appropriate Technical and Management Personnel** – individuals responsible for the resources needed and required to track the access attempt through the telecommunications network and the system.
- **Audit Processing Failures** – includes software/hardware errors, failures in the audit

capturing mechanisms, and audit storage capacity being reached or exceeded.

- **Audit Reduction** – includes using tools and techniques that reduce audit data in order to save storage space and to extract more useful, higher-level data for the review process.
- **Availability** – ensuring timely and reliable access to, and use of, information.
- **Incident** – an occurrence that actually or potentially jeopardizes the confidentiality, integrity or availability of an information system, or the information the system processes, stores or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures or acceptable use policies.
- **Information** – an instance of an information type.
- **Information Security** – the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction in order to provide confidentiality, integrity and availability.
- **Information Security Policy** – an aggregate of directives, regulations, rules and practices that prescribe how an organization manages, protects and distributes information.
- **Information System** – a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information.
- **Media** – physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration (LSI) memory chips, printouts (but not including display media) onto which information is recorded, stored or printed within an information system. Digital media include diskettes, tapes, removable hard drives, flash/thumb drives, compact disks, digital video disks. Examples of non-digital media are paper or microfilm. This term also applies to portable and mobile computing and communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones).
- **Organization** – a federal agency or, as appropriate, any of its operational elements.
- **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.
- **Records** – the recordings of evidence of activities performed or results achieved (e.g., forms, reports, test results) which serve as the basis for verifying that the organization and the information system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items).
- **User** – individual or (system) process authorized to access an information system.
- **Written** (or in writing) – means 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-03.3, Information Security – Audit and Accountability 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 08:04:51 -04'00'

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

APPENDIX A: ACRONYMS AND ABBREVIATIONS

AU	Audit and Accountability
CISO	Chief Information Security Officer
FIPS	Federal Information Processing Standards
GRS	General Records Schedules
ISO	Information Security Officer
ISSO	Information System Security Officer
LSI	Large-Scale Integration
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
OISP	Office of Information Security and Privacy
OMB	Office and Management and Budget
OMS	Office of Mission Support
SA	System Administrator
SO	System Owner
SP	Special Publication
U.S.C.	United States Code