INFORMATION PROCEDURE

Information Security – Audit and Accountability Procedures			
EPA Classification No.:	CIO-2150-P-3.2	CIO Approval Date:	09/28/2015
CIO Transmittal No.:	16-001	Review Date:	09/28/2018

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

INFORMATION SECURITY – AUDIT AND ACCOUNTABILITY PROCEDURES

1. PURPOSE

To implement the 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 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

2. SCOPE AND APPLICABILITY

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

The procedures apply to all EPA employees, contractors, and all other users of EPA information and information systems that support the operations 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 that all offices within the Agency meet the minimum security requirements defined in the *Federal Information Processing Standards* (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*. All EPA information systems shall meet 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 Audit and Accountability 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, to amend 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 U.S.C. 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-06-16, "Protection of Sensitive Agency Information," June 2006
- OMB Circular A-130, "Management of Federal Information Resources," Appendix III, "Security of Federal Information Resources," November 2000
- Federal Information Processing Standards (FIPS) 140-2, Security Requirements for Cryptographic Modules, May 2001
- FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006
- EPA Information Security Program Plan
- EPA Information Security Policy
- EPA Roles and Responsibilities Procedures
- EPA Information Security Continuous Monitoring Strategic Plan
- CIO Policy Framework and Numbering System

6. PROCEDURES

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

Abbreviations including acronyms are summarized in Appendix A.

AU-2 – Audit Events

For All Information Systems:

1) System Owners (SO), in coordination with Information Owners (IO), for EPA-operated systems, shall; and Service Managers (SM), in coordination with IOs, for systems operated on behalf of the EPA[1], shall ensure service providers:
   a) Configure information systems to audit for the following events:
      i) The following events shall be identified within server audit logs:
         (1) Server startup and shutdown
         (2) Loading and unloading of services
         (3) Installation and removal of software
         (4) System alerts and error messages
         (5) User logon and logoff
         (6) System administration activities
         (7) Accesses to sensitive information, files, and systems
         (8) Account creation, modification, or deletion
         (9) Modifications of privileges and access controls
         (10) Additional security-related events, as required by the SO or to support the nature of the supported business and applications
      ii) The following events shall be identified within application and database audit logs:
         (1) Modifications to the application
         (2) Application alerts and error messages
         (3) User logon and logoff
         (4) System administration activities
         (5) Accesses to information and files
         (6) Account creation, modification, or deletion
         (7) Modifications of privileges and access controls
      iii) The following events shall be identified within network device (e.g., router, firewall, switch, wireless access point) audit logs:
         (1) Device startup and shutdown
         (2) Administrator logon and logoff
         (3) Configuration changes
         (4) Account creation, modification, or deletion
         (5) Modifications of privileges and access controls
         (6) System alerts and error messages

[1] [1] *Information Owners and Service Managers shall follow FedRAMP requirements for all services obtained where EPA information is transmitted, stored, or processed on non-EPA operated systems.*

b) Configure audit logging for desktops in accordance with United States Government Configuration Baseline (USGCB) requirements.

c) Coordinate the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events.

d) Provide rationale as to why the list of auditable events is deemed adequate to support after-the-fact investigations of security incidents.

e) Configure the information system to be able to adjust depth and breadth of audit logging capabilities to allow for an increase and decrease of these capabilities based on current threat information and ongoing assessment of risk.

AU-2 (1) – Audit Events | Compilation of Audit Events from Multiple Sources

Incorporated into AU-12.

AU-2 (2) – Audit Events | Selection of Audit Events by Component

Incorporated into AU-12.

For FedRAMP[2] Moderate Information Systems:

1) SMs, in coordination with IOs, for systems operated on behalf of the EPA,[3] shall ensure service providers:
   a) Verify that the information system backs up audit records weekly onto a different system or media than the system being audited.
   b) Review and update audited events annually, or when there is a change in the threat environment.
      i) The Senior Agency Security Officer (SAISO) shall communicate changes in the threat environment.

