DHS ADMINISTRATIVE PROCEDURES MANUAL

Chapter 120

Title: Information Systems Security Audit and Compliance Procedures

I. Applicability

These procedures establish a framework for conducting audit related reviews and compliance requirements of information resources at DHS in accordance with all applicable state and federal regulations. All DHS employees, Business Associates, contractors, and vendor partners must comply.

II. Scope

(a) Security Audits can be conducted on any entity within DHS or any outside entity that has signed a Business Associate Agreement or Third-Party Agreement with DHS. Security Audits can be conducted on any information system, to include applications, servers, networks, devices, and any process or procedure by which these systems are administered and/or maintained.

(b) Employees, contractors, and vendor partners of DHS are subject to the policies and procedures of DHS and the Department of Information Systems. Some of those include manual or automated controls (where possible) that can result in a formal review by the DHS Chief Information Security Officer (CISO), an external auditor, or law enforcement, as appropriate.

(c) This procedure plays a key role in security design, providing both preventative controls through alerts of suspicious activity and forensic security records of events essential for incident investigation. Capable components in the protected systems must record security relevant events and will record events to either a local logging facility or by sending events to DHS authorized process.

III. Failure to Comply

Failure to comply with these procedures as well as any DHS IT Security Policy or Procedure may result in restriction or suspension of all network access to DHS systems or applications. Employees who cannot complete job duties or assignments without such access may be terminated or face disciplinary action as outlined in DHS Policies 4002 “Privacy and Security Sanctions” and 1084, “Employee Discipline.”

IV. Procedures

(a) All audits from external sources related to the security of systems, applications, or data are to be coordinated with the DHS IT Security Office and DHS Privacy Office prior to the audit.

(b) The IT Security Office and the DHS Privacy Office will conduct security audits and reviews of identified systems and resources at least once a year as required by federal and state regulations and in support of assessing the security posture of the organization's critical and business systems. The IT Security Office will develop and maintain a review methodology to include the following:

(1) Audit/ Review approval procedures;

(2) Internal Inspections Plan;

(3) Preliminary risk analysis;

(4) Planning phase;

(5) Testing phase;

(6) Communicating results;

(7) Remediation validation; and,

(8) Final reporting.

(c) Audits and reviews must be approved in writing by the DHS CISO and the CIO. In addition, detailed documentation of all audits must be produced and securely archived by the IT Security Office in compliance with DHS retention policies. Work may be performed completely in-house or by an outside firm. In addition, the IT Security Office will collect and monitor applicable log data to identify intrusion attempts and potential attacks. Audit logs will be maintained per the "Information Systems Change Management Procedure" (APM 124).

(d) DHS entities and personnel will provide the appropriate divisions with timely and complete responses to all audit results, Plans of Action & Milestones ((POAMs), and corrective action plans required.

(e) Audits will be performed based on federal and state guidelines as needed. The baseline for compliance will be based on FISMA (NIST) and modified based on the federal and state laws that may apply to the application or division. Programs containing access to FTI data will follow the internal inspections plan at minimum of every eighteen (18) months in addition to the standard audit.

(f) Log aggregation, correlation, alerting, and retention requirements will be met using a Security Information and Event Management (SIEM) tool. The IT Security Office includes a security component and continuity of operations component. These maintain an overview of the DHS' risks, operational issues, mitigating controls, and recovery methods including some audit related functions.

(g) The IT Security Office will define procedures to include inspections for compliance with federal, state, and local laws and regulations based on alignment with Federal Information Management Security Act (FISMA), National Institute of Standards and Technology (NIST) 800-53, Internal Revenue Service (IRS) Publication 1075, Health Insurance Portability and Accountability Act of 1996 (HIPAA), Social Security Administration (SSA), and any other system determined to hold, collect or modify protected information.

(h) OST, Security, or System Support groups may request device specifics (such as Operating System (OS), version, and patch level) for review – especially for devices that cannot support any service account ID. The CISO must approve any additions to the system. The CIO shall be notified when operational issues may arise and before making changes within the change management process. All changes shall be approved by the CIO or designee.

(i) Primary accounts shall be defined by the CISO and other applicable groups.

