Office of Information Technology

1902 Audit and Accountability Policy

2026-11-04

Table of Contents

Policy . . . 2
Authority . . . 3
References . . . 4
Applicability . . . 5
Definitions . . . 6
Responsibilities . . . 7
- AU-1 Audit and Accountability Policy . . . 7
- AU-2 Auditable Events . . . 7
- AU-3 Content of Audit Records . . . 8
- AU-4 Audit Storage Capacity . . . 9
- AU-5 Response to Audit Processing Failures . . . 9
- AU-6 Audit Review, Analysis, and Reporting . . . 9
- AU-7 Audit Reduction and Report Generation . . . 10
- AU-8 Time Stamps . . . 10
- AU-9 Protection of Audit Information . . . 10
- AU-10 Non-Repudiation . . . 11
- AU-11 Audit Record Retention . . . 11
- AU-12 Audit Generation . . . 11
- AU-16 Cross-Agency Auditing . . . 11

History . . . 13
Evaluation . . . 14

	Department of Human Services Online Directives Information System	Index:	POL1902
		Revised:	06/02/2025
		Next Review:	06/02/2027

Subject: DHS Information Security Policies

Policy

This policy establishes the Agency Audit and Accountability Policy, for managing risks from inadequate event logging and transaction monitoring through the establishment of an effective Audit and Accountability program. The audit and accountability program helps DHS implement security best practices with regard to event and transaction logging and the retention of audit evidence.

Authority

1. United States Department of Commerce National Institute for Standards and Technology (NIST)
2. United States Internal Revenue Service
3. United States Department of Health & Human Services – Administration of Children and Families (ACF), Office of Child Support Services (OCSS)
4. United States Department of Health & Human Services - Centers for Medicare & Medicaid Services (CMS)
5. Georgia Technology Authority
6. Social Security Administration
7. Federal Bureau Investigation (Criminal Justice Information Services)

References

- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations, Revision 5, December 2020
- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-100 “Information Security Handbook: A Guide for Manager” March 2007
- Federal Information Security Management Act of 2002 (FISMA)
- Georgia Technology Authority Enterprise Information Security Policy
- United States Internal Revenue Service, IRS Publication 1075 Tax Information Security Guidelines For Federal, State and Local Agencies Safeguards for Protecting Federal Tax Returns and Return Information
- Centers for Medicare & Medicaid Services, Volume II: Minimum Acceptable Risk Standards for Exchanges
- Social Security Administration (“SSA”) Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the Social Security Administration (“TSSR”)
- Criminal Justice Information Services Security Policy
- ACF/OCSS - Security Agreement

Applicability

The scope of this policy is applicable to all Information Technology (IT) resources owned or operated by DHS. Any information, not specifically identified as the property of other parties, that is transmitted or stored on DHS IT resources (including email, messages, and files) is the property of DHS. All users (DHS employees, contractors, vendors, or others) of IT resources are responsible for adhering to this policy.

Definitions

Controlled Unclassified Information (CUI)

Controlled Unclassified Information (CUI) is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended.

Responsibilities

DHS shall adopt the Audit and Accountability principles established in NIST SP 800-53 “Audit and Accountability Control Family guidelines,” as the official policy for this domain. The following subsections outline the Audit and Accountability standards that constitute DHS policy. Each DHS Business System is then bound to this policy and shall develop or adhere to a program plan which demonstrates compliance with the policy related the standards documented. In conjunction with appropriate tools and procedures, audit trails will assist in detecting security violations, performance problems, and flaws in applications.

AU-1 Audit and Accountability Policy

a. Develop, document, and disseminate to designated agency personnel:
    1. All organizational level audit and accountability policy that:
        i. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
        ii. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
    2. Procedures to facilitate the implementation of the audit and accountability policy and the associated controls.
b. Designate an **agency official** to manage the development, documentation, and dissemination of the audit and accountability policy and procedures; and
c. Review and update the current audit and accountability:
    i. Policy every **one (1) year (or if there is a significant change)**; and
    ii. Procedures every **one (1) year, (or when there is a significant change)**.

AU-2 Auditable Events

1. Identify the types of events that the system is capable of logging in support of the audit function and assign account managers:
    a. All accesses or attempts to access a CUI system, including the identity of each user and device;
    b. Log off system;
    c. Activities that might modify, bypass, or negate IT security safeguards;
    d. Security-relevant actions associated with processing CUI;
    e. User generation of reports and extracts containing CUI;
    f. Any interaction with CUI through an application
    g. Viewing of screens that contain CUI;
    h. Password changes;
    i. Creation or modification of groups;

j. Privileged user actions;
k. Access to the system;
l. Creating and deleting files;
m. Change of permissions or privileges;
n. Command line changes and queries;
o. Changes made to an application or database;
p. System and data interactions;
q. Opening and/or closing of files; and
r. Program execution activities.

2. Coordinate the event logging function with other organizational entities requiring audit related information to guide and inform the selection criteria for events to be logged
3. Specify the following event types for logging within the system: agency-defined subset of AU-2 1. requirements (e.g. Systems capable of required event types relevant to the use or administration of CUI
4. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and
5. Review and update the event types selected for logging annually or when there is a system change. Document changes in the SSR and/or SSP.

