# VERSION HISTORY/CHANGE RECORD

<table>
<thead>
<tr>
<th>Change Number</th>
<th>Person Posting Change</th>
<th>Change</th>
<th>Reason for Change</th>
<th>Page Number of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Scott/Heard</td>
<td>Changes made throughout the document to reflect FISMA, NIST and GSA CIO P 2100.1B requirements.</td>
<td>Updated to reflect and implement various FISMA, NIST and GSA CIO P 2100.1B requirements.</td>
<td>Various</td>
</tr>
<tr>
<td>2</td>
<td>Scott/Heard</td>
<td>Changes throughout the document to correspond with revisions made to CIO-IT Security-10-09, CIO-IT Security-01-03 and CIO-IT Security-01-04.</td>
<td>Updated to reflect the correlation of the CIO-IT Security Guides; and to further express policy within them as standalone documents</td>
<td>Various</td>
</tr>
<tr>
<td>3</td>
<td>Hummel/Windelberg</td>
<td>Changes throughout the document to correspond with update of the current version of GSA CIO P 2100 and other updates</td>
<td>Update to the most current version of GSA CIO P 2100 and provide more detailed guidance on implementing policy.</td>
<td>Various</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Revision 2 – January 29, 2008</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Berlas/Cook</td>
<td>Changes throughout the document to correspond with update of the current version of GSA CIO P 2100 and NIST 800-53 rev3.</td>
<td>Update to the most current version of GSA CIO P 2100 and provide more detailed guidance on implementing policy.</td>
<td>Various</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Revision 3 – June 30, 2010</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Wilson/Yardley/Klemens</td>
<td>Changes throughout the document to correspond with update of the current version of NIST 800-53 Rev4.</td>
<td>Update to NIST 800-53, Rev 4 and correlate with GSA Guidance on parameters and implementation.</td>
<td>Various</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Revision 4 – March 22, 2017</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Feliksa/Heffron/Klemens</td>
<td>Updated format and NIST SP 800-53 control parameters, and incorporated current Federal regulations and guidance.</td>
<td>Incorporate most current Federal regulations, NIST guidance, and GSA requirements.</td>
<td>Various</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Revision 5 – November 3, 2017</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| 1             | Sibley/Weaver/Klemens/Dean | Revised to address:  
  • Updated control parameters and implementation details, especially regarding the ELP  
  • Added information identifying controls as common, hybrid, or system-specific  
  • Added a section regarding NIST SP 800-161 SCRM controls  
  • Updated to current format and style, including Section 508 compliance  
  • Revised how the CSF is related to audit and accountability | Update to current Federal, NIST, and GSA regulations, guidance, and requirements. | Various               |
|                |                       | **Revision 6 – December 3, 2020**                                       |                                                                                    |                       |
Approval

IT Security Procedural Guide: Audit and Accountability (AU), CIO-IT Security 01-08, Revision 6, is hereby approved for distribution.

Bo Berlas
GSA Chief Information Security Officer

Contact: GSA Office of the Chief Information Security Officer (OCISO), Policy and Compliance Division (ISP) at ispcompliance@gsa.gov.
Table of Contents

1 Introduction .................................................................................................................. 1
  1.1 Purpose .................................................................................................................. 3
  1.2 Scope ....................................................................................................................... 3
  1.3 Policy ....................................................................................................................... 4
  1.4 References .............................................................................................................. 4

2 Roles and Responsibilities .......................................................................................... 5
  2.1 Authorizing Officials (AOs) .................................................................................... 5
  2.2 Information Systems Security Managers (ISSMs) .................................................... 5
  2.3 Information Systems Security Officers (ISSOs) ....................................................... 6
  2.4 System Owners (SOs) ........................................................................................... 6
  2.5 Data Owners ......................................................................................................... 6
  2.6 System/Network Administrators ............................................................................ 7
  2.7 ELP Personnel ........................................................................................................ 7

3 GSA Implementation Guidance for AU Controls ......................................................... 7
  3.1 Integration with the ELP ......................................................................................... 8
  3.2 AU-1 Audit and Accountability Policy and Procedures ............................................. 8
  3.3 AU-2 Auditable Events ......................................................................................... 9
  3.4 AU-3 Content of Audit Records .......................................................................... 10
  3.5 AU-4 Audit Storage Capacity .............................................................................. 12
  3.6 AU-5 Response to Audit Processing Failures ....................................................... 13
  3.7 AU-6 Audit Review, Analysis, and Reporting ....................................................... 14
  3.8 AU-7 Audit Reduction and Report Generation ..................................................... 16
  3.9 AU-8 Time Stamps .............................................................................................. 17
  3.10 AU-9 Protection of Audit Information ................................................................. 18
  3.11 AU-10 Non-Repudiation ..................................................................................... 19
  3.12 AU-11 Audit Record Retention ........................................................................... 20
  3.13 AU-12 Audit Generation ..................................................................................... 21

4 Audit and Accountability and Supply Chain Risk Management ..................................... 22
  4.1 AU-1 Audit and Accountability Policy and Procedures (ICT SCRM) ....................... 23
  4.2 AU-2 Audit Events (ICT SCRM) .......................................................................... 23
  4.3 AU-6 Audit Review, Analysis, and Reporting (ICT SCRM) ................................... 24
  4.4 AU-10 Non-Repudiation (ICT SCRM) ................................................................ 24
  4.5 AU-12 Audit Generation (ICT SCRM) ................................................................ 25
  4.6 AU-13 Monitoring for Information Disclosure (ICT SCRM) ............................... 25
  4.7 AU-16 Cross-organizational Auditing (ICT SCRM) ........................................... 26

5 Summary ....................................................................................................................... 26

Table of Figures and Tables

<table>
<thead>
<tr>
<th>Table</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-1</td>
<td>CSF Categories/Subcategories</td>
</tr>
<tr>
<td>3-1</td>
<td>Designation of AU Controls</td>
</tr>
<tr>
<td>3-2</td>
<td>Log Storage</td>
</tr>
<tr>
<td>3-3</td>
<td>Log Review Responsibility</td>
</tr>
<tr>
<td>3-4</td>
<td>Examples of System Component Logs</td>
</tr>
</tbody>
</table>
Notes:

- Hyperlinks in running text will be provided if they link to a location within this document (i.e., a different section or an appendix). Hyperlinks will be provided for external sources unless the hyperlink is to a webpage or document listed in Section 1.4. For example, Google Forms, Google Docs, and websites will have links.
- It may be necessary to copy and paste hyperlinks in this document (Right-Click, Select Copy Hyperlink) directly into a web browser rather than using Ctrl-Click to access them within the document.
1 Introduction

Audit trails maintain a record of system activity both by system and application processes and by user activity of systems and applications. When complemented with appropriate tools and procedures, audit trails can provide a means to help accomplish several security-related objectives, including but not limited to: (1) establishing individual accountability; (2) detecting security violations and intrusions; (3) identifying flaws in systems and applications; (4) performing problem analysis; and (5) assisting in incident reconstruction.

When auditing is not implemented, is improperly configured, and/or the resultant audit logs are not regularly reviewed, the following outcomes may occur in the event of a system compromise:

- An incident may go undetected;
- An attacker may hide their location, malicious software, and activities on the compromised host;
- User accountability for actions may be unsupported;
- System changes may not be noticed.

If a compromise is detected, without properly protected and complete logging records, those charged with the security responsibility for the system are blind to the details of the attack. The attack may go unnoticed, with attackers sometimes controlling compromised machines for months or years without anyone in the organization knowing, even though the evidence of the attack has been recorded in unexamined log files. Audit records may be the only evidence of a successful attack.