AU-2 (3) – Audit Events | Reviews and Updates for Moderate and High Information Systems:

1) SOs, in coordination with IOs, for EPA-operated systems, shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Review and update the list of the auditable events annually, or when a major change to the information system occurs.
      i) When operating in an environment of increased risk, based on current threat information, the list shall be reviewed on a monthly basis as a minimum.

.

[2] *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.*

[3] *Information Owners and Service Managers shall follow FedRAMP requirements for all services obtained where EPA information is transmitted, stored, or processed on non-EPA operated systems.*

ii) The list of events to be audited by the information system shall include the execution of privileged functions.

For FedRAMP Moderate Information Systems:

1) SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Review and update audited events at least annually, or whenever changes occur within the threat environment.
      i) The SAISO shall communicate changes in the threat environment to the service provider.

AU-2 (4) – Audit Events | Privileged Functions

Incorporated into AC-6 (9)

AU-3 – Content of Audit Records For All Information Systems:

1) SOs, in coordination with IOs, for EPA-operated systems, shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Configure information systems to generate audit records containing sufficient information to establish what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. At a minimum, the following elements shall be identified within each audit record:
      i) Date and time when the event occurred
      ii) The software or hardware component of the information system where the event occurred
      iii) Source of the event (e.g., network address, console)
      iv) Type of event that occurred
      v) Subject identity (e.g., user, device, process context)
      vi) The outcome (i.e., success or failure) of the event
      vii) Security-relevant actions associated with processing

AU-3 (1) – Content of Audit Records | Additional Audit Information For Moderate and High Information Systems:

1) SOs, in coordination with IOs, for EPA-operated systems, shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Configure information systems to generate audit records containing the following additional elements:
      i) Manufacturer-specific event name / type of event
      ii) Source and destination network addresses

iii) Source and destination port or protocol identifiers

iv) Outcome of the event

v) Identity of the user/subject associated with the event

Note: EPA requires information systems, when system functionality permits, to include more detailed information in the audit records. The detailed information that shall be included may be defined as significant system events or risks.

AU-3 (2) – Content of Audit Records | Centralized Management of Planned Audit Record Content

For High Information Systems:

1) SOs, in coordination with IOs, for EPA-operated systems, shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Manage the content of audit records generated by defined information system components centrally.

AU-4 – Audit Storage Capacity For All Information Systems:

1) SOs, in coordination with IOs, for EPA-operated systems, shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Comply with EPA Records Schedule 1012, *Information and Technology Management* for the disposition of historically significant and routine IT management records.
      i) EPA Records Schedule 1012 excludes Information Technology (IT) management logs and records for specific, individual systems (e.g. AQS, CERCLIS), which must be scheduled separately, in coordination with the SAISO and associated SOs, IOs, and SMs, for systems operated on behalf of the EPA.
      ii) EPA Records Schedule is found at http://www.epa.gov/records/policy/schedule/sched/1012.htm

AU-4 (1) – Audit Storage Capacity | Transfer to Alternate Storage

Not selected as part of the control baseline.

AU-5 – Response to Audit Processing Failures For All Information Systems:

1) SOs, in coordination with IOs, for EPA-operated systems, shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Configure the information system to alert designated officials in the event of an audit failure or when audit capacity is 70%, 80%, and again at 90% utilization automatically. This alert should be distributed by a mechanism that allows system administrators to receive it at any time including after normal working hours (e.g., email, text message).
      i) Once the maximum storage capacity for audit logs is reached or there is an audit failure, the information system shall overwrite the oldest audit records or automatically

shut down in an effort to eliminate the chance of an incident, in the absence of auditing and accountability.

ii) When devices cannot generate logs, the information system should be configured to send an alert to system administrators within 2 minutes. Procedures should reflect escalation of priority resolution actions after 24 hours for high information systems.

AU-5 (1) – Response to Audit Processing Failures | Audit Storage Capacity For High Information Systems:

1) SOs, in coordination with IOs, for EPA-operated systems, shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Configure information systems to provide a warning to designated officials (to include the system administrator(s), ISSO, ISO and SO) within two minutes when allocated audit record storage volume reaches 70%, 80%, 90% and 100% of repository maximum audit record storage capacity. At 90% and 100% of maximum audit record storage capacity, alerts shall be sent to the SO, ISO and ISSO by the system. Procedures should reflect escalation of priority resolution actions after 24 hours for high-value systems.