AU-3 Content of Audit Records

1. Configure information systems to generate audit records containing sufficient information to establish what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. At a minimum, the following elements shall be identified within each audit record:
   a. What type of event occurred
   b. When (date and time) the event occurred
   c. Where the event occurred
   d. Source of the event
   e. Outcome (success or failure) of the event
   f. Identity of any individuals, subjects, or objects/entities associated with the event

AU-3 (1) *Additional Audit Information:*

Generate audit records containing the following additional information and event details explicitly needed for audit requirements:

a. Details that facilitate the reconstruction of events if
   i. Unauthorized activity occurs or is suspected; or

ii. A malfunction occurs or is suspected.

AU-3 (3) *Limit Personally Identifiable Information Elements:*

Limit personally identifiable information contained in audit records to the following elements identified in the privacy risk assessment: agency- defined elements.

AU-4 Audit Storage Capacity

Allocate audit storage capacity to accommodate at a minimum, storage capacity of ninety (90) days and any other organization-defined audit log retention requirement.

AU-5 Response to Audit Processing Failures

1. Alert designated organizational officials (e.g., SA,/ISSO) in the event of an audit processing failure.
2. Take the following additional actions:
    a. Monitor system operational status using operating system or system audit logs and verify functions and performance of the system. Logs shall be able to identify where system process failures have taken by the system administrator.
    b. If logs are not available, shut down the system.
    c. Shut down systems that do not support automatic shutdown within one (1) hour of the audit processing failure.

AU-5 (1) *Storage Warning Capacity:*

Provide a warning to the SA and ISSO within 24 hours when allocated audit record storage volume is reaches a specified percentage of repository maximum audit log storage capacity.

AU-6 Audit Review, Analysis, and Reporting

1. Review and analyze system audit records weekly for indications of inappropriate or unusual activity and the potential impact of the inappropriate or unusual activity involving CUI.
2. Report findings to the individual(s) specified within the agency's incident response procedures; and
3. Adjust the level of audit review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.

AU-6 (1) *Automated Process Integration:*

Integrate audit record review, analysis, and reporting processes using automated mechanisms to support organizational processes for investigation and response to suspicious activities.

AU-6 (3) *Correlate Audit Repositories:*

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

AU-6 (7) *Permitted Actions:*

Specify the permitted actions for each role or user associated with the review, analysis, and reporting of audit record information.

AU-6 (9) *Correlation with Information from Nontechnical Sources:*

Correlate information from nontechnical sources with audit record information to enhance organization-wide situational awareness.

AU-7 Audit Reduction and Report Generation

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

AU-7 (1) *Automatic Processing:*

Provide and implement the capability to process, sort, and search audit records for events of interest based on the following content: likelihood of potential inappropriate access or unauthorized disclosure of CUI.

AU-8 Time Stamps

1. Use internal system clocks to generate time stamps for audit records; and
2. Record time stamps for audit records that are accurate to within one hundred (100) milliseconds and that use Coordinated Universal Time (UTC), or that include the local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.

AU-9 Protection of Audit Information

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

AU-9 (4) *Access by Subset of Privileged Users:*

Authorize access to management of audit logging functionality to only authorized security administrators.

AU-10 Non-Repudiation

Provide irrefutable evidence that an individual (or process acting on behalf of an individual) has performed organization-defined actions to be covered by non-repudiation.

AU-11 Audit Record Retention

a. Audit records on agency information systems that host, store, and transmits CUI data are maintained for **90 days** and archive old records for **one year**.

b. Audit records for information systems which host, store and transmits CUI data to support after-the- fact investigations of security incidents and to meet regulatory and organizational information retention requirements are maintained for **seven years** for IRS and **ten years** for CMS.

AU-11 (1) Long-Term Retrieval Capability

Employ organization-defined measures to ensure that long-term audit records generated by the system can be retrieved.

AU-12 Audit Generation

DHS shall:

a. Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2a on all systems that receive, process, store, access, protect and/or transmit CUI;

b. Allow SA and ISSO to select the event types that are to be audited by specific components of the system; and

c. Generate audit records for the events types defined in AU-2c that include the audit record content defined in AU-3.

AU-12 (1) *System-Wide and Time-Correlated Audit Trail:*

Compile audit records from systems that receive, process, store, access, protect and/or transmit FTI into a system-wide logical audit trail that is time-correlated to within agency-defined level of tolerance for the relationship between time stamps of individual records in the audit trail.

AU-16 Cross-Agency Auditing

DHS employs agency defined mechanisms for coordinating agency-defined audit information among external organizations when audit information is transmitted across agency boundaries.

AU-16 (1) *Identity Preservation:*

Preserve the identity of individuals in cross-organizational audit trails.

AU-16 (2) *Sharing of Audit Information:*

Provide cross-organizational audit information to agency-defined organizations based on agency-defined cross-organizational sharing agreements.

History

Date	Change/Review	Reviewed By	Version
5/1/2026	Review	Manju Balachander	N/A

Evaluation

The Office of Information Technology (OIT), upon recommendation of the DHS Chief Information Security Officer (CISO), evaluates this policy annually by:

1. Comparing its content and intent to evolving regulatory compliance standards imposed upon the Agency, such as, IRS 1075, NIST 800-53, and CMS MARS-E.
2. Addressing any deficiencies or gaps discovered during periodic audits conducted by Georgia DOAA or other regulatory bodies, such as, IRS, CMS, SSA, FBI, etc.