Audit logging cannot be just for compliance purposes. Audit logs must be used for proactive review, including real-time analysis, ongoing periodic reviews, and to establish what occurred after an event. Reviewers should know what to look for to effectively spot unusual activity, and understand the normal activity for the systems under their purview.

Every General Services Administration (GSA) Information Technology (IT) system must follow the practices described in this guide. Any deviations from the security requirements established in GSA Order CIO 2100.1, “GSA Information Technology (IT) Security Policy,” must be coordinated by the appropriate Information Systems Security Officer (ISSO) through the appropriate Information Systems Security Manager (ISSM) and approved by the Authorizing Official (AO). Any deviations, exceptions, or other conditions not following GSA policies and standards must be submitted using the Security Deviation Request Google Form.

The audit and accountability principles and practices described in this guide are based on guidance from National Institute of Standards and Technology (NIST) including NIST Special

Executive Order (EO) 13800, “Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure” requires all agencies to use “The Framework for Improving Critical Infrastructure Cybersecurity (the Framework) developed by NIST or any successor document to manage the agency’s cybersecurity risk.” This NIST document is commonly referred to as the Cybersecurity Framework (CSF).

The CSF focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization’s risk management processes. The core of the CSF consists of five concurrent and continuous Functions—Identify (ID), Protect (PR), Detect (DE), Respond (RS), and Recover (RC). The CSF complements, and does not replace, an organization’s risk management process and cybersecurity program. GSA uses NIST’s Risk Management Framework (RMF) from NIST SP 800-37, Revision 2, “Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. Table 1-1, CSF Categories/Subcategories lists the Categories and Subcategories from the CSF that are identified as related to the implementation of policies, procedures, and processes implementing the NIST SP 800-53 Audit and Accountability control family, hereinafter the identifier AU will be used when referring to the controls or control family. GSA CIO Order 2100.1 and this procedural guide provide GSA’s policies and procedural guidance regarding audit and accountability for GSA IT systems and AU controls.

<table>
<thead>
<tr>
<th>CSF Category/Subcategory Identifier</th>
<th>Definition/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Governance (ID.GV)</td>
<td>The policies, procedures, and processes to manage and monitor the organization’s regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.</td>
</tr>
<tr>
<td>ID.GV-1</td>
<td>Organizational cybersecurity policy is established and communicated</td>
</tr>
<tr>
<td>ID.GV-3</td>
<td>Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed</td>
</tr>
</tbody>
</table>

1 NIST SP 800-53, Revision 5, “Security and Privacy Controls for Information Systems and Organizations,” became final in September 2020 and NIST SP 800-53B, “Control Baselines for Information Systems and Organizations,” became final in October 2020. This guide remains aligned with Revision 4 and its baselines; prior to November 2021 this guide will be updated to reflect the new NIST guidance.
<table>
<thead>
<tr>
<th>CSF Category/Subcategory Identifier</th>
<th>Definition/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supply Chain Risk Management (ID.SC)</td>
<td>The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.</td>
</tr>
<tr>
<td>ID.SC-4</td>
<td>Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations</td>
</tr>
<tr>
<td>Data Security (PR.DS)</td>
<td>Information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information.</td>
</tr>
<tr>
<td>PR.DS-4</td>
<td>Adequate capacity to ensure availability is maintained</td>
</tr>
<tr>
<td>Protective Technology (PR.PT)</td>
<td>Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.</td>
</tr>
<tr>
<td>PR.PT-1</td>
<td>Audit/log records are determined, documented, implemented, and reviewed in accordance with policy</td>
</tr>
<tr>
<td>Anomalies and Events (DE.AE)</td>
<td>Anomalous activity is detected and the potential impact of events is understood.</td>
</tr>
<tr>
<td>DE.AE-2</td>
<td>Detected events are analyzed to understand attack targets and methods</td>
</tr>
<tr>
<td>DE.AE-3</td>
<td>Event data are collected and correlated from multiple sources and sensors</td>
</tr>
<tr>
<td>Security Continuous Monitoring (DE.CM)</td>
<td>The information system and assets are monitored to identify cybersecurity events and verify.</td>
</tr>
<tr>
<td>DE.CM-1</td>
<td>The network is monitored to detect potential cybersecurity events</td>
</tr>
<tr>
<td>DE.CM-3</td>
<td>Personnel activity is monitored to detect potential cybersecurity events</td>
</tr>
<tr>
<td>DE.CM-7</td>
<td>Monitoring for unauthorized personnel, connections, devices, and software is performed</td>
</tr>
<tr>
<td>Detection Processes (DE.DP)</td>
<td>Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.</td>
</tr>
<tr>
<td>DE.DP-4</td>
<td>Event detection information is communicated</td>
</tr>
<tr>
<td>Communications (RS.CO)</td>
<td>Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).</td>
</tr>
<tr>
<td>RS.CO-2</td>
<td>Incidents are reported consistent with established criteria</td>
</tr>
<tr>
<td>Analysis (RS.AN)</td>
<td>Analysis is conducted to ensure effective response and support recovery activities.</td>
</tr>
<tr>
<td>RS.AN-1</td>
<td>Notifications from detection systems are investigated</td>
</tr>
<tr>
<td>RS.AN-3</td>
<td>Forensics are performed</td>
</tr>
</tbody>
</table>

1.1 Purpose

The purpose of this guide is to provide guidance for the AU security controls identified in NIST SP 800-53 and auditing and accountability requirements specified in CIO Order 2100.1. The guide provides GSA Federal employees, contractors with significant security responsibilities (as identified in CIO Order 2100.1), and other IT personnel involved in implementing auditing and monitoring, the specific procedures they are to follow for implementing AU features and functions for systems under their purview.

1.2 Scope

The requirements outlined within this guide apply to and must be followed by all GSA Federal employees and contractors who are involved in audit and accountability of GSA information...
systems and data. All GSA systems must adhere to the requirements and guidance provided with regard to audit and accountability as described in this guide.

1.3 Policy

CIO 2100.1 contains the following policy statements regarding audit and accountability.

Chapter 4, Paragraph 6, Protective technology.

a. The requirements for security auditing/logging capabilities and their review must be implemented on GSA systems IAW GSA CIO-IT Security-01-08: Audit and Accountability.

b. Auditing of actions regarding PII stored on network drives and/or application databases must be captured (e.g., type of action, date/time, user, source of action, outcome of action)

Chapter 5, Paragraph 1, Anomalies and Events.

c. The OCISO will regularly review/analyze data provided with the ELP for indications of inappropriate or unusual activity. Suspicious activity or suspected violations must be investigated. Any findings must be reported to appropriate officials IAW GSA CIO-IT Security-01-02.

d. Information systems must produce audit/log records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.

e. The OCISO ELP will be used for the collection and correlation from GSA systems/sensors.

Chapter 5, Paragraph 2, Security continuous monitoring.

d. Monitoring procedures must include specific steps to be taken and protocol to be applied when reviewing audit/log data.

e. The OCISO must be informed in the event of an audit processing failure and system personnel must take one of the following additional actions: shut down information system, overwrite oldest audit records, or stop generating audit records.

1.4 References

Federal Laws, Standards, Regulations, and Publications:

- **EO 13800**, “Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure”
- **NIST Cybersecurity Framework**, “Framework for Improving Critical Infrastructure Cybersecurity”
- **NIST SP 800-53, Revision 4**, “Security and Privacy Controls for Federal Information Systems and Organizations”
2 Roles and Responsibilities

There are many roles associated with implementing effective auditing and logging, and reviews of the records produced. The roles and responsibilities provided in this section have been extracted or paraphrased from CIO 2100.1 or summarized from GSA and Federal guidance. The responsibilities listed in this guide are focused on auditing and accountability, a complete set of GSA security roles and responsibilities can be found in CIO 2100.1. Throughout this guide, specific processes and procedures for implementing NIST’s AU controls are described.

