Homeland Security

DHS 4300A Sensitive Systems Handbook

Attachment R

Compliance Framework for CFO-Designated Systems

Version 9.1

July 24, 2012

Protecting the Information that Secures the Homeland

This page intentionally blank

Document Change History

Version	Date	Description
1.0	September 30, 2007	Initial draft
5.5	September 30, 2007	No changes. Updated version number to coincide with current Handbook.
6.0	May 14, 2008	Section 1.2.9, second bullet - Changed “Audit Trail Content” to “Audit Record Content”
6.1	September 23, 2008	No change
7.0	August 7, 2009	No change
7.1	June 21, 2010	Updated and aligned content with the revised GAO Federal Information System Control Audit Manual (FISCAM), NIST SP800-53 Rev.3, and DHS Sensitive Systems Policy Directive 4300A, Version 7.1.
7.2	March 20, 2012	Updated Section 1. to include the DHS CFO designated system key controls; added FY2012 list of CFO Designated Systems.
9.1	July 24, 2012	Edited for style, grammar, spelling, and format.

Table of Contents

1.0 INTRODUCTION

DHS Chief Financial Officer (CFO) Designated Systems are systems that require additional management accountability to ensure effective internal control exists over financial reporting. The DHS CFO publishes the approved list of CFO Designated Systems annually. Section 3.15 of DHS Sensitive Systems Policy Directive 4300A provides additional requirements for these systems based on Office of Management and Budget (OMB) Circular No. A-123, "Management's Responsibility for Internal Control", Appendix A, "Implementation Guide, Internal Control over Financial Reporting, Understanding the IT Infrastructure and Associated Risks."

OMB A-123 Appendix A defines Information Technology General Controls (ITGC), controls that address structure, policies, and procedures related to an entity's overall computer operations. ITGCs are not tied to any one business process, but may be related to a number of applications, associated technical infrastructure elements, and information systems management organizations that support Line of Business processes.

The Federal Information System Controls Audit Manual (FISCAM), which provides guidance on how to incorporate robust and secure financial auditing controls, is used to assess ITGCs.

In accordance with OMB A-123 Appendix A, the following five domains are required in the assessment ITGCs:

- Security Management (SM)
- Access Controls (AC)
- Configuration Management (CM)
- Contingency Planning (CP)
- Segregation of Duties (SD)

To support this requirement, the DHS CISO developed the Compliance Framework for CFO Designated Systems. The framework maps the relevant National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 revision 3 controls to the five FISCAM domains identified above and identifies the compliance activities that should be performed each year to address the domains. The CFO Designated Systems requirements are in addition to the other financial system Line of Business requirements developed by the CFO.

These additional requirements provide a strengthened assessment process and form the basis for management's assurance of internal control over financial reporting. The strengthened process requires management to document the design and to test the operating effectiveness of controls for CFO Designated Systems.

The system owner is responsible for ensuring that all requirements, including security requirements, are implemented on DHS systems. Component Chief Information Security Officers (CISOs) and Information System Security Managers (ISSMs) must coordinate with their CFO organization to ensure that requirements are met.

2.0 COMPLIANCE ACTIVITIES BY FISCAM DOMAIN

2.1 Security Management

Security Management controls provide reasonable assurance that security management is effective in the following areas:

- Security management program
- Periodic assessments and validation of risk
- Security control policies and procedures
- Security awareness training and other security-related personnel issues
- Periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices
- Remediation of information security weaknesses
- Security over activities performed by external third parties

2.1.1 SM Compliance Activities

Compliance Review
Conduct the following compliance review procedures in RTM:
•Plan of Action and Milestones (CA-5)
• Security Authorization (CA-6)
• DHS Sensitive Systems Policy Directive 4300A (PD 4300A), 3.15.e: CFO Approval
• DHS PD 4300A, 3.15.j: CFO Waivers
• DH S PD 4300A, 4.6.1.a: Wireless Assessments
• DHS PD 4300A, 4.6.1.b: Wireless vulnerabilities
• DHS PD 4300A, 4.6.1.e: Legacy Wireless
• System Security Plan (PL-2)
• Privacy Impact Assessment (PL-5)
• DHS PD 4300A, 3.14.2.a: PTA
• DHS PD 4300A, 3.14.5.a: PII 1
• DHS PD 4300A, 3.14.5.b: PII 2
• DHS PD 4300A, 3.14.5.c: PII 3
• DHS PD 4300A, 3.14.5.d: PII 4
• DHS PD 4300A, 3.15.k: CFO Designated System ISSO
• DHS PD 4300A, 3.15.l: CFO C&A
• DHS PD 4300A, 4.8.5.a: ROB
• DHS PD 4300A, 4.8.5.e: Consent to Monitor
• DHS PD 4300A, 4.8.5.f: Contractor Privileges
• Personnel Screening (PS-3)
• Personnel Termination (PS-4)