AU-5 (2) – Response to Audit Processing Failures | Real-Time Alerts For High Information Systems:

1) SOs, in coordination with IOs, for EPA-operated systems, shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers: a)
   Configure information systems to provide an alert within two minutes to System Administrators (SAs), ISSOs, ISOs, and SOs when the system experiences a failure to write to audit logs or overwrite old logs.

AU- 5 (3) – Response to Audit Processing Failures | Configurable Traffic Volume Thresholds

Not selected as part of the security control baseline.

AU- 5 (4) – Response to Audit Processing Failures | Shutdown on Failure

Not selected as part of the security control baseline.

AU - 6 – Audit Review, Analysis, and Reporting For All Information Systems:

1) SOs, in coordination with IOs, for EPA-operated systems, shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Review and analyze audit logs and records weekly for the following:
      i) Indications of inappropriate or unusual activity.
      ii) Assurance that logging is functioning properly
      iii) Adherence to logging standards identified in this procedure.

b) Adhere to the following review and analysis requirements:
   i) Logs on critical systems shall be reviewed daily.
   ii) The level of audit review, analysis, and reporting may be adjusted if there is a change in risk to organizational operations, assets, or personnel. Adjustments shall be based upon advisories and warnings such as those provided by the National Terrorism Advisory System, or EPA internal advisory mechanisms.
   iii) Logs for firewalls, routers, and other network devices shall be time-correlated (to within 30 seconds) with logs of other critical systems and examined daily to determine if any incidents have occurred.
   iv) All other logs, including access server logs, shall be reviewed weekly.
   v) Logs identifying Personally Identifiable Information (PII) access and extracts shall be reviewed monthly.
      (1) For information systems containing PII, the monthly review of audit logs will assist in determining what data extracts shall be deleted.

c) Review audit logs for logons, logoffs, and accesses to system weekly.

d) Ensure all staff involved with log management responsibilities are trained on how to review and analyze audit logs, and how to report incidents when applicable.
   i) Personnel performing the review shall have the level of background screening equivalent to the information system's sensitivity.

e) Ensure personnel report findings to Information Security Officers (ISOs).
   i) ISOs shall promptly report findings to EPA Computer Security Incident Response Capability (CSIRC), which may escalate the incident to United States Computer Emergency Readiness Team (US-CERT).
      (1) CSIRC may notify law enforcement about the incident.
   ii) The appropriate actions, including notification of local legal counsel, the Office of Inspector General (OIG), and local and federal law enforcement officials shall be coordinated when investigations reveal that the incident is a prosecutable offense under statutes.
   iii) Additionally, anomalies shall be reported in accordance with EPA incident reporting requirements and procedures.
      (1) Refer to the EPA Information Security –Incident Response Procedures for requirements on incident reporting.
   iv) If the investigation reveals an exploitable system or procedural vulnerability, coordination shall occur between the appropriate management and technical personnel to ensure that the vulnerability is addressed.

AU-6 (1) – Audit Review, Analysis and Reporting | Process Integration For Moderate and High Information Systems:

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

a) Employ automated mechanisms to integrate audit review, analysis, and reporting processes to support EPA processes[4] for investigation and response to suspicious activities.

For FedRAMP Moderate Information Systems:

1) SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Employ automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.
   b) Analyze and correlate audit records across different audit repositories to gain situational awareness.

AU-6 (2) – Audit Review, Analysis and Reporting | Automated Security Alerts

Incorporated into SI-4.

AU-6 (3) – Audit Review, Analysis and Reporting | Correlate Audit Repositories For Moderate and High Information Systems:

1) SOs, in coordination with IOs, for EPA-operated systems, shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Analyze and correlate audit records across different repositories to gain EPA-wide situational awareness across all three tiers of risk management (i.e., organizational, mission/business process, and information system).

For FedRAMP Moderate Information Systems:

1) SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Analyze and correlate audit records across different repositories to gain EPA-wide situational awareness.

AU-6 (4) – Audit Review, Analysis and Reporting | Central Review and Analysis

Not selected as part of the security control baseline.

