U.S. Customs and Border Protection

Attachment R

DHS Compliance Framework for CFO Designated Financial Systems

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

Version 2.0

July 27, 2009

epic.org EPIC-18-07-31-CBP-FOIA-20190618-2ndInterim-Production-pt3 000803

DOCUMENT CHANGE HISTORY

Version Number	Date	Description
1.0	July 27, 2009	Initial CBP 1400-05D release based solely on DHS 4300A, Version 6.1.1, attachment. There are no substantive differences between this CBP attachment and its source DHS attachment. This attachment is included as part of the CBP 1400-05D handbook suite to enable the CBP user to be able to access all IT security policies (DHS as well as CBP specific) at one location.
2.0	December 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.

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. The DHS *Sensitive Systems Policy Directive 4300A*, Section 3.15, provides additional requirements for these systems based on Office of Management and Budget (OMB) Circular No. A-123, *Management's Responsibility for Internal Control (A-123),* Appendix A.

In accordance with OMB A-123, Appendix A, the following five domains are required in the assessment of information technology general controls (ITGCs):

1. Security Management;
2. Access Controls;
3. Configuration Management;
4. Contingency Planning; and
5. Segregation of Duties.

In order to support this requirement, the DHS CIO mapped the relevant National Institute of Standards and Technology Special Publication 800-53 controls to the five domains identified above and identified the compliance activities that should be performed each year to address the domains. This attachment documents the CIO's compliance framework for CFO Designated Systems. The CFO Designated Systems requirements are in addition to the other CFO developed financial system Line of Business requirements.

These additional requirements provide a strengthened assessment process and form the basis for management's assurance on the internal control over financial reporting. The strengthened process requires management to document the design and 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)/Information System Security Managers (ISSMs) must coordinate with their CFO organization to ensure that these requirements are implemented.

2.0 COMPLIANCE ACTIVITIES BY FISCAM DOMAIN

2.1 Security Management (SM)

Controls provide reasonable assurance that security management is effective, including effective

- security management program,

epic.org EPIC-18-07-31-CBP-FOIA-20190618-2ndInterim-Production-pt3 000806

- 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, and
- 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 SSH, 3.15.e CFO C&A Approval • DHS SSH, 3.15.j CFO Waivers • DHS SSH, 4.06.01.a Wireless Assessments • DHS SSH, 4.06.01.b Wireless vulnerabilities • DHS SSH, 4.06.01.e Legacy Wireless • System Security Plan (PL-2) • Privacy Impact Assessment (PL-5) • DHS SSH, 3.14.02.a PTA • DHS SSH, 3.14.05.a PII 1 • DHS SSH, 3.14.05.b PII 2 • DHS SSH, 3.14.05.c PII 3 • DHS SSH, 3.14.05.d PII 4 • DHS SSH, 3.15.k CFO Designated System ISSO • DHS SSH, 3.15.l CFO C&A • DHS SSH, 4.08.05.a ROB • DHS SSH, 4.08.05.e Consent to Monitor • DHS SSH, 4.08.05.f Contractor Privileges • Personnel Screening (PS-3)

epic.org EPIC-18-07-31-CBP-FOIA-20190618-2ndInterim-Production-pt3 000807

- Personnel Termination (PS-4)
- Personnel Transfer (PS-5)
- Access Agreements (PS-6)
- Third-Party Personnel Security (PS-7)
- DHS SSH, 4.01.01.a Position Sensitivity
- DHS SSH, 4.01.01.b Personnel Security
- DHS SSH, 4.01.01.c Favorably adjudication
- DHS SSH, 4.01.01.d Access
- DHS SSH, 4.01.01.e Access
- DHS SSH, 4.01.06.b Media Transfer
- Security Categorization (RA-2)
- Risk Assessment (RA-3)
- DHS SSH, 3.06.c Custom Code Review
- DHS SSH, 3.15.a Security Assessment
- DHS SSH, 3.15.c Vulnerability Assessment
- DHS SSH, 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

epic.org EPIC-18-07-31-CBP-FOIA-20190618-2ndInterim-Production-pt3 000808

- Vulnerability Assessment Results/Scan Letter
- Contingency Plan Test Results
- Plans of Actions & Management (POA&Ms)
- Valid Interconnections Security Agreement
- Memorandums of Agreement (MOA) / Memorandums of Understanding (MOU) (if applicable)

- *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/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 (AC)

Controls provide reasonable assurance that access to computer resources (data, equipment, and facilities) is reasonable and restricted to authorized individuals, including effective

- protection of information system boundaries,
- identification and authentication mechanisms,
- authorization controls,
- protection of sensitive system resources,
- audit and monitoring capability, including incident handling, and
- physical security controls.

2.2.1 AC Compliance Activities

epic.org EPIC-18-07-31-CBP-FOIA-20190618-2ndInterim-Production-pt3 000809

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 SSH, 4.01.03.a Need to Know • DHS SSH, 4.01.06.a System Access • DHS SSH, 4.03.01.e Media level • DHS SSH, 4.03.01.f USB media • DHS SSH, 4.05.02.b FAX • DHS SSH, 4.05.03.c Teleconference • DHS SSH, 4.06.02.c Wireless • DHS SSH, 4.06.02.l PED Approvals • DHS SSH, 4.06