- Personnel Transfer (PS-5)
- Access Agreements (PS-6)
- Third-Party Personnel Security (PS-7)
- DHS PD 4300A, 4.1.1.a: Position Sensitivity
- DHS PD 4300A, 4.1.1.b: Personnel Security
- DHS PD 4300A, 4.1.1.c: Favorably adjudication
- DHS PD 4300A, 4.1.1.d: Access
- DHS PD 4300A, 4.1.1.e: Access
- DHS PD 4300A, 4.1.6.b: Media Transfer
- Security Categorization (RA-2)
- Risk Assessment (RA-3)
- DHS PD 4300A, 3.6.c: Custom Code Review
- DHS PD 4300A, 3.15.a: Security Assessment
- DHS PD 4300A, 3.15.c: Vulnerability Assessment
- DHS PD 4300A, 3.15.d: CFO CIA Minimum

Vulnerability Assessment

Minimum required tests for CFO Designated Systems:

- None

Additional recommended tests for CFO Designated Systems

- None

Documentation

Ensure that the following documents are complete, accurate, and current:

- DHS artifacts in TAF:
  - System Security Plan (SSP)
  - Risk Assessment (RA)
  - Privacy Threshold Analysis (PTA)
  - Privacy Impact Assessment (PIA)
  - Authority to Operate (ATO)/Interim ATO Letter
  - Compliance Test Results/RTM Artifact
  - Vulnerability Assessment Results/Scan Letter
  - Contingency Plan Test Results
  - Plans of Actions & Management (POA&Ms)
  - Valid Interconnections Security Agreement
  - Memorandums of Agreement (MOA) and Memorandums of Understanding

(MOU) (if applicable)

- Documents to be managed by ISSO:
- Completed Rules of Behavior forms
- POA&Ms

• Documents to be managed by ISSO:

- Completed Rules of Behavior forms
- POA&Ms

• Documents to be monitored by ISSO:

- List of user accounts: System generated list of users, including date created and date of last logon
- List of privileged user accounts: System generated list of system administrators, DBAs, and application developers/programmers, including date created and date of last logon
- List of transferred or separated employees and contractors, including date of separation and date of access removal (account disabled or removed)
- Contractor NDAs: Copies of completed Non-Disclosure Agreements (NDA) for all contractor personnel
- POA&Ms

2.2 Access Controls

Access Controls (AC) provide reasonable assurance that access to computer resources (data, equipment, and facilities) is reasonable and is restricted to authorized individuals. Access controls include effective:

- Protection of information system boundaries
- Identification and authentication mechanisms
- Authorization controls
- Protection of sensitive system resources
- Audit and monitoring capability, including incident handling
- Physical security controls

2.2.1 AC Compliance Activities

Compliance Review

Conduct the following compliance review procedures in RTM:

- Account Management (AC-2)
- Access Enforcement (AC-3)
- Information Flow Enforcement (AC-4)
- Least Privilege (AC-6)
- Unsuccessful Login Attempts (AC-7)
- System Use Notification (AC-8)
- Session Lock (AC-11)
- Remote Access (AC-17)
- DHS PD 4300A, 4.1.3.a: Need to Know
- DHS PD 4300A, 4.1.6.a: System Access
- DHS PD 4300A, 4.3.1.e: Media level
- DHS PD 4300A, 4.3.1.f: USB media
- DHS PD 4300A, 4.5.2.b: FAX
- DHS PD 4300A, 4.5.3.c: Teleconference
- DHS PD 4300A, 4.6.2.c: Wireless
- DHS PD 4300A, 4.6.2.l: PED Approvals
- DHS PD 4300A, 4.6.4.b: RFID
- DHS PD 4300A, 4.8.1.c: Unattended Workstations
- DHS PD 4300A, 4.8.4.b: System Access
- DHS PD 4300A, 4.8.5.c: Privacy
- DHS PD 4300A, 4.8.5.d: Consent to Monitor
- DHS PD 4300A, 4.9.a: Monitoring
- DHS PD 4300A, 5.2.a: Access Controls
- DHS PD 4300A, 5.2.b: Access Controls
- DHS PD 4300A, 5.2.d: Temp Access
- DHS PD 4300A, 5.2.e: Account Identifiers
- DHS PD 4300A, 5.2.1.a: Failed Logon Attempts
- DHS PD 4300A, 5.2.1.b: Account Lockout
- DHS PD 4300A, 5.2.1.c: Account Reset
- DHS PD 4300A, 5.2.2.a: Session Inactivity
- DHS PD 4300A, 5.2.2.b: Session Lockout
- DHS PD 4300A, 5.2.2.c: Session Inactivity II
- DHS PD 4300A, 5.4.1.a: Modem Usage
- DHS PD 4300A, 5.4.1.b: Remote Access

