EPA INFORMATION PROCEDURES

OFFICE OF ENVIRONMENTAL INFORMATION

EPA Classification No.:	CIO-2150.3-P-03.1	CIO Approval Date:	08/06/2012
CIO Transmittal No.:	12-003	Review Date:	08/06/2015

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

INFORMATION SECURITY –
INTERIM AUDIT AND ACCOUNTABILITY PROCEDURES
V3.2
JULY 16, 2012

1. PURPOSE

The purpose of this procedure is to facilitate the implementation of Environmental Protection Agency (EPA) security control requirements for Audit and Accountability control family, as identified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 3 *Recommended Security Controls for Federal Information Systems and Organizations.*

2. SCOPE AND APPLICABILITY

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

These procedures apply to all EPA employees, contractors, and all other users of EPA information and information systems that support the operations and assets of EPA.

3. AUDIENCE

These procedures apply to all EPA employees, contractors, and all other users of EPA information and information systems that support the operations and assets of EPA.

4. BACKGROUND

Based on federal requirements and mandates, the EPA is responsible for ensuring that all Offices within the Agency meet the minimum security requirements defined in the Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*. All EPA information systems must meet the security requirements through the use of the security controls defined in the NIST SP 800-53, Revision 3 *Recommended Security Controls for Federal Information Systems and Organizations*. This chapter addresses the procedures and standards set forth by EPA, and in compliance with, the audit and accountability family of controls found in NIST SP 800-53, Revision 3.

EPA Classification No.:	CIO-2150.3-P-03.1	CIO Approval Date:	08/06/2012
CIO Transmittal No.:	12-003	Review Date:	08/06/2015

5. AUTHORITY

- E-Government Act of 2002, Public Law 107-347, Title III*, Federal Information Security Management Act (FISMA)* as amended
- Freedom of Information Act (FOIA), 5 U.S.C. § 552, as amended by Public Law 104-231, 110 Stat. 3048, Electronic Freedom of Information Act Amendments of 1996
- Clinger-Cohen Act of 1996, Public Law 104-106
- Paperwork Reduction Act of 1995 (44 USC 3501-3519)
- Privacy Act of 1974 (5 USC § 552a) as amended
- USA PATRIOT Act of 2001, Public Law 107-56
- Code of Federal Regulations, Part 5 Administrative Personnel, Subpart C—*Employees Responsible for the Management or Use of Federal Computer Systems*, Section 930.301 through 930.305 (5 C.F.R 930.301-305)
- Office of Management and Budget (OMB) Memorandum M-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

6. PROCEDURES

AU-2 – Auditable Events

a. Audit logging must be determined, based on a risk assessment and mission/business needs, that the information system must be capable of auditing for the following events:

   i. The following events must be identified within server audit logs:
      - Server startup and shutdown
      - Loading and unloading of services
      - Installation and removal of software
      - System alerts and error messages
      - User logon and logoff
      - System administration activities

- Accesses to sensitive information, files, and systems
- Account creation, modification, or deletion
- Modifications of privileges and access controls
- Additional security-related events, as required by the System Owner (SO) or to support the nature of the supported business and applications

ii. The following events must be identified within application and database audit logs:

- Modifications to the application
- Application alerts and error messages
- User logon and logoff
- System administration activities
- Accesses to information and files
- Account creation, modification, or deletion
- Modifications of privileges and access controls

iii. The following events must be identified within network device (e.g., router, firewall, switch, wireless access point) audit logs:

- Device startup and shutdown
- Administrator logon and logoff
- Configuration changes
- Account creation, modification, or deletion
- Modifications of privileges and access controls
- System alerts and error messages

b. Audit logs for desktops must be in accordance with United States Government Configuration Baseline (USGCB) requirements.

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

d. A rationale must be provided as to why the list of auditable events is deemed to be adequate to support after-the-fact investigations of security incidents.

e. The information system should 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.