2.1 Authorizing Officials (AOs)

Responsibilities include the following:

- Ensuring that GSA information systems under their purview have implemented the required AU controls in accordance with GSA and Federal policies and requirements.
- Identifying the level of acceptable risk for an information system and determining whether an acceptable level of risk has been obtained, including risks associated with AU controls.
- Ensuring all information systems, applications, or sets of common controls under their purview have a current ATO issued IAW GSA CIO-IT Security-06-30.
- Ensuring a plan of action and milestones (POA&M) item is established and managed to address AU controls that are not fully implemented.

2.2 Information Systems Security Managers (ISSMs)

Responsibilities include the following:

- Assisting ISSOs to ensure the necessary AU security controls are in place and operating as intended.
- Coordinating with ISSOs to establish and manage auditing and monitoring procedures (e.g., reviewing and coordinating the reporting of security alerts, performance of audit log reviews, supporting the use of auditing/logging as part of security incident investigations and reports, etc.).
• Working with the ISSO and System Owner to develop, implement, and manage POA&Ms regarding AU controls for their respective systems IAW GSA CIO-IT Security-09-44.

2.3 Information Systems Security Officers (ISSOs)

Responsibilities include the following:

• Ensuring necessary AU security controls are in place and operating as intended.
• Coordinating with ISSMs to establish and manage auditing and monitoring procedures (e.g., reviewing and coordinating the reporting of security alerts, performance of audit log reviews, supporting the use of auditing/logging as part of security incident investigations and reports, etc.).
• Reviewing audit/log reports for systems integrated with the GSA Enterprise Logging Platform (ELP) for potential security issues.
• Verifying systems not integrated with the GSA ELP/audit logging tool perform similar reviews to identify potential security issues.
• Working with the System Owner and ISSM to develop, implement, and manage POA&Ms regarding AU controls for their respective systems IAW GSA CIO-IT Security-09-44.

2.4 System Owners (SOs)

Responsibilities include the following:

• Ensuring necessary AU security controls are in place and operating as intended.
• Working with ELP personnel to ensure audit record formats for their systems can be processed by the ELP.
• Working with Data Owners to ensure the appropriate level of auditing and logging data is enabled and generated to support monitoring activities, and archived for a period of not less than 180 days.
• Working with Data Owners to audit user activity for indications of fraud, misconduct, or other irregularities.
• Working with Data Owners to document all phases of monitoring activity including monitoring procedures, response processes, and steps performed when reviewing user activity.
• Working with the ISSO and ISSM to develop, implement, and manage POA&Ms regarding AU controls for their respective systems IAW GSA CIO-IT Security-09-44.
• Assigning system personnel to review any logs not forwarded to the ELP.

2.5 Data Owners

Responsibilities include the following:

• Coordinating with IT security personnel including the ISSM, ISSO, and System Owners to ensure implementation of system and data controls, including AU controls.
• Working with the System Owner to ensure the appropriate level of auditing and logging data is enabled and generated to support monitoring activities, and archived for a period not less than 180 days.
• Working with the System Owner to audit user activity for indications of fraud, misconduct, or other irregularities.
• Working with the System Owner to document all phases of monitoring activity including monitoring procedures, response processes, and steps performed when reviewing user activity.

2.6 System/Network Administrators

Responsibilities include the following:
• Ensuring the appropriate AU security requirements are implemented consistent with GSA IT security policies and hardening guidelines.
• Performing audit/log reviews for systems not integrated with the GSA ELP to identify potential security issues as specified in the system’s system security plan (SSP).

2.7 ELP Personnel

Responsibilities include the following:
• Working with the ISSM, ISSO, System Owner, and System Administrators to ensure audit/log data is enabled and configured to send logs to the ELP.
• Investigating with the ISSM, ISSO, System Owner, and System Administrators when issues are identified regarding audit/log data being sent to the ELP.
• Coordinating with the ISSM, ISSO, System Owner, and System Administrators regarding alerts, responses to audit/log failure, and reviews of audit/log data.

3 GSA Implementation Guidance for AU Controls

The GSA-defined parameter settings included in the control requirements are italicized and offset by brackets in the control text. As stated in Section 1.2, Scope, the requirements outlined within this guide apply to and must be followed by all GSA Federal employees and contractors who are involved in audit and accountability of GSA information systems and data, and are applicable to all GSA systems. The GSA implementation guidance stated for each control applies to personnel and/or the systems operated on behalf of GSA. Any additional instructions or requirements for contractor systems will be included in the “Additional Contractor System Considerations” portion of each control section.

Each AU control or control enhancement paragraph indicates the applicability based on FIPS 199 security categorization of the control/control enhancement. Table 3-1 identifies the designation of AU controls as Common, Hybrid, or System-Specific Controls for both Federal and Contractor systems. Effectively, common controls are provided by GSA at the enterprise level or by one of GSA’s Major Information Systems (previously General Support System), system specific controls are implemented at the system level, and hybrid controls have shared
responsibilities for control implementation. CIO-IT Security 18-90, “Information Security Program Plan (ISPP),” describes the GSA enterprise-wide common and hybrid controls and outlines the responsible parties for implementing them.

Table 3-1: Designation of AU Controls

<table>
<thead>
<tr>
<th>System Type</th>
<th>Federal</th>
<th>Contractor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common</td>
<td>AU-1; AU-6(3); AU-8(1)</td>
<td></td>
</tr>
<tr>
<td>Hybrid</td>
<td>AU-2, 2(3); AU-3, 3(1), 3(2); AU-4; AU-5, 5(1), 5(2); AU-6, 6(1), 6(5), 6(6); AU-7, 7(1); AU-8; AU-9, 9(2), 9(3), 9(4); AU-10; AU-11; AU-12</td>
<td>AU-1</td>
</tr>
<tr>
<td>System-Specific</td>
<td>AU-12(1), 12(3)</td>
<td>AU-2, 2(3); AU-3, 3(1), 3(2); AU-4; AU-5, 5(1), 5(2); AU-6, 6(1), 6(3), 6(5), 6(6); AU-7, 7(1); AU-8, 8(1); AU-9, 9(2), 9(3), 9(4); AU-10; AU-11; AU-12, 12(1), 12(3)</td>
</tr>
</tbody>
</table>

3.1 Integration with the ELP

The GSA Security Operations Division (ISO) team, also known as SecOps, operates the ELP to provide support to GSA systems for logging, log review, and security monitoring. This platform is part of the Security Tools (SecTools) Federal Information Security Modernization Act (FISMA) system. Systems deployed within the GSA on premise network or Federal Acquisition Service Cloud Services (FCS) FISMA system in Amazon Web Services (AWS) can leverage the ELP and inherit parts of a number of NIST controls from the SecTools FISMA system in order to reduce their own responsibilities. The hybrid nature of these controls requires the ISSO and system personnel to work with the SecOps team to configure agents and documentation of how the customer responsibilities of the controls are being met. For a list of the inherited controls provided by SecTools, reference the SecTools CIS/CRM Google Sheet.

Teams wanting to inherit from SecOps systems must be on-boarded by SecOps using the Log Forward/Collection On-board Request form.

**Note:** If a GSA system is integrated with SecTools, and does not contain any Personally Identifiable Information (PII)/sensitive (e.g., financial, Controlled Unclassified Information [CUI]) data a number of its audit logging requirements are satisfied by inheriting those controls and fulfilling the SecTools customer responsibilities. Integration with SecTools means that GSA security agents and SecTools logging configuration and/or agents are installed.