- DHS PD 4300A, 5.4.1.c: Remote Access of PII
- DHS PD 4300A, 5.4.1.d: Remote Access of PII 2
- DHS PD 4300A, 5.4.1.f: Remote Access PSTN
- DHS PD 4300A, 5.4.3.a: Network Security
- DHS PD 4300A, 5.4.4.a: Restrict Firewall Access
- DHS PD 4300A, 5.4.4.b: Strong Firewall I&A
- DHS PD 4300A, 5.4.4.c: Firewall Maintenance
- DHS PD 4300A, 5.4.5.f: Remote Desktop Authentication
- Auditable Events (AU-2)
- Contents of Audit Records (AU-3)
    - Audit Monitoring, Analysis, and Reporting (AU-6)
    - Protection of Audit Information (AU-9)
    - Audit Generation (AU-12)
    - DHS PD 4300A, 5.3.a Audit Trail Content
    - DHS PD 4300A, 5.3.b: Financial/PII Audit Review
    - DHS PD 4300A, 5.3.c: Audit Records and Logs Protection
    - DHS PD 4300A, 5.3.e: Risks from PII
    - DHS PD 4300A, 5.3.f: Threat-specific logging
    - Identifier Management (IA-4)
    - Authenticator Management (IA-5)
    - DHS PD 4300A, 3.14.7.a: E-Authentication
    - DHS PD 4300A, 3.14.7.b: E-Authentication
    - DHS PD 4300A, 3.14.7.c: E-Authentication
    - DHS PD 4300A, 4.3.1.d: Encryption
    - DHS PD 4300A, 4.6.b: Wireless PKI
    - DHS PD 4300A, 4.6.4.f: RFID
    - DHS PD 4300A, 5.1.c Disable USERID
    - DHS PD 4300A, 5.1.d: I & A
    - DHS PD 4300A, 5.1.1.a: Strong Passwords
    - DHS PD 4300A, 5.1.1.b: Password Aging
    - DHS PD 4300A, 5.1.1.c: Password Sharing
    - DHS PD 4300A, 5.1.1.d: Group Passwords
    - DHS PD 4300A, 5.1.1.e: Scripted Passwords
    - DHS PD 4300A, 5.1.1.f: Encrypted Passwords

- DHS PD 4300A, 5.1.1.3: Account Name Restriction
- DHS PD 4300A, 5.1.1.3: Account Validation
- DHS PD 4300A, 5.1.1.3: Guest Account
- DHS PD 4300A, 5.1.1.3: Initial Password
- DHS PD 4300A, 5.1.1.3: No Null Passwords
- DHS PD 4300A, 5.1.1.3 Password Storage
- DHS PD 4300A, 5.1.1.3 Privileged Accounts
- DHS PD 4300A, 5.2.c: Sharing Passwords
- Incident Response Training (IR-2)
- Incident Response Testing (IR-3)
- Incident Handling (IR-4)
- Incident Monitoring (IR-5)
- Incident Reporting (IR-6)
- Incident Response Assistance (IR-7)
- DHS PD 4300A, 3.14.c: Privacy Inc. Reporting
- DHS PD 4300A, 3.14.6.d: Privacy Inc. Reporting
- DHS PD 4300A, 3.15.g: CFO Incident Response
- DHS PD 4300A, 3.15.h: CFO Incident Reporting
- DHS PD 4300A, 4.9.b: SOC
- DHS PD 4300A, 4.9.1.a: Incident Response
- DHS PD 4300A, 4.9.1.b: Incident Response
- DHS PD 4300A, 4.9.1.c: HSDN Incidents
- DHS PD 4300A, 4.9.1.d: Minor Incidents
- DHS PD 4300A, 4.9.1.e: Incident Reporting
- DHS PD 4300A, 4.9.1.f: Incident Reporting
- DHS PD 4300A, 4.9.1.k: SOC/CSIRC
- DHS PD 4300A, 4.9.1.r: Incident testing
- DHS PD 4300A, 4.9.2.a: External law enforcement
- DHS PD 4300A, 4.9.2.b: LE/CI Incident Handling
- DHS PD 4300A, 5.4.4.e: Security ops
- Media Access (MP-2)
- Media Storage (MP-4)