AU-6 (5) – Audit Review, Analysis and Reporting | Scanning and Monitoring Capabilities For High Information Systems:

1) SOs, in coordination with IOs, for EPA-operated systems, shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Integrate analysis of audit records with analysis of vulnerability scan information, performance data, information system and insider threats monitoring information, monitoring information from scanning and Intrusion Detection and Prevention System

[4] [4] *EPA processes benefiting from integrated audit review, analysis, and reporting include, for example, incident response, continuous monitoring, contingency planning, and Inspector General audits.*

(IDPS) tools, and data/information collected from other sources to enhance the ability to identify inappropriate or unusual activity further.

AU-6 (6) – Audit Review, Analysis and Reporting | Correlation with Physical Monitoring For High Information Systems:

1) SOs, in coordination with IOs, for EPA-operated systems, shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Correlate information from audit records with information obtained from monitoring physical access to enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity further.

AU-6 (7) – Audit Review, Analysis and Reporting | Permitted Actions

Not selected as part of the security control baseline.

AU-6 (8) – Audit Review, Analysis and Reporting | Full Text Analysis of Privileged Commands

Not selected as part of the security control baseline.

AU-6 (9) – Audit Review, Analysis and Reporting | Correlation with Information from Non-technical Sources

Not selected as part of the security control baseline.

AU-6 (10) – Audit Review, Analysis and Reporting | Audit Level Adjustment

Not selected as part of the security control baseline.

AU-7 – Audit Reduction and Report Generation For Moderate and High Information Systems:

1) SOs, in coordination with IOs, for EPA-operated systems, shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Configure the information system to provide an audit reduction[5] and report generation capability that:
      i) Supports near real-time audit review, analysis, and reporting requirements described in AU-6 and after-the-fact investigations of security incidents; and
      ii) Does not alter the original content or time recording of audit records.

[5] [5] *Audit reduction includes using tools and techniques that reduce audit data in order to save storage space and to extract more useful and readable data for the review process.*

AU-7(1) – Audit Reduction and Report Generation | Automatic Processing For Moderate and High Information Systems:

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

a) Employ automated tools to review audit records. The following audit analysis tools may be used:

i) Audit analysis tools based on attack signature, variance techniques, and audit reduction methodologies to detect intrusion

ii) Data reduction audit tools to help reduce the amount of information contained in audit records, as well as to distill useful information from the raw data

iii) Query applications that have the ability to query an audit log by username, location, application name, date, and time, or other applicable parameters; and have the ability to execute reports with the results of the query

b) Ensure information systems provide the capability to process audit records for events of interest based on selectable event criteria including event types, event locations, event times, event dates, system resources involved, IP addresses involved, or information objects accessed.

AU-7(2) – Audit Reduction and Report Generation | Automatic Sort and Search

Not selected as part of the security control baseline.

AU-8 – Time Stamps

For All Information Systems:

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

a) Configure information systems to use internal system clocks to generate time stamps for audit records.

i) Time stamps generated by the information system shall include both the date and time.

b) Configure information systems to record time stamps that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets thirty (30) seconds accuracy (i.e., the degree of synchronization between information system clocks and reference clocks).

AU-8(1) – Time Stamps | Synchronization with Authoritative Time Source For Moderate and High Information Systems:

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

a) Configure information systems to synchronize internal information system clocks at least daily with EPA's defined authoritative time source to ensure that time stamps in audit

records are as accurate as possible and correlated across different systems or system components. EPA time sources will synchronize to stratum 1 Network Time Protocol (NTP) servers.

b) Configure information systems to synchronize the internal system clocks to the authoritative time source when the time difference is greater than 30 seconds.

For FedRAMP Moderate Information Systems:

1) SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Ensure the information system is configured to compare the internal information system clocks with primary and secondary timeservers used by the NIST Internet time service using NTP.
      i) The secondary server is selected from a different geographic region than the primary server; the service provider synchronizes the system clocks of network computers that run operating systems other than Windows to the Windows Server Domain Controller emulator or to the same time source for that server.
   b) Synchronize the internal system clocks to the authoritative time source when the time difference is greater than 30 seconds.