3.2 AU-1 Audit and Accountability Policy and Procedures

Control AU-1 is applicable at all FIPS 199 levels. Parameter assignments and implementation guidance are provided in CIO-IT Security 18-90, “Information Security Program Plan (ISPP),” for the AU-1 control.
3.3 AU-2 Auditable Events

Control: The organization:

a. Determines that the information system is capable of auditing the following events: [(1) successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events, (2) Web applications should log all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes, (3) for technologies with limited auditing features, the capabilities will be recommended by the GSA S/So or Contractor, based on an industry source such as vendor guidance or Center for Internet Security benchmark, and approved by the GSA AO];

b. Coordinates 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;

c. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and

d. Determines that the following events are to be audited within the information system: [(1) audit configuration requirements as documented in applicable GSA IT Security Technical Guides and Standards (i.e., hardening and technology implementation guides), (2) for web applications see GSA IT Security Procedural Guide 07-35, Section 2.8.10, What to Log, (3) for technologies where a Technical Guide and Standard does not exist, events from an industry source such as vendor guidance or Center for Internet Security benchmark, recommended by the GSA S/So or Contractor and approved by the GSA AO].

Control Enhancements:

(3) Audit Events | Reviews and Updates. The organization reviews and updates the audited events [annually or whenever there is a change in the system’s threat environment as communicated by the GSA S/So AO or the GSA OCISO].

GSA Implementation Guidance: Control AU-2 is applicable at all FIPS 199 levels. Enhancement AU-2(3) is applicable at FIPS 199 Moderate and High levels. AU-2 and AU-2(3) are Hybrid Controls for Federal systems, shared between Platforms and Hosted Applications, and System-Specific Controls for Contractor systems.

Federal System Common Control Implementation:
The GSA SecOps team operates the ELP; system owners may forward operating system auditable events to it. The customer’s (i.e., system owners/personnel) responsibilities for leveraging the SecTools environment have been detailed in the SecTools CIS/CRM Spreadsheet.

The GSA SecOps team uses host-based security agents and the ELP in order to correlate operating system auditable events which may trigger alerts on security events which are further analyzed and correlated with other security systems in the ELP. FISMA system owners should request to have host-based security agents installed on an individual operating system, and, if supported, host-based security agent events will be forwarded to the ELP. These security events
are maintained, managed, and correlated by SecOps and reviewed in the ELP by the ISO division’s Security Operations Center (SOC).

GSA has created a series of system hardening guides and associated benchmarks that are available on the IT Security Technical Guides and Standards webpage where the configuration of audit events is defined to support GSA operations.

For enhancement AU-2(3), GSA SecOps reviews and updates the audited events forwarded to the ELP annually.

**Federal System System-Specific Expectation:**
For systems integrated with the ELP, ISSOs retain the responsibility of verifying that logging is correctly configured and processed in accordance with the control statement. For systems not integrated with the ELP and for events from components the ELP does not support (e.g., database, application) the ISSO must coordinate with the System Owner to ensure the AU-2 controls, including enhancements, are met.

For enhancement AU-2(3), ISSOs/System Owners are responsible for reviewing the events forwarded to the ELP annually or whenever there is a change in the system’s threat environment as communicated by the GSA S/So AO or the GSA OCISO. If auditable events are managed locally on the server or a separate log server, audited system events must be reviewed and updated by the ISSO/system owner annually or whenever there is a change in the system’s threat environment.

**Additional Contractor System Considerations:** Vendors/contractors are required to comply with the control statements.

### 3.4 AU-3 Content of Audit Records

**Control:** The information system generates audit records containing information that establishes 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.

**Control Enhancements:**

1. **Content of Audit Records | Additional Audit Information.** The information system generates audit records containing the following additional information:
   i. Session, connection, transaction, or activity duration.
   ii. For client-server transactions, the number of bytes received and bytes sent. This gives bidirectional transfer information that can be helpful during an investigation or inquiry.
   iii. For client-server transactions, unique metadata or properties about the client initiating the transaction. This could include properties such as an IP address, user name, session identifier or browser characteristics (e.g., a ‘User-Agent’ string).
   iv. Details regarding the event ‘type’: the type of method (for HTTP: GET/POST/HEAD,
etc.) or action (Database INSERT, UPDATE, DELETE).

v. Characteristics that describe or identify the object or resource being acted upon.

vi. Additional informational messages to diagnose or identify the event].

(2) Content of Audit Records | Centralized Management of Planned Audit Record Content. The information system provides centralized management and configuration of the content to be captured in audit records generated by [GSA S/ISO or Contractor recommended information system components to be approved by the GSA AO].

GSA Implementation Guidance: Control AU-3 is applicable at all FIPS 199 levels. Enhancement AU-3(1) is applicable at the FIPS 199 Moderate and High levels. Enhancement AU-3(2) is also applicable at the FIPS 199 High level. AU-3, 3(1), and 3(2) are Hybrid Controls for Federal systems, shared between Platforms and Hosted Applications, and System-Specific Controls for Contractor systems.

Federal System Common Control Implementation:
Audit records that are forwarded to the ELP must be formatted such that they can be properly processed by the ELP, e.g., in a standard syslog format or the Common Event Format. The ELP may have different requirements depending on the data source vendor, version, etc., to ensure it meets the base control requirements. Generally, if an audit record can be parsed by the ELP, it will meet the base control requirements.

For enhancement AU-3(1) parameters i and ii, only traffic that traverses the GSA perimeter firewall or Intrusion Prevention Systems (IPS) devices is captured and contained by the ELP. For AU-3(1) parameters iii, iv, v, and vi, only HTTP traffic and HTTPS traffic (when the HTTPS private key is available for session decryption) where the traffic traverses the perimeter firewalls or IPSs is also captured and contained by the ELP.

For enhancement AU-3(2)—applicable to FIPS 199 High systems, the GSA OCISO ISO division will work with the system owner to determine the appropriate information system components.

Federal System System-Specific Expectation:
The FISMA system owner is responsible for ensuring that audit records meet the base control requirements and that the formatting can be processed by the ELP. This could involve working with the vendor/OCISO SecOps regarding creation of log parsers; or alternatively working with the vendor of the audit record source to ensure the records are formatted in a parsable common event format.

For enhancement AU-3(1), the FISMA system owner is responsible for ensuring that the system is configured properly and meets the requirements. Typically, this means that a web server has Worldwide Web Consortium (W3C) extended logging enabled and includes the required fields, including any significant GET/PUT parameters used in the application. System owners are responsible ensuring PII data and sensitive data such as financial data are NOT stored in the logs, unless they are obfuscated.
For enhancement AU-3(2)—applicable to FIPS 199 High systems, the GSA OCISO ISO division will work with the system owner to determine the appropriate information system components.

**Note:** The system owner may choose to manage and configure the content to be captured locally unless enhancement AU-3(2) is required (i.e., a FIPS 199 High system). The system owner may also elect to coordinate with the GSA OCISO ISO division to manage and configure content to be captured, regardless of FIPS 199 security categorization.

**Additional Contractor System Considerations:** Vendors/contractors are required to comply with the control statements.

### 3.5 AU-4 Audit Storage Capacity

**Control:** The organization allocates audit record storage capacity in accordance with [GSA policies and guidance: audit log sizes are documented in applicable GSA IT Security Technical Guides and Standards (i.e., hardening and technology implementation guides) available on the IT Security Technical Guides and Standards webpage](https://www.gsa.gov/ITSecurityTechnicalGuidesAndStandards).