For moderate and high information systems

f. The list of the auditable events should be reviewed and updated annually, or when a major change to the information system occurs. When operating in an

environment of increased risk, based on current threat information, the list should be reviewed on a monthly basis. The list of events to be audited by the information system must include the execution of privileged functions.

AU-3 – Content of Audit Records

a. The information system must capture sufficient information in audit records.

Note: Audit record content should include, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, file names involved, and access control or flow control rules invoked.

b. At a minimum, the following elements must 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

c. The following additional elements must be identified within each server and network device audit record:
   i. Manufacturer-specific event name / type of event
   ii. Source and destination network addresses
   iii. Source and destination port or protocol identifiers

For high information systems

d. The content of audit records generated by defined information system components must be centrally managed

AU-4 – Audit Storage Capacity

a. The information system must allocate audit record storage capacity to prevent such capacity being exceeded.
b. If audit logs are archived daily, three times the size of the current daily log file must be free to hold the audit logs.
c. If the audit logs are archived weekly, 10 times the size of the current daily log file must be free to hold the audit logs.
d. If the audit logs are not archived except on a monthly basis or longer, a server must be dedicated to generating and storing said audit records.

AU-5 – Response to Audit Processing Failures

a. The information system should automatically alert designated officials in the event of an audit failure or when audit capacity is 70%, 80%, and again at 90% utilization. This alert should be distributed by a mechanism that allows system administrators to receive it after hours (e.g., email, text message).
b. Once the maximum storage capacity for audit logs is reached or there is an audit failure, the information system should 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.

AU-6 – Audit Review, Analysis, and Reporting

a. Audit logs and records must be reviewed and analyzed 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. The following review and analysis requirements must be adhered to:
    i. Logs on critical systems must be reviewed daily
    ii. The level of audit review, analysis, and reporting must be adjusted if there is a change in risk to organizational operations, organizational assets, individuals, other organizations, or the Nation based on advisory warnings issued through the Homeland Security Advisory System, EPA Operational Status Categories During Alerts and Risks (OSCAR), or other internal advisory mechanisms.
    iii. Logs for firewalls, routers, and other network devices must be correlated with logs of other critical systems and examined daily to determine if any incidents have occurred.
    iv. All other logs, including access server logs, must be reviewed weekly.
    v. Logs identifying PII access and extracts must be reviewed monthly.
        - For information systems containing PII, the monthly review of audit logs will assist in determining what data extracts must be deleted.
c. The audit logs for logons and logoffs and accesses to system information must be reviewed weekly.
d. All staff involved with log management responsibilities must be trained on how to review and analyze audit logs, and how to report incidents when applicable.
    i. Personnel performing the review must have the level of background screening equivalent to the information system's sensitivity.
e. Personnel should report findings must be reported to the Information Security Officials (ISOs).
    i. ISO's must promptly report findings to EPA Computer Security Incident Response Center (CSIRC), which may escalate the incident to United States Computer Emergency Readiness Team (US-CERT).
        - 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 must be coordinated when investigations reveal that the incident is a prosecutable offense under statutes.

iii. Additionally, anomalies must be reported in accordance with EPA incident reporting requirements and procedures.

- Refer to *Information Security – Interim Incident Response Procedures* for requirements on incident reporting.

iv. If the investigation reveals an exploitable system or procedural vulnerability, coordination must occur between the appropriate management and technical personnel to ensure that the vulnerability is addressed.

For moderate and high information systems

f. Audit logs and records must be reviewed and analyzed continuously using automated processes.

g. The information system must integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.

AU-7 – Audit Reduction and Report Generation

For moderate and high information systems

a. The information system must provide an audit reduction and report generation capability

b. The information system must be capable of providing an audit reduction and report generation capability to support near real-time audit review, analysis, and reporting requirements described in AU-6 and after-the-fact investigations of security incidents.

i. Audit reduction and reporting tools must not alter original audit records

ii. 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

c. Automated tools must be employed 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

d. The information system must provide the capability to automatically process audit records for events of interest based on selectable event criteria.