AU-8 (2) – Time Stamps | Secondary Authoritative Time Source

Not selected as part of the security control baseline

AU-9 – Protection of Audit Information For All Information Systems:

1) SOs, in coordination with IOs, for EPA-operated systems, shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Protect audit information[6] and audit tools from unauthorized modification, access, or destruction while online and during offline storage.
   b) Rotate log files to a system other than their source system

AU-9 (1) – Protection of Audit Information | Hardware Write-Once Media

Not selected as part of the security control baseline.

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

For High Information Systems:

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

[6] *Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity.*

a) Configure information systems to back up audit records nightly onto a physically different system or system component than the system or component being audited.

For FedRAMP Moderate Information Systems:

3) SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Ensure the information system backs up audit records onto a physically different system or system component than the system or component being audited at least weekly.

AU-9(3) – Protection of Audit Information | Cryptographic Protection For High Information Systems:

1) SOs, in coordination with IOs, for EPA-operated systems, shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Implement cryptographic[7] mechanisms on information systems 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 Information Systems:

1) SOs, in coordination with IOs, for EPA-operated systems, shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Authorize access to management of audit functionality to only SOs, authorized system administrators, and the designated security officials.

AU-9 (5) – Protection of Audit Information | Dual Authorization

Not selected as part of the security control baseline.

AU-9 (6) – Protection of Audit Information | Read-Only Access

Not selected as part of the security control baseline.

AU-10 – Non-repudiation

For High Information Systems:

1) SOs, in coordination with IOs, for EPA-operated systems, shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Configure information systems to protect against an individual (or a process acting on behalf of an individual) falsely denying having performed a particular action.
      i) Actions covered by non-repudiation includes, for example, creating information, sending and receiving messages, approving information (e.g., indicating concurrence or signing a contract).

[7] *All cryptography is expected to be implemented using FIPS 140-2 validated modules in FIPS mode.*

For FedRAMP Moderate Information Systems:

4) SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Verify that the information system protects against an individual falsely denying having performed a specific action (e.g., non-repudiation).
   b) Employ only FIPS-140-2 validated cryptography to implement digital signatures.

AU-10 (1) – Non-repudiation | Association of Identities

Not selected as part of the security control baseline.

AU-10 (2) – Non-repudiation | Validate Binding of Information Producer Identity

Not selected as part of the security control baseline.

AU-10 (3) – Non-repudiation | Chain of Custody

Not selected as part of the security control baseline.

AU-10 (4) – Non-repudiation | Validate Binding of Information Viewer Identity

Not selected as part of the security control baseline.

AU-10 (5) – Non-repudiation | Digital Signatures

Not selected as part of the security control baseline.

AU-11 – Audit Record Retention For All Information Systems:

1) SOs, in coordination with IOs, for EPA-operated systems, shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Retain audit records to provide support for after-the-fact investigations of IT security incidents and to meet regulatory and organizational information retention requirements.
      i) These records include system, application, and database-level audit logs and logs for network devices.
   b) Retain all audit information and records in accordance with the following:
      i) The records schedule found in EPA Records Schedule 1012 – Information and Technology Management.
      ii) The records retention policy provided by the National Archives and Records Administration (NARA) General Records Schedules (GRS).
   c) Archive audit records for a period of no less than one (1) year with 90 days online and the remaining time stored offline.
   d) Transfer audit records for remote access devices from the devices to a central log server where they are retained for up to three (3) years.

i) After being retained on the central log server for three (3) years, they will be retained in accordance with the records schedule found in *EPA Records Schedule* 1012 – *Information and Technology Management*.

e) Maintain audit records associated with known incidents, including those used for legal action, in accordance with the records schedule found in *EPA Records Schedule 1012 – Information and Technology Management*, after the incident is closed.

f) Dispose of audit records when the retention time has expired, as detailed in this procedure, in accordance with the records schedule found in *EPA Records Schedule 1012 – Information and Technology Management*.

i) Refer to the EPA Information Security – Media Protection Procedures for requirements on media disposal.