- DHS PD 4300A, 4.3.1.a: Media
- DHS PD 4300A, 4.3.1.c: Removable Media
- Physical Access Authorizations (PE-2)
- Physical Access Control (PE-3)
- Visitor Control (PE-7)
- Delivery and Removal (PE-16)
- DHS PD 4300A, 4.2.1.c: Security Controls
- DHS PD 4300A, 4.2.1.d: Visitor Access
- DHS PD 4300A, 4.2.1.e: Physical Controls
- DHS PD 4300A, 4.2.2.a: Facility Protection
- Boundary Protection (SC-7)
- Protection of Information at Rest (SC-28)
- WITHDRAWN: Transmission Preparation Integrity (SC-33)
- DHS PD 4300A, 4.5.2.a: Fax Controls
- DHS PD 4300A, 4.5.3.b: Teleconference
- DHS PD 4300A, 5.4.3.i: Policy Enforcement Points
- DHS PD 4300A, 5.4.4.d: Quarterly Firewall Testing
- DHS PD 4300A, 5.4.4.f: Firewall Administration
- DHS PD 4300A, 5.4.4.g: Policy Enforcement Points (PEP)
- DHS PD 4300A, 5.4.4.h: Protocols and Services
- DHS PD 4300A, 5.4.5.a: Internet Connectivity
- DHS PD 4300A, 5.4.5.c: Mobile code

Vulnerability Assessment

Minimum required tests for CFO Designated Systems:

Configure testing tools to verify that:

• Firewalls, routers, and network devices within the system boundary are configured in accordance with DHS guidelines

• System is not vulnerable to buffer overflow or similar attacks

• All relevant application, database, and operating system security patches have been appropriately applied in accordance with DHS guidelines

• System default accounts are renamed or deleted if not needed

• Blank, generic, and anonymous passwords to services such as ftp, telnet, and Web servers are not being used

• Inappropriate access rights have not been granted to account profiles, roles, or groups

• Audit records are configured appropriately

• Access to audit records and tools is appropriately restricted

Additional recommended tests for CFO-Designated Systems

• Review open ports to identify any unnecessary network services

• Review scan results for indications of unauthorized and/or unlicensed software

• Ensure that intrusion detection mechanisms are appropriately configured and identified network traffic associated with the vulnerability assessment scans

Documentation

Ensure that the following documents are complete, accurate, and current:

• DHS artifacts in TAF:

- SSP
- RA
- Interconnection Security Agreements (ISA)
- Memorandums of Agreement (MOA) / Memorandums of Understanding (MOU)

• Documents to be managed by ISSO:

- Security alerts and advisories, including date received and actions taken
- Security incident/privacy incident reports: Copies of all security incident/privacy incident reports, including actions taken and date/time reported, as well as any follow-up or after action reports
- Records of audit record review: including date of each review and person(s) performing review, as well as any suspicious activity identified and actions taken
- Audit trails and activity logs
- Physical access policies and procedures (if not in SSP)

• Documents to be monitored by ISSO:

- List of user accounts: System generated list of users, including date created and date of last logon
- List of transferred or separated employees/contractors, including date of separation and date of access removal (account disabled or removed)
- User recertification results: Date of last validation of user and administrator access privileges, including person(s) performing the review and access changes
- Access authorization forms: Access request and approval forms for users, system administrators, DBAs, and application developers/programmers
- List of privileged user accounts: System generated list of system administrators, DBAs, and application developers/programmers, including date created and date of last logon

- User, system administrator, DBA, and application developer/programmer access authorization forms: Access request and approval forms for users, system administrators, DBAs, and application developers/programmers
- List of system software and utility users
- List of application programmers
- Tape and media control logs
- Incident response training records, including dates of most recent initial or refresher incident response training for each individual with significant incident response roles and responsibilities
- Access list for facility and data center: A list of all personnel granted physical access, including the date access was granted and the areas/facilities authorized for access
- Physical access request and authorization forms (Examples and for specific users)
- Emergency exit and re-entry procedures for the data center

2.3 Configuration Management

Configuration Management (CM) Controls provide reasonable assurance that changes to information system resources are authorized and systems are configured and securely and as intended, including effective

- Configuration management policies, plans, and procedure
- Proper authorization, testing, approval, and tracking of all configuration changes
- Routine monitoring of the configuration
- Updating software on a timely basis to protect against known vulnerabilities
- Documentation and approval of emergency changes to the configuration

