U.S. Customs and Border Protection

Attachment T

Auditing Procedures

HB 1400-05D
Information Systems Security Policies and Procedures Handbook

Version 2.0

July 27, 2009

DOCUMENT CHANGE HISTORY

Version	Date	Description
1.0	July 27. 2009	Initial CBP 1400-05D release is based solely on existing 1400-05C, Version 2.1 appendices which were found to be unrelated to existing DHS 4300A, Version 6.1.1 attachments. The policy content of this attachment is exactly the same as the 1400-05C, Version 2.1 appendix. It is now presented in the attachment format.
2.0	December 21, 2010	No changes

CONTENTS

All CBP information systems are required to have audit trail capabilities in order to meet security requirements for auditing in accordance with the Computer Security Act of 1987 and the Computer Security Enhancement Act of 1996. Security-relevant events must be captured and these events will be defined after analyzing business and IA requirements, and assessing the impact of the system architecture and design alternatives.

This attachment provides specific procedures and instructions on what information must be contained in audit trail records, how to implement an audit trail, and what should be checked for in an audit review. Additionally, guidelines to implement audit capabilities are detailed in NIST SP 800-53, which supports the Federal Information Security Management Act (FISMA) of 2002.

1.0 AUDIT-TRAIL RECORDS

For systems processing sensitive or classified, audit records must be sufficient in detail to facilitate the reconstruction of events if compromise or malfunction occurs or is suspected. The ISSO and SA are responsible for the implementation of the audit trail capability in the operational environment. Audit records shall be reviewed as previously specified or in the System Security Plan (SSP). The type of security events captured within an audit record should be considered annually by the ISSO. The audit record shall contain at least the following information:

1. Identity of each user and device accessing or attempting to access an IT system.
    a. Personnel access, and authentication.
2. Time and date of the access log-on and the log-off.
3. Activities that might modify, bypass, or negate IT security safeguard.
    a. Unauthorized attempts to access files or programs.
    b. Program aborts and anomalies.
4. Security-relevant actions associated with processing.
    a. Disconnects and outages of remote terminals and peripheral devices.
    b. Generated hardcopy outputs
    c. Security anomalies that occur in the network that provide for reconstructing the activities of users, processes, and terminals.
5. All activities performed using an administrator's identity.
    a. Start/stop time of events changing role-based access controls.
    b. All functions initiated by the system's console operators.
6. Time of log-on and log-off (date and time).

If any of the above items are not included in audit trail records, those items require documented justification by the ISSO. Only the Assistant Commissioner, OIT, can waive audit trail requirements under extreme circumstances. If the audit trail requirement is waived, user authentications, file passwords, magnetic media-control procedures, and a logging mechanism for recording terminal usage, must be implemented.

2.0 AUDIT-TRAIL IMPLEMENTATION

An audit-trail capability must be automated. Many computer contingency plans require data similar to that needed for security-audit purposes. The data used for file recovery can actually substitute for some parts of the security audit-trail. In some cases, the software to support contingencies may be used to accommodate audit-trail implementation. The following are requirements for audit-trail implementation:

Automated. Audit-trail software must be able to accomplish the following actions:

1. Create and maintain a record of accesses to the data it protects.
2. Protect audit software and data from unauthorized access, tampering, or destruction.
3. Restrict read access of audit data to the ISSO and the SA, if applicable.
4. Support permanent storage of audit data residing on separate storage media from the media where files and data are processed.

Manual. Manual logs have been determined to be insufficient as audit trails and cannot be relied on for audit trail purposes. Therefore, automated audit-trail software shall be used whenever possible.

3.0 AUTOMATED AUDIT-TRAIL PROCEDURES

1. Protect audit-trail data at the same security level as the information used by the system.
2. If hard-copy audit-trail products are generated on a system, print them on continuous paper whenever possible. If continuous paper is not used, all pages will be numbered with a sequence number on each printed line. This is required to protect the integrity of the audit-trail data. In order to reduce workload, generate a report that reflects a particular anomaly rather than listing the entirety of the audit-trail database, if possible.
3. Generate summary reports to reduce storage volume of detailed information and produce them at least every thirty days. Summary reports may eliminate time-related detailed records but retain higher-level information by date such as who performed what functions and to what databases.
4. Document the archival procedures for audit data.

5. Document an alternate procedure to archive audit data in the event of completely filled audit files. This procedure must document the system alerts for this event, automated roll-over to an alternate file, and/or system shut down.

4.0 AUDIT-TRAIL CHECKS AND REVIEWS

The ISSO or SA must perform reviews of the automated audit-trail logs to ensure that all pertinent activity is properly recorded and appropriate action has been taken to correct any anomaly. Audit trail checks and reviews must include the following tasks:

1. Review audit-trails on a routine basis.

2. Review system audit-trails when a potential security violation, compromise or deviation occurs and as soon as possible after the occurrence.

3. Notify the CISO of detected anomalies.

4. Report incidents to the CSIRC, as appropriate.

5. Review, alert and follow-up actions must be recorded and documented.

6. Audit Trails must be maintained online for at least ninety days, thereby allowing rapid access to recent information. Audit trails should be preserved for a minimum of seven years as part of managing records for each system to allow audit information to be placed online for analysis with reasonable ease. Unique systems with unique data might require a longer period of retention to support their mission objectives. Retain summary reports for one year.