AU-8 – Time Stamps

a. The information system must use internal system clocks to generate time stamps for audit records.
    i. Time stamps generated by the information system must include both the date and time

Note: The time may be expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC.

For moderate and high information systems

b. The information system must 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 can be correlated across different systems or system components. EPA time sources will synchronize will synchronize to stratum 1 NTP servers.

AU-9 – Protection of Audit Information

a. Audit logs must be protected from unauthorized modification, access, or destruction while online and during offline storage
b. Only the SO, authorized system administrators, and the designated security official for the system are permitted access to audit logs and audit tools
c. Log files must be rotated to a system other than their source system.
d. Logs containing sensitive information (e.g., CUI, PII) must be encrypted.

AU-10 – Non-repudiation

For high information systems

a. The information system must protect against an individual falsely denying having performed a particular action.

Note: Examples of particular actions taken by individuals include creating information, sending a message, approving information (e.g., indicating concurrence or signing a contract), and receiving a message.

AU-11 – Audit Record Retention

a. Audit logs must be retained to provide support for after-the-fact investigations of IT security incidents and to meet regulatory and organizational information retention requirements.
    i. These logs include system, application, and database-level audit logs and logs for network devices.
b. All audit logs must be retained in accordance with the following:

i. The records schedule found in *EPA Records Schedule 736 – IT Legal Regulatory Compliance Records*.

ii. The records retention policy provided by the National Archives and Records Administration (NARA) General Records Schedules (GRS).

c. Log files must be archived for a period of no less than one (1) year with 90 days online and the remaining time stored offline.

d. Log files for remote access devices must be transferred from the devices to a central log server where they are retained for up to three years.

i. After being retained on the server for three years, they will be copied to optical permanent storage media where they will be retained in accordance with the records schedule found in *EPA Records Schedule 736 – IT Legal Regulatory Compliance Records.*

e. Audit logs associated with known incidents, including those used for legal action, must be maintained in accordance with the records schedule found in *EPA Records Schedule 736 – IT Legal Regulatory Compliance Records*, after the incident is closed, or after all legal actions have been completed (whichever occurs later).

f. When the retention time has expired, as detailed in this procedure, logs must be disposed of in accordance with the records schedule found in *EPA Records Schedule 736 – IT Legal Regulatory Compliance Records*.

i. Refer to *Information Security – Media Protection Procedures* for requirements on media disposal.

For moderate and high information systems

g. The following requirements must be met for information systems containing Personally Identifiable Information (PII) and Confidential Business Information (CBI):

i. A usage policy must be established that identifies authorized computer-readable extracts that are needed for more than 90 days.

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

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

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

AU-12 – Audit Generation

a. The information system must provide audit record generation capability for the list of auditable events defined in AU-2 on, *at a minimum*, the following information system components:

- Desktop and laptop computers (end-user environment)
- Servers (e.g., file and print, web, firewalls, terminal)

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

For high information systems

b. The information system must 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 (UTC) format for consistency. Audit records should be time correlated to within 1 minute of UTC.

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.

7. RELATED DOCUMENTS

- NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009
- NIST SP 800-92, *Guide to Computer Security Log Management*, September 2006
- NIST SP 800-123, *Guide to General Server Security*, July 2008

8. ROLES AND RESPONSIBILITIES

Information Owner (IO)

a. The IO has the following responsibilities with respect to audit and accountability:
    i. Assist SO with implementing and maintaining appropriate auditable events for the information resources for which they are responsible.
    ii. Review auditable events for needed changes.