**GSA Implementation Guidance:** Control AU-4 is applicable at all FIPS 199 levels. AU-4 is a Hybrid Control for Federal systems, shared between GSA’s SecTools FISMA system and the Federal systems, and a System-Specific Control for Contractor systems.

Table 3-2 identifies, at the various system layers, which logs should be stored locally and/or forwarded when integrated with the ELP.

<table>
<thead>
<tr>
<th>System Layers</th>
<th>Store Logs Locally</th>
<th>Forward Logs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Service Provider (e.g., AWS)</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Operating Systems</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Databases</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Applications</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Tools</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Security Agent/Device Events</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

**Local Log Storage:** Logs should be stored by the system team, either on the host itself or in a storage repository the team has access to such as network-attached storage or S3. The storage type used must be durable to avoid loss of audit logs. Per control AU-11, logs must be retained for a minimum of 180 days.

**Forwarded Logs:** Logs should be forwarded to SecOps for storage. The logs will not be parsed or reviewed unless there is a security incident identified by correlated security events or CyberHunt activities conducted...
by OCISO. Per control AU-11, logs will be retained for a minimum of 180 days.

Federal System Common Control Implementation:
Common control implementation guidance is provided in CIO-IT Security 18-90, “Information Security Program Plan (ISPP),” for systems integrated with the ELP for the AU-4 control.

Federal System System-Specific Expectation:
System-specific implementation guidance is provided in CIO-IT Security 18-90, “Information Security Program Plan (ISPP),” for systems integrated with the ELP for the AU-4 control. Systems not integrated with the ELP, and logs that are not forwarded to the ELP must have sufficient storage capacity provided by the system in accordance with the control requirement.

Additional Contractor System Considerations: Vendors/contractors are required to comply with the control statement.

3.6 AU-5 Response to Audit Processing Failures

Control: The information system:

a. Alerts [the GSA ISO Division via the Enterprise Logging Platform for systems integrated with the Enterprise Logging Platform; Administrators (Application, System, Network, etc.) for systems not integrated with the Enterprise Logging Platform] in the event of an audit processing failure; and

b. Takes the following additional actions: [shut down information system, overwrite oldest audit records, or stop generating audit records].

Control Enhancements:

1. Response to Audit Processing Failures | Audit Storage Capacity. The information system provides a warning to [Administrators (Application, System, Network, etc.)] within [GSA S/So or Contractor recommended time period as approved by the GSA AO] when allocated audit record storage volume reaches [GSA S/So or Contractor recommended percentage as approved by the GSA AO] of repository maximum audit record storage capacity.

2. Response to Audit Processing Failures | Real-Time Alerts. The information system provides an alert in [GSA S/So or Contractor recommended time period as approved by the GSA AO] to [the GSA ISO Division via the Enterprise Logging Platform for systems integrated with the Enterprise Logging Platform; Administrators (Application, System, Network, etc.) for systems not integrated with the Enterprise Logging Platform] when the following audit failure events occur: [GSA S/So or Contractor recommended audit failure events requiring real-time alerts as approved by the GSA AO].

GSA Implementation Guidance: Control AU-5 is applicable at all FIPS 199 levels. Enhancements AU-5(1) and (2) are applicable at the FIPS 199 High level. AU-5, 5(1), and 5(2) are Hybrid Controls for Federal systems, shared between Platforms and Hosted Applications, and System-Specific Controls for Contractor systems.
Federal System Common Control Implementation:
Logging sources managed in the ELP may be configured to alert if auditing or event logging ceases for a system, doing so will address part a of the base control for systems integrated with the ELP.

Federal System System-Specific Expectation:
The system owner must define which of the specified actions is to be taken upon log failure and must coordinate any ELP alerting with the GSA OCISO ISO Division. The System Owner should troubleshoot the cause of the logging failure and work with the GSA OCISO ISO Division to restore logging to the ELP.

For enhancement AU-5(1) and (2)—applicable to FIPS 199 High systems, the System Owner is responsible for ensuring the system is configured and meets the requirements outlined. For systems integrated with the ELP the System Owner must coordinate any ELP alerting with the GSA OCISO ISO Division.

Additional Contractor System Considerations: Vendors/contractors are required to comply with the control statements.

3.7 AU-6 Audit Review, Analysis, and Reporting

Control: The organization:

a. Reviews and analyzes information system audit records [on business days when security related events are forwarded to the Enterprise Logging Platform for automated analysis and correlation, otherwise on a periodic basis (specific period recommended by the GSA S/SO or Contractor and approved by the GSA AO)] for indications of [GSA S/SO or Contractor recommended inappropriate or unusual activity as approved by the GSA AO]; and

b. Reports findings to [Information System Security Manager, Information System Security Officer, System Owner, Custodian, as designated and approved by the GSA AO, via a dashboard when security related events are forwarded to the Enterprise Logging Platform, otherwise via manual reporting mechanisms].

Control Enhancements:

(1) Audit Review, Analysis, and Reporting | Process Integration. The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.

(3) Audit Review, Analysis, and Reporting | Correlate Audit Repositories. The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.

(5) Audit Review, Analysis, and Reporting | Integration / Scanning and Monitoring Capabilities. The organization integrates analysis of audit records with analysis of [information system monitoring information; GSA S/SO or Contractor recommended]
data/information collected from other sources as approved by the GSA AO] to further enhance the ability to identify inappropriate or unusual activity.

(6) Audit Review, Analysis, and Reporting | Correlation with Physical Monitoring. The organization correlates information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.

GSA Implementation Guidance: Control AU-6 is applicable at all FIPS 199 levels. Enhancements AU-6(1) and (3) are applicable at the FIPS 199 Moderate level. Enhancements AU-6(1), (3), (5) and (6) are applicable at the FIPS 199 High level. AU-6 and 6(1) are Hybrid Controls for Federal systems, shared between GSA’s SecTools FISMA system and the Federal Systems. AU-6(5) and 6-(6) are Hybrid Controls, shared between the OCISO ISO Division and the Federal Systems. AU-6 and all of its enhancements are System-Specific Controls for Contractor systems. AU-6(3) is Common Control provided by GSA SecTools.

Table 3-3 identifies, at the various system layers, who is responsible for reviewing logs.

<table>
<thead>
<tr>
<th>System Layers</th>
<th>Who Reviews Logs (Integrated with ELP)</th>
<th>Who Reviews Logs (Not Integrated with ELP)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Service Provider (e.g., AWS)</td>
<td>SecOps (Only Reviewed Under Incident)</td>
<td>System Team</td>
</tr>
<tr>
<td>Operating Systems</td>
<td>SecOps (Only Reviewed Under Incident)</td>
<td>System Team</td>
</tr>
<tr>
<td>Log types reviewed only if PII or sensitive data (e.g., financial, CUI) is in scope:</td>
<td>System Team</td>
<td>System Team</td>
</tr>
<tr>
<td>- Databases</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Applications</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Tools</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Agent/Device Events</td>
<td>SecEng</td>
<td>System Team</td>
</tr>
</tbody>
</table>

Federal System Common Control Implementation:
For systems integrated with the ELP, aggregated and correlated logs and security-related events within the ELP are reviewed by GSA OCISO ISO Division for indications of compromise on business days. If these reviews indicate a possible compromise that is not already indicated on the ELP dashboard, the GSA OCISO ISO division will initiate a manual report. For enhancements AU-6(1) and (3) implementation guidance is provided in CIO-IT Security 18-90, “Information Security Program Plan (ISPP).”