(j) If the device supports login credentials (local or directory based [such as Active Directory or LDAP]), the entity responsible for configuring the device will include an audit service account on the device as specified below. The SIEM reports real-time events as they occur, escalating significant events to the SIEM administrators and security management. Logs from the enterprise intrusion prevention system, network class devices, server class devices, operating system related logs, application software logs and third-party logs, including reputation services, are incorporated into the SIEM.

(k) The inspection accounts shall be created on each applicable device with sufficient rights to allow review of all data on such a device via the device's standard operating system access methods or physical environments necessary to ensure compliance. Audit and System logs will be maintained as documented per NIST requirements.

(l) In order to meet state and federal guidelines, individuals will coordinate service accounts with the IT Security Office and other applicable support groups. All system components, including applications, databases, server operating systems, and network firewalls and proxies are required to record the following key security events to a local audit log, per the NIST security requirements for inspection:

(1) User account creation and deletion;

(2) User account enabled or disabled;

(3) User account modified;

(4) Security or audit configuration changed;

(5) Privileged task/command executed;

(6) Successful login and unsuccessful login;

(7) Successful or unsuccessful access of protected data;

(8) Network packet blocked by firewall or access control list;

(9) System startup and shutdown;

(10) User permissions changed; and,

(11) Audit logging enabled and disabled.

(m) For the events listed above in item (l), all systems will log the following data elements:

(1) Event type;

(2) Time and date using the local system clock;

(3) Source of event, including source IP address, if available;

(4) Object of event, including destination IP address, if available;

(5) Outcome (success or failure); and,

(6) Users/subjects associated with the event (or system if no user associated).

(n) System components will log either to a local logging facility, or may send events to the SEIM for logging, following the format described in the SEIM section below. For local logging, use of the operating system logging facility (syslog, Windows Event log) is preferred.

V. Vulnerability Assessment

(a) The IT Security Office will perform vulnerability assessments on systems, applications, networks, or devices where DHS data is located to the extent necessary to allow the IT Security Office or contracted company to perform the scans authorized by this procedure. DHS application owners shall provide protocols, addressing information, and network connections sufficient for auditing to utilize the software to perform network scanning.

(b) Access may include:

(1) User level and/or system level access to any computing or communications device;

(2) Access to information (electronic, hard copy, etc.) that may be produced, transmitted, or stored on DHS equipment or premise;

(3) Access to work areas (labs, offices, cubicles, storage areas, etc.); and,

(4) Access to interactively monitor and log traffic on DHS networks.

VI. Network Control

In the event DHS protected data is located outside of the DHS network, third parties will be required to perform a vulnerability assessment scan on an annual basis reporting findings to the DHS CISO and DHS Privacy Officer with a remediation plan and corrective action plan within thirty (30) days of finding the vulnerability. Failure to comply may result in loss of contract or connectivity. A risk evaluation will be performed as stated in "Information Systems Risk Management Procedures" (APM Chapter 121), to determine the risk and impact to DHS data, clients, and networks.

VII. Service Degradation and/or Interruptions

Network performance and/or availability may be affected by network scanning. The IT Security Office will plan accordingly to mitigate the impact to the network and the server.

VIII. Scanning Period

(a) DHS Application owners and the IT Security Office shall identify in writing the allowable dates and times for audit scans and periodic scans to take place. Automated application scanning will be performed at a minimum of once every quarter. Alerts will be sent to the IT Security Office for any vulnerability found during automated alert which will be addressed per the incident response procedure.

(b) DHS application owners shall identify in writing a person to be available if the IT Security Office or Privacy Office has questions regarding data discovered during the scan or if the offices require assistance in addressing an issue.

IX. Penetration Testing

Periodic penetration testing will be performed on DHS systems and applications. All scans will be non-intrusive unless approval is obtained from the application owner prior to testing. Exceptions may be made by the CIO or designee based on risk and known vulnerabilities.

X. Red/Blue Team Testing

DHS will build and train a group of engineers, security professionals, and developers to serve as active defense for cyber-attacks, breach evaluation, and vulnerability assessors. These teams will rotate responsibilities to build a strong skill set capable of protecting and evaluating the defense of DHS information systems. All actions will be coordinated with the divisions prior to the training or scenarios take place. Documentation of all actions will be recorded in a secured location for training purposes and all scenarios must be approved by the CIO and CISO prior to implementation.