2.3.1 CM Compliance Activities

Compliance Review
Conduct the following compliance review procedures in RTM: • Configuration Change Control (CM-3) • Monitoring Configuration Changes (CM-4) • Access Restrictions for Change (CM-5) • DHS PD 4300A, 4.4.1.a: PBX • DHS PD 4300A, 4.5.1.a: Telecomm Protection • DHS PD 4300A, 4.6.3.a: Wireless Security • DHS PD 4300A, 4.8.1.a: Workstations • DHS PD 4300A, 4.8.4.c: CM • DHS PD 4300A, 4.8.4.d Risk Mgmt • DHS PD 4300A, 4.1.b: Documentation • DHS PD 4300A, 5.4.3.l: CCB • DHS PD 4300A, 5.4.5.b: Firewalls and PEPs • DHS PD 4300A, 5.4.5.d Telnet • DHS PD 4300A, 5.4.5.e: FTP • Information System Documentation (SA-5) • User Installed Software (SA-7) • DHS PD 4300A, 3.6.b Life-Cycle Documentation • DHS PD 4300A, 4.8.03.b: Personal Equipment • Flaw Remediation (SI-2) • Security Alerts and Advisories and Directives (SI-5) • DHS PD 4300A, 3.7.c: CM • DHS PD 4300A, 5.4.2.a: Network Continuous Monitoring • DHS PD 4300A, 5.4.8.d: Compliance
Vulnerability Assessment
Minimum required tests for CFO Designated Systems: • Ensure software in use is currently supported by vendor Configure testing tools to verify that: • All appropriate application, database, and operating system patches and updates are installed Based on the results of the vulnerability assessment scans, ensure that: • Change request and approval forms are on file for any changes made to system hardware and software (e.g., software version upgrades) since the system was granted ATO • Necessary waivers and/or exceptions are maintained on file for any deviations from DHS Configuration

Guidelines identified during the vulnerability assessment scan Additional recommended tests for CFO Designated Systems: • None
Documentation
Ensure that the following documents are complete, accurate, and current: • DHS artifacts in TAF: ◦ SSP ◦ Change Management Plan • Documents to be managed by ISSO: ◦ Configuration Baseline (after hardening) ◦ Listing of all vendor supplied software ◦ System software documentation • Documents to be monitored by ISSO: ◦ System/program change requests and approvals ◦ Security alerts and advisories, including date received and actions taken ◦ System/program change requests and approvals

2.4 Contingency Planning

Contingency Planning (CP) controls provide reasonable assurance that contingency planning (1) protects information resources and minimizes the risk of unplanned interruptions and (2) provides for recovery of critical operations should interruptions occur, including effective:

- Assessment of the criticality and sensitivity of computerized operations and identification of supporting resources,
- Steps taken to prevent and minimize potential damage and interruption,
- Comprehensive contingency plan, and
- Periodic contingency plan testing, with appropriate adjustments to the plan based on testing results

2.4.1 CP Compliance Activities

Compliance Review
Conduct the following compliance review procedures in RTM: • Contingency Plan Testing (CP-4) • Alternate Processing Sites (CP-7) • Telecommunications Services (CP-8) • DHS PD 4300A, 3.15.f Contingency Planning • DHS PD 4300A, 4.11.c Backup Procedures • Security Categorization (RA-2) • DHS PD 4300A, 3.15.d CFO CIA Minimum • Information System Documentation (SA-5)
Vulnerability Assessment
Minimum required tests for CFO Designated Systems: • None Additional recommended tests for CFO-Designated Systems • None
Documentation
Ensure that the following documents are complete, accurate, and current: • DHS artifacts in TAF: ◦ Contingency Plan ◦ Annual Contingency Plan Test Results ◦ Annual Disaster Recovery Exercise Results (for high availability systems) • Documents to be managed by ISSO: ◦ Backup and restoration test results • Documents to be monitored by ISSO: ◦ None

2.5 Segregation of Duties

Segregation of Duties (SD) controls provide reasonable assurance that incompatible duties are effectively segregated, including effective

- Segregation of incompatible duties and responsibilities and related policies, and
- Control of personnel activities through formal operating procedures, supervision, and review.

2.5.1 SD Compliance Activities

Compliance Review
Conduct the following compliance review procedures in RTM: • Separation of duties (AC-5) • DHS PD 4300A, 4.1.4.a Separation of Duties • Access Agreements (PS-6)
Vulnerability Assessment
Minimum required tests for CFO Designated Systems: Configure testing tools to verify that: • Inappropriate access rights have not been granted to account groups, roles, or profiles Additional recommended tests for CFO-Designated Systems • None
Documentation
Ensure that the following documents are complete, accurate, and current: • DHS artifacts in TAF: ◦ SSP • Documents to be managed by ISSO: ◦ None • Documents to be monitored by ISSO: ◦ List of users and their positions ◦ Copies of all position descriptions