For enhancement AU-6(5) and (6)—applicable to FIPS 199 High systems, as requested the GSA OCISO ISO Division will coordinate with the GSA Incident Response Team to integrate analysis from other sources while suspicious activities are investigated.

Federal System System-Specific Expectation:
For systems not integrated with the ELP and for logs not sent to the ELP, the system owner maintains the responsibility to ensure information system logs are reviewed for unusual activity.
on a periodic basis defined on a system-by-system basis as approved by the GSA AO. Logs must be kept to validate that such a review has taken place. Systems storing and/or processing PII or sensitive (e.g., financial, CUI) data must review database/application/tool logs. Systems without such data are not required to review database/application/tool logs.

For systems hosting PII/sensitive (e.g., financial, CUI) data, system personnel assigned by the System Owner, are responsible for conducting reviews for anomalous activity for layers identified in Table 3-3. A list of specific anomalous activities for a system with PII/sensitive (e.g., financial, CUI) should be identified for review and analysis. Some examples are:

- Unusual authentication and authorization events
- Unauthorized data or content manipulation
- Excessive web application or database activity
- Unauthorized or unusual transactions

Teams must define their own approach for conducting review of these events and activities, at a frequency accepted and approved by the AO. It is not necessary for every team to deploy their own centralized tool such as a SIEM in order to comply with this guide. Teams can construct an approach which covers audit log review within specific applications, tools, and databases that form their system.

Example methods that could be used for audit log review are:

- Create a roster for audit log review that assigns one team member to this function every week
- Create a form to certify that audit log review has been conducted on a given day/week by a specific member of the team. For example, a Google Form can be used.
- The reviewer reviews Drupal logs daily, looking for authentication events which occurred outside of normal business hours.

Implementation guidance is provided in CIO-IT Security 18-90, “Information Security Program Plan (ISPP),” for enhancements AU-6(1) and (3).

For enhancement AU-6(5) and (6)—applicable to FIPS 199 High systems, as requested the GSA OCISO ISO division will coordinate with the GSA Incident Response Team to integrate analysis from other sources while suspicious activities are investigated.

**Additional Contractor System Considerations**: Vendors/contractors are required to comply with the control statements.

### 3.8 AU-7 Audit Reduction and Report Generation

**Control**: The information system provides an audit reduction and report generation capability that:

- Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and
b. Does not alter the original content or time ordering of audit records.

Control Enhancements:

(1) Audit Reduction and Report Generation | Automatic Processing. The information system provides the capability to process audit records for events of interest based on:

- Source IP
- Destination IP
- Account Names
- Date and Time of Events
- Event Type.

GSA Implementation Guidance: Control AU-7 and enhancement AU-7(1) are applicable at the FIPS 199 Moderate and High Levels. AU-7 and 7(1) are Hybrid Controls for Federal systems, shared between GSA’s SecTools FISMA system and the Federal systems, and System-Specific Controls for Contractor systems.

Federal System Common Control Implementation:
Common control implementation guidance is provided in CIO-IT Security 18-90, “Information Security Program Plan (ISPP),” for systems integrated with the ELP for AU-7 and AU-7(1).

Federal System System-Specific Expectation:
System-specific implementation guidance is provided in CIO-IT Security 18-90, “Information Security Program Plan (ISPP),” for systems integrated with the ELP for AU-7 and AU-7(1).

Systems not integrated with the ELP, and logs that are not forwarded to the ELP, must have a capability to support the audit review, analysis, reporting, and investigation requirements specified by the control requirements. The capability must not alter the original content or time ordering of audit records.

Additional Contractor System Considerations: Vendors/contractors are required to comply with the control statements.

3.9 AU-8 Time Stamps

Control: The information system:

a. Uses internal system clocks to generate timestamps for audit records; and
b. Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets [GSA S/SO or Contractor recommended granularity of time measurement to be approved by the GSA AO].

Control Enhancements:

(1) Time Stamps | Synchronization with Authoritative Time Source. The information system:

(a) Compares the internal information system clocks [at least hourly (the Microsoft default is every 45 minutes)] with [the internal network’s authoritative time source]; and
(b) Synchronizes the internal system clocks to the authoritative time source when
the time difference is greater than [GSA S/SO or Contractor recommended time
period as approved by the GSA AO].

GSA Implementation Guidance: Control AU-8 is applicable at all FIPS 199 levels. Enhancement
AU-8(1) is applicable at the FIPS 199 Moderate and High levels. AU-8 and 8(1) are Hybrid
Controls for Federal systems, shared between Platforms and Hosted Applications, and System-
Specific Controls for Contractor systems.

Federal System Common Control Implementation:
Platforms must be configured to record time stamps such that they can be mapped to UTC or
GMT. For systems integrated with the ELP, it maintains audit events in EST/EDT. The ELP can
receive logs in any time zone, and can display the log events in the users’ local time zone.

For AU-8(1), platforms must be configured to synchronize with the GSA time servers at
ntp.gsa.gov, which uses General Packet Radio Services (GPRS) for time synchronization. The ELP
is synchronized with ntp.gsa.gov.

Federal System System-Specific Expectation:
Systems and applications must be configured to synchronize with an authoritative time source
that is synchronized with ntp.gsa.gov, NIST, or the Cloud Service Provider’s time servers, e.g.,
Amazon Web Services.

Additional Contractor System Considerations: Vendors/contractors are required to comply
with the control statements.

3.10 AU-9 Protection of Audit Information

Control: The information system protects audit information and audit tools from unauthorized
access, modification, and deletion.

Control Enhancements:

(2) Protection of Audit Information | Audit Backup on Separate Physical
Systems/Components. The information system backs up audit records [at least weekly,
unless the data is being sent to a secondary system, e.g., the Enterprise Logging
Platform. The CISO reserves the right to determine if backups of specific audit records
are required or not] onto a physically different system or system component than the
system or component being audited.

(3) Protection of Audit Information | Cryptographic Protection. The information system
implements cryptographic mechanisms to protect the integrity of audit information and
audit tools.

(4) Protection of Audit Information | Access by Subset of Privileged Users. The organization
authorizes access to management of audit functionality to only [privileged users
specifically authorized to perform audit management functions (i.e., specified
administrators of applications, systems, networks, etc.)].
**Note:** ISSOs, ISSMs, and System Owners may be provided read access to audit data; however, they will not have access to audit management functions.

**GSA Implementation Guidance:** Control AU-9 is applicable at all FIPS 199 levels. Enhancement AU-9(4) is applicable at the FIPS 199 Moderate level. Enhancements AU-9(2), (3) and (4) are applicable at the FIPS 199 High level. AU-9, 9(2), 9(3) and 9(4) are Hybrid Controls for Federal systems, shared between Platforms and Hosted Applications, and System-Specific Controls for Contractor systems.

**Federal System Common Control Implementation:**
For AU-9 and AU-9(4), when systems are integrated with the ELP access to audit events is restricted to users authorized by the OCISO ISO Division and/or the system ISSO or ISSM. Platforms must restrict access to audit events to users authorized by the platform ISSO or ISSM. Although AU-9(2) is not required for FIPS 199 Low and Moderate systems, the ELP provides backup of audit logs for systems integrated with it sufficient to support retention requirements in AU-11. The ELP is part of the SecTools FISMA system which is a FIPS 199 Moderate system and does not receive logs from any FIPS 199 High systems. Therefore, the ELP does not support AU-9(3) regarding encryption.

**Federal System System-Specific Expectation:**
For AU-9 and AU-9(4), systems not integrated with the ELP, and logs not sent to the ELP, the system owner must protect audit logs and any tools used in support of auditing/logging functions by restricting access to only authorized personnel as designated by the ISSO or ISSM.