g) Ensure the following requirements are met for information systems containing PII and Confidential Business Information (CBI):

i) A usage policy shall be established and implemented by the SO, in coordination with the EPA Privacy Officer, which identifies authorized computer-readable extracts that are needed for more than 90 days.

ii) The information system shall be configured to log sensitive PII and CBI-related accesses and extracts.

iii) The logs shall be reviewed and analyzed to identify all extracts containing sensitive PII and CBI.

iv) All computer-readable data extracts containing PII or CBI shall be erased or deleted within 90 days if the extract is not explicitly authorized by the 90-day usage policy or its use shall be documented as still being required.

v) For PII data protection measures, refer to Office of Management and Budget (OMB) 07-16 – *Safeguarding information maintained by the United States Government*. For protection and disclosure of CBI data, refer to Code of Federal Regulations (CFR), Title 40, Part II, Subpart B.

AU-11 (1) – Audit Record Retention | Long-term Retrieval Capability

Not selected as part of the security control baseline.

AU-12 – Audit Generation

For All Information Systems:

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

a) Configure information systems to provide audit record generation capability for the list of auditable events defined in AU-2 with content prescribed in AU-3 on, *at a minimum*, the following information system components:

i) Desktop and laptop computers (end-user environment)

ii) Servers (e.g., file and print, web, firewalls, terminal)

iii) Network components (e.g., switches, routers wireless)

b) Allow ISSO, ISO, SO and system administrators to select which auditable events are to be audited by specific components of the information system.

AU-12(1) – Audit Generation | System-Wide / Time-Correlated Audit Trail For High Information Systems:

1) SOs, in coordination with IOs, for EPA-operated systems, shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Configure information systems to compile audit records into a system-wide (logical or physical) audit trail that is time-correlated to within acceptable levels of tolerance for relationship between time stamps of individual records in the audit trail.
      i) Audit records should be stored in Coordinated Universal Time Code (UTC) format for consistency. Audit records should be time correlated to within 30 seconds of EPA standard time reference.

      Note: The audit trail is time-correlated if the time stamp in the individual audit records can be reliably related to the time stamp in other audit records to achieve a time ordering of the records within the organization-defined tolerance.

AU-12(2) – Audit Generation | Standardized Formats

Not selected as part of the security controls baseline.

AU-12(3) – Audit Generation | Changes by Authorized Individuals For High Information Systems:

1) SOs, in coordination with IOs, for EPA-operated systems, shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Configure information systems to provide the capability for system administrators to change the auditing to be performed on all applicable system components based on EPA policy, procedures and standards in coordination with the applicable ISSO, ISO and SO.

AU-13 – Monitoring for Information Disclosure

Not selected as part of the security controls baseline.

AU-13 (1) – Monitoring for Information Disclosure | Use of Automated Tools

Not selected as part of the security controls baseline.

AU-13 (2) – Monitoring for Information Disclosure | Review of Monitored Sites

Not selected as part of the security controls baseline.

AU-14 – Session Audit

Not selected as part of the security controls baseline.

AU-14 (1) – Session Audit | System Start-up

Not selected as part of the security controls baseline.

AU-14 (2) – Session Audit | Capture / Record and Log Content

Not selected as part of the security controls baseline.

AU-14 (3) – Session Audit | Remote Viewing / Listening

Not selected as part of the security controls baseline.

AU-15 – Alternate Audit Capability

Not selected as part of the security controls baseline.

AU-16 – Cross-organizational Auditing

Not selected as part of the security controls baseline

AU-16 (1) – Cross-organizational Auditing | Identity Preservation

Not selected as part of the security controls baseline.

AU-16 (2) – Cross-organizational Auditing | Sharing of Audit Information

Not selected as part of the security controls baseline.

7. RELATED DOCUMENTS

- NIST Special Publications, 800 Series

8. ROLES AND RESPONSIBILITIES

Information Owner (IO)

1) IOs have the following responsibilities with respect to audit and accountability:
   a) Assist SO with implementing and maintaining appropriate auditable events for the information resources for which they are responsible.
   b) Review auditable events for needed changes.