XI. External Audits

Audits managed by an external company will be performed annually unless previous exclusion is given by the CIO for the fiscal year. Audits performed by other departments, agencies, or external parties shall be submitted to the IT Security Office to ensure issues are addressed to comply with state and federal regulations

XII. Evaluation of Security and Privacy Policies and Procedures

Evaluation of Security and Privacy Policies and Procedures will be performed at minimum annually per federal and state guidelines unless significant changes are made within the annual timeframe. Policies and procedures will be evaluated based on information security measurements, performance, and documented activities.

XIII. Other

(a) This procedure does not replace the auditing and monitoring responsibilities of individual system administrators and data owners.

(b) The IT Security Office oversees the DHS "Security Audit Process". For information regarding the process, contact the IT Security Office.

(c) Requests for exceptions to this procedure must be submitted in writing and approved in writing by the DHS CIO. Exceptions, if granted, will not violate compliance with any federal or state law, rule, or regulation and must be renewed by the CIO annually.

XIV. Definitions

(a) "Entity" means any business unit, department, group, or third party, internal or external to DHS responsible for maintaining DHS assets.

(b) "Risk" means those factors that could affect confidentiality, availability, and integrity of DHS's key information assets and systems. The IT Security Office is responsible for ensuring the integrity, confidentiality, and availability of critical information and computing assets, while minimizing the impact of security procedures and policies upon business productivity.

(c) "Security Audit" means formally testing and evaluating vulnerabilities and controls within the Information Technology environment, performed by an independent party, requiring independent corroboration (sampling in nature) to substantiate information provided by personnel.

(d) "Security Review" means similar evaluation performed in a security audit but typically omits obtaining independent corroboration (non-sampling in nature) and testing to substantiate information provided by personnel. Security reviews may be performed in-house or outsourced to a third party.

(e) "System Administrator" means an individual who performs network/system administration duties and or technical support of network/systems that are accessed by other people, systems, or services. Only full-time and permanent part-time employees of DHS and or third-party vendors approved by IT may function as system/network administrators.

(f) "Data Owners" means the person responsible for, or the person with administrative control over, granting access to an organization's documents or electronic files while protecting the data as defined by the DHS

IT Security policies or standard IT practices. Data owners shall only be State Employees unless approved by the DHS CIO prior to receiving this responsibility.

(g) "Application Owners" means the person responsible for development or management of an application containing DHS information.

(h) "Resource" means one element of hardware, software or data that is part of a larger system.

XV. References

(a) Arkansas Data and System Security Classification
http://www.techarch.state.ar.us/domains/security/standards/SS-70-__001_dataclass_standard.pdf>

(b) Arkansas Encryption Standard
http://www.techarch.state.ar.us/drafts/DRAFT_encryp_standardSS-70-006.pdf>

(c) CMS Minimum Acceptable Risk Standards (CMS MARS-E)
http://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Minimum-Acceptable-Risk-Standards-for-Exchanges-ERA-Supp-v-1-0-08012012-a.pdf

(d) Health Insurance Portability and Accountability Act CFR parts 160, 162 and 164 (HHS HIPAA)
http://www.hhs.gov/ocr/privacy/

(e) Health Information Technology for Economic and Clinical Health Act (HHS HITEC)
http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html

(f) Social Security Administration Safeguards (SSA)
http://www.ssa.gov/dataexchange/security.html

(g) US Privacy Act of 1974 (Dept of State)
http://foia.state.gov/Learn/PrivacyAct.aspx

(h) Cybersecurity Enhancement Act of 2014
https://www.congress.gov/bill/113th-congress/senate-bill/1353

(i) Federal Information Security Management Act of 2002 (FISMA)
http://csrc.nist.gov/groups/SMA/fisma/

(j) Internal Revenue Service (IRS) Publication 1075, pertaining to Federal Tax Information (FTI)
http://www.irs.gov/pub/irs-pdf/p1075.pdf