Enhancements AU-9 (2) and AU-9(3) are only applicable to FIPS 199 High systems.

For enhancement AU-9(2), audit logs for FIPS 199 High systems must be backed up at least weekly but preferably daily. Where possible, backups will be sent to Network Attached Storage or another form of highly redundant storage.

For enhancement AU-9(3), audit logs for FIPS 199 High systems must be encrypted at rest using encrypted disk volumes. A means of ensuring the integrity of the audit records will be implemented by leveraging mechanisms such as cryptographic checksums.

For enhancement AU-9(4), the system owner must protect the management of audit tools/functions on the local systems by restricting access to only authorized personnel as designated by the ISSO/ISSM.

**Additional Contractor System Considerations:** Vendors/contractors are required to comply with the control statements.

**3.11 AU-10 Non-Repudiation**

**Control:** The information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed [system specific actions, *e.g.*, such as electronically signing a document, approving a request, or receiving a message].
GSA Implementation Guidance: Control AU-10 is applicable at the FIPS 199 High Level. AU-10 is a Hybrid Control for Federal systems, shared between Platforms and Hosted Applications, and a System-Specific Control for Contractor systems.

Federal System Common Control Implementation: Platform System Owners are responsible for ensuring logging and audit settings are configured per GSA OCISO Security Engineering Division’s Technical Guides and Standards for their platforms. This ensures an audit trail for non-repudiation purposes.

Federal System System-Specific Expectation: System and application System Owners are responsible for ensuring that logging and audit settings are configured per GSA OCISO Security Engineering Division’s Technical Guides and Standards for their system/application. This ensures an audit trail for non-repudiation purposes.

Additional Contractor System Considerations: Vendors/contractors are required to comply with the control statement.

3.12 AU-11 Audit Record Retention

Control: The organization retains audit records for [archived for a period of not less than 180 days] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

GSA Implementation Guidance: Control AU-11 is applicable at all FIPS 199 levels. AU-11 is a Hybrid Control for Federal systems, shared between Platforms, Hosted Applications, and the ELP when a system is integrated with the ELP. It is a System-Specific Control for Contractor systems.

Federal System Common Control Implementation: Systems integrated with the ELP will have their forwarded audit records stored for at least 180 days. Such records do not simultaneously have to be retained at the log source though it is recommended that they be retained for 180 days, if possible.

A platform, if not integrated with the ELP, must retain audit records for at least 180 days in support of systems and applications residing on the platform.

Federal System System-Specific Expectation: For systems not integrated with the ELP and logs not sent to the ELP the system owner must ensure audit records are retained for at least 180 days. The retention method chosen should support after the fact investigation, and be compliant with policy and regulatory guidelines.

Additional Contractor System Considerations: Vendors/contractors are required to comply with the control statement.
3.13 AU-12 Audit Generation

**Control:** The information system:

- a. Provides audit record generation capability for the auditable events defined in AU-2 a. at [all components];
- b. Allows [Information System Security Manager, Information System Security Officer, System Owners (e.g., System Program Managers, System Project Managers), Custodians] to select which auditable events are to be audited by specific components of the information system; and
- c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.

**Control Enhancements:**

1. Audit Generation | System-Wide / Time-Correlated Audit Trail. The information system compiles audit records from [all components] into a system-wide (logical or physical) audit trail that is time correlated to within [1 minute of UTC].

2. Audit Generation | Changes by Authorized Individuals. The information system provides the capability for [Administrators (Application, System, Network, etc.), Information System Security Officer, Information System Security Manager, System Owners (e.g., System Program Managers, System Project Managers)] to change the auditing to be performed on [all components] based on [change management decisions] within [minutes].

**GSA Implementation Guidance:** Control AU-12 is applicable at all FIPS 199 levels. Enhancements AU-12(1) and (3) are applicable at the FIPS 199 High level. AU-12 is a Hybrid Control for Federal systems, shared between Platforms and Hosted Applications, and a System-Specific Control for Contractor systems. AU-12(1) and (2) are System-Specific Controls for both Federal and Contractor systems.

**Federal System Common Control Implementation:**

GSA information systems must be able to generate audit records for the auditable events specified in AU-2a with the content in AU-3 for all information system components. System Owners, Custodians, ISSOs, and ISSMs must collaborate on which specific events are to be audited by specific components.

Platforms, including the cloud service provider layer where applicable, must coordinate with systems and applications they support to ensure that components at the platform level meet the AU-12 requirement.

Below are examples of system components and the logs associated with them that are capable of generating audit records.

Table 3-4: Examples of System Component Logs
### System Components

<table>
<thead>
<tr>
<th></th>
<th>Logs</th>
</tr>
</thead>
</table>
| Cloud Service Provider (e.g., AWS, Azure, etc.) | • Cloud Trail  
• CloudWatch logs (if used for security alerting)  
• VPC Flow logs |
| Operating Systems | • Linux/UNIX  
• Windows |
| Databases    | • Oracle  
• MySQL  
• PostgreSQL  
• Others |
| Applications | • Apache  
• Drupal  
• WordPress  
• Solr  
• Security agents  
• Others |
| Tools        | • Jenkins  
• Tableau  
• Others |
| Security Agent/Device Events | • Bit9  
• ClamAV  
• Others |

For enhancement AU-12(1), audit records must be time correlated to within 1 minute of UTC.

For enhancement AU-12(3), on a case-by-case basis, coordination between the GSA OCISO ISO and ISE Divisions, System Owners, and ISSOs/ISSMs can identify changes to system auditing and, following the system’s change management process, adjust auditing as necessary.

**Additional Contractor System Considerations:** Vendors/contractors are required to comply with the control statements.

### 4 Audit and Accountability and Supply Chain Risk Management

NIST SP 800-161, recommends Information and Communication Technology (ICT) Supply Chain Risk Management (SCRM) practices be used for FIPS 199 High systems. ICT SCRM processes increase the costs, both financial and time expended in supporting them, not just for GSA, but also for system integrators, suppliers, and service providers. ICT SCRM should be considered in the context of the system’s missions, operational environments, and risks. Due to the increased costs involved in incorporating SCRM in auditing and accountability the System Owner, IST Division Director, ISSM, and ISSO must carefully consider these costs prior to incorporating system specific SCRM processes into audit and accountability controls. Any questions with regard to including SCRM controls should be sent to ispcompliance@gsa.gov.

NIST SP 800-161 states, “Audit and accountability controls for ICT SCRM provide information useful in case of an ICT supply chain compromise. Organizations should ensure that they designate and audit ICT supply chain-relevant events within their information system boundaries using appropriate audit mechanisms (e.g., system logs, Intrusion Detection System...
(IDS) logs, firewall logs, paper reports, forms, clipboard checklists, digital records). These audit mechanisms should also be configured to work within reasonable time-frame boundaries, as defined by organizational policy. Organizations may encourage their system integrators and external service providers to do the same and may include in agreements requirements for such monitoring. However, organizations should not deploy audit mechanisms on systems outside of their organizational boundary, including those of system integrators and external service providers.”

The AU controls addressed in NIST SP 800-161 are provided in the following sections along with NIST SP 800-161 supplemental guidance on the controls and GSA’s implementation guidance.

4.1 AU-1 Audit and Accountability Policy and Procedures (ICT SCRM)

NIST SP 800-161 Supplemental ICT SCRM Guidance: Audit mechanisms provide data for tracking activities in an organization’s ICT supply chain infrastructure. Audit and accountability policy and procedures should appropriately address such tracking and its availability for other various ICT supply chain activities, such as configuration management. System integrator, supplier, and external service provider activities should not be included in such policy, unless those are performed within the acquirer’s ICT supply chain infrastructure.