System Owner (SO)

a. The SO has the following responsibilities with respect to audit and accountability:
    i. Implement and maintain audit trails for his/her resources and ensure auditable events are sufficient to protect the information system.
    ii. Capture sufficient information in audit records to establish the occurrence of events, the sources of events, and the outcome of events.
    iii. Allocate sufficient audit record storage capacity to prevent such capacity from being exceeded.
    iv. Ensure that the information system automatically alerts appropriate officials when there is an audit failure or storage capacity is close to being reached.
    v. Review and analyze logs and records.
    vi. Investigate any suspicious activity or suspected violations and take the necessary actions.
    vii. Employ automated tools to review audit records.

viii. Train all staff involved with log management responsibilities on how to:
- Review and analyze audit logs.
- Report incidents, when applicable.

ix. Ensure that the system time is periodically updated from an authoritative resource.

x. Ensure that audit information and audit tools are protected.

xi. Ensure that audit records are retained in accordance with the EPA Records Schedule 736 – IT Legal and Regulatory Compliance Records.

Information System Security Officer (ISSO)

a. The ISSO has the following responsibilities with respect to audit and accountability:
   i. 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.
   ii. Review auditable events for necessary changes in conjunction with incident information and requirements to protect the information system.

Office of Technology Operations and Planning (OTOP) Security Officer

a. The OTOP security officer has the following responsibilities with respect to audit and accountability:
   i. Coordinate with appropriate technical and management personnel to investigate patterns indicating system penetration attempts or unauthorized alterations or modifications of operating system files.
   ii. Coordinate appropriate actions, including notification of local legal counsel, the OIG, and local and federal law enforcement officials when investigations reveal that the incident is a prosecutable offense under existing statutes.
   iii. Coordinate with appropriate management and technical personnel to ensure that the vulnerability is addressed if the investigation reveals an exploitable system or procedural vulnerability.

Supervisor

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

System Administrator

a. System administrators have the following responsibilities with respect to audit and accountability:
   i. Report any operational or security problems to the appropriate authorities.
   ii. Configure audit logs to capture important events in all EPA information systems.
   iii. 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 and includes a signature. The documentation can be accomplished manually or electronically.

10. WAIVERS

Waivers may be requested from the CIO by submitting a justification based on:

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

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

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

11. RELATED POLICY, PROCEDURES, STANDARDS AND 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 Manual, Directive 2195A1, 1999 Edition, Section 13 and Appendix A

13. ADDITIONAL INFORMATION

NA

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

APPENDIX A: ACRONYMS

CBI	Confidential Business Information
CSIRC	Computer Security Incident Response Center
EPA	Environmental Protection Agency
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
GMT	Greenwich Mean Time
GRS	General Records Schedule
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
SAISO	Senior Agency Information Security Officer
SP	Special Publication
USC	United States Code
US-CERT	United States Computer Emergency Readiness Team
UTC	Coordinated Universal Time

DOCUMENT CHANGE HISTORY

Version	Release Date	Summary of Changes	Author of Changes	DCN
0.5	9/22/08	Initial draft	Heather Flager	Procedures-AU-Draft_TO62_020_1
1.0	12/11/08	Incorporated EPA comments	Heather Flager	Procedures-AU-Final_TO62_020_2
2.0	6/17/09	Revised Final	Heather Flager	Procedures-AU-Final_TO62_020_3
2.1	9/18/09	Incorporated comments	William Gill	Procedures_AU_Final_v2.1
2.9	7/12/10	Updated per NIST SP 800-53 Rev 3	Heather Flager	Procedures_AU_Draft.TO-062_050_1.0
2.9	7/16/10	TISS comments and changes	Charleen Johnson	Procedures_AU_Draft.TO-062_050_1.0
3.0	1/14/11	TISS Final Draft Review	Charleen Johnson & Mark Hubbard	Procedures_AU_Draft.TO-062_050_1.0
3.1	4/17/2012	SAISO Final Review	Abe Getchell	Procedures-AU-Final
3.2	7/16/2012	Document Review	LaToya Gordon	Procedures_AU_Draft.TO-062_050_1.0