Service Manager (SM)

1) SMs have the following responsibilities with respect to audit and accountability procedures:
   a) 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.
   b) Ensure service providers deploy malicious code software / mechanism, flaw remediation, patch and vulnerability management in accordance with EPA standards.

c) Coordinate with IOs to ensure service providers' systems supporting non-enterprise services are configured, monitored, and maintained to protect supported information stored, processed, or transmitted within acceptable risks adequately.

d) Ensure service provider information systems are configured to verify the correct operation of security functions and tools in order to detect, prevent, quarantine, eradicate, track, and notify the appropriate personnel when anomalies are discovered.

System Owner (SO)

1) SOs have the following responsibilities with respect to audit and accountability:
   a) Implement and maintain audit trails for his/her resources and ensure auditable events are sufficient to protect the information system.
   b) Capture sufficient information in audit records to establish the occurrence of events, the sources of events, and the outcome of events.
   c) Allocate sufficient audit record storage capacity to prevent such capacity from being exceeded.
   d) Ensure that the information system automatically alerts appropriate officials when there is an audit failure or storage capacity is close to being reached.
   e) Review and analyze logs and records.
   f) Investigate any suspicious activity or suspected violations and take the necessary actions.
   g) Employ automated tools to review audit records.
   h) Train all staff involved with log management responsibilities on how to:
   i) Review and analyze audit logs.
   j) Report incidents, when applicable.
   k) Ensure that the system time is periodically updated from an authoritative resource.
   l) Ensure that audit information and audit tools are protected.
   m) Ensure that audit records are retained in accordance with the EPA Records Schedule 736 – IT Legal and Regulatory Compliance Records.

Information Security Officers (ISO) are responsible for:

1) ISOs have the following responsibility with respect to audit and accountability:
   a) Coordinate with the SAISO in developing, documenting, implementing, and reporting of audit records to all pertinent personnel.

Information System Security Officer (ISSO)

1) ISSOs have the following responsibilities with respect to audit and accountability:
   a) Review audit trails for all information systems for which he/she is assigned responsibility for security to ensure compliance with EPA's policies, procedures, and standards.
   b) Review auditable events for necessary changes in conjunction with incident information and requirements to protect the information system.

c) Coordinate with the ISO and SAISO in responding to information security data calls, audit requests, and reporting.

Supervisor

1) Supervisors have the following responsibilities with respect to audit and accountability:
   a) Assist the ISSO in reconciling audit trail anomalies.

System Administrator

1) System administrators have the following responsibilities with respect to audit and accountability:
   a) Report any operational or security problems to the appropriate authorities.
   b) Configure audit logs to capture important events in all EPA information systems.
   c) Assist the ISSO in determining the need to modify auditable events.

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 Reduction* – includes using tools and techniques that reduce audit data in order to save storage space and to abstract 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).
- *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 may be requested from the CIO by submitting a justification based on:

- Substantive business case need(s)
- Demonstration of, or a proposal for, establishment of adequate compensating controls that provide a suitable alternative to the mandated protection

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

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

11. RELATED POLICY, PROCEDURES, STANDARDS AND GUIDLINES

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 Audit and Accountability Procedures, Version 3.1, July 16, 2012.

13. ADDITIONAL INFORMATION

N/A

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

APPENDIX A: ACRONYMS & ABBREVIATIONS

CBI	Confidential Business Information
CSIRC	Computer Security Incident Response Capability
EPA	Environmental Protection Agency
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
GMT	Greenwich Mean Time
GRS	General Records Schedule
IDPS	Intrusion Detection and Prevention System
IO	Information Owner
ISO	Information Security Officer
ISSO	Information System Security Officer
IT	Information Technology
LSI	Large-Scale Integration
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OIG	Office of Inspector General
OMB	Office of Management and Budget
OSCAR	Operational Status Categories During Alerts and Risks
OTOP	Office of Technology Operations and Planning
PII	Personally Identifiable Information
SA	System Administrator
SAISO	Senior Agency Information Security Officer
SM	Service Manager
SO	System Owner
SP	Special Publication
USC	United States Code
US-CERT	United States Computer Emergency Readiness Team
USGCB	United States Government Configuration Baseline
UTC	Coordinated Universal Time