GSA Implementation Guidance: FIPS 199 High systems that have incorporated SCRM must identify how AU policy and procedures address audit mechanisms supporting ICT SCRM tracking activities and its use for other ICT supply chain activities, including configuration management.

Additional Contractor System Considerations: Contractor systems may defer to GSA policy and procedures or separately implement audit and accountability policy and procedures that facilitate the implementation of SCRM.

4.2 AU-2 Audit Events (ICT SCRM)

NIST SP 800-161 Supplemental ICT SCRM Guidance: An observable occurrence within the information system or ICT supply chain infrastructure should be identified as an ICT supply chain auditable event, based on the organization’s SDLC context and requirements. Auditable events may include software/hardware changes, failed attempts to access ICT supply chain infrastructure systems, or movement of source code. Information on such events should be captured by appropriate audit mechanisms and should be traceable and verifiable. Information captured may include type of event, date/time, length, and frequency of occurrence. Among other things, auditing may help detect misuse of the ICT supply chain infrastructure caused by insider threat.

GSA Implementation Guidance: FIPS 199 High systems that have incorporated SCRM must identify observable occurrences that can be captured, such as events described in the NIST supplemental guidance above, based on the system’s SDLC context and requirements. These events or occurrences should be traceable and include the event and date/time of occurrence.
**Additional Contractor System Considerations:** Vendor/contractor systems are required to comply with the control per the guidance above.

### 4.3 AU-6 Audit Review, Analysis, and Reporting (ICT SCRM)

**NIST SP 800-161 Supplemental ICT SCRM Guidance:** The organization should ensure that both ICT supply chain and information security auditable events are appropriately filtered and correlated for analysis and reporting. For example, if new maintenance or a patch upgrade is recognized to have an invalid digital signature, the identification of the patch arrival qualifies as an ICT supply chain auditable event, while invalid signature is an information security auditable event. The combination of these two events may provide information valuable to ICT SCRM.

**Control Enhancements:**

(9) Audit Review, Analysis, and Reporting | Correlation with Information from Nontechnical Sources. In an ICT SCRM context, nontechnical sources include changes to organizational security or operational policy, changes to procurement or contracting processes, and notifications from system integrators, suppliers, and external service providers regarding plans to update, enhance, patch, or retire/dispose of a system/component.

**GSA Implementation Guidance:** FIPS 199 High systems that have incorporated SCRM must identify how the review, analysis, and reporting of SCRM events (e.g., receipt of invalid hardware or software) is integrated with other audit events, including nontechnical sources such as notifications from suppliers/integrators, to determine if a root cause or flaw in the supply chain can be identified.

**Additional Contractor System Considerations:** Vendor/contractor systems are required to comply with the controls per the guidance above.

### 4.4 AU-10 Non-Repudiation (ICT SCRM)

**NIST SP 800-161 Supplemental ICT SCRM Guidance:** Organizations should implement non-repudiation techniques to protect both information systems and ICT supply chain infrastructure. Examples of what may require nonrepudiation include ICT supply chain metadata describing the components, ICT supply chain communication, delivery acceptance information, etc. For information systems, it can be patch or maintenance upgrades for software as well as component replacement in a large hardware system. Verifying that such components originate from the OEM is part of non-repudiation.

**Control Enhancements:**

(1) Non-Repudiation | Association of Identities. This enhancement helps traceability in ICT supply chain. It also facilitates the accuracy of provenance.

(2) Non-Repudiation | Validate Binding of Information Producer Identity. This enhancement validates the relationship of provenance and the component. Therefore, it ensures integrity of provenance.
(3) Non-Repudiation | Chain of Custody. Chain of custody is fundamental to provenance and traceability in the ICT supply chain. It also helps verification of system and component integrity.

**GSA Implementation Guidance:** FIPS 199 High systems that have incorporated SCRM must include a description of how non-repudiation techniques protect the supply chain and any actions taken when non-repudiation of actions is not verified. For example, describing how components (hardware or software) have been verified as having come from the manufacturer and have not been modified without authorization using practices such as validating that the producer is bound to a component, or verifying the chain of custody of components.

**Additional Contractor System Considerations:** Vendor/contractor systems are required to comply with the controls per the guidance above.

### 4.5 AU-12 Audit Generation (ICT SCRM)

**NIST SP 800-161 Supplemental ICT SCRM Guidance:** Organizations should ensure that audit generation mechanisms are in place to capture all relevant supply chain auditable events. Examples of such events include: component version updates, component approvals from acceptance testing results, logistics data-capturing inventory or transportation information, etc.

**GSA Implementation Guidance:** FIPS 199 High systems that have incorporated SCRM must identify how they include audit generation sources (e.g., receipt data concerning components—analysing how it was received, configuration management approvals for updates, acceptance of test results, etc.) supporting supply chain events.

**Additional Contractor System Considerations:** Vendor/contractor systems are required to comply with the control per the guidance above.

### 4.6 AU-13 Monitoring for Information Disclosure (ICT SCRM)

**NIST SP 800-161 Supplemental ICT SCRM Guidance:** Within the ICT SCRM context, information disclosure may occur via multiple avenues including open source information. For example, supplier-provided errata may reveal information about an organization’s system that may provide insight into the system that increases the risk to the system.

**GSA Implementation Guidance:** FIPS 199 High systems that have incorporated SCRM must describe how they monitor supplier information for evidence of unauthorized disclosure of organizational information (e.g., error messages providing organizational or system information that malicious actors could use.)

**Additional Contractor System Considerations:** Vendor/contractor systems are required to comply with the control per the guidance above.
4.7 AU-16 Cross-organizational Auditing (ICT SCRM)

NIST SP 800-161 Supplemental ICT SCRM Guidance: In an ICT SCRM context, this control includes the organization’s use of system integrator or external service provider infrastructure.

Control Enhancements:

(2) Cross-organizational Auditing | Sharing of Audit Information. Whether managing a distributed audit environment or an audit data-sharing environment between organizations and its system integrators or external services providers, organizations should establish a set of requirements for the process of sharing audit information. In the case of the system integrator and external service provider and the organization, a service-level agreement of the type of audit data required vs. what can be provided must be agreed to in advance to ensure that the organization obtains the relevant audit information needed for ensuring that appropriate protections are in place to meet its mission operation protection needs. Ensure that coverage of both information systems and ICT supply chain infrastructure are addressed for the collection and sharing of audit information.

GSA Implementation Guidance: FIPS 199 High systems that have incorporated SCRM must methods used to accomplish cross-organizational auditing and how any relevant auditing information will be shared with other organizations (e.g., a cross-organizational sharing agreement).

Additional Contractor System Considerations: Vendor/contractor systems are required to comply with the controls per the guidance above.

5 Summary

Auditing, when properly implemented, helps to accomplish several security-related objectives, including but not limited to individual accountability, detecting security violations and intrusions, identifying flaws in systems and applications, and supporting incident investigation and reconstruction.

The audit function including the proper setting of audit configurations and the subsequent review and analysis of resultant records is tedious and time consuming work. Accurately detecting and assessing possible incidents—determining whether an incident has occurred and, if so, the type, extent, and magnitude of the problem is challenging but made easier with automated tools. Such tools can make logs far more useful and reduce the amount of time required for review. Even with automated tools, reviewers must be skilled in information security and know what to look for. They must be effective in spotting unusual activity, understand the normal activity for the systems, and able identify and understand attacks.

Where there is a conflict between NIST guidance and GSA guidance, contact the OCISO, ISP Division for guidance, at ispcompliance@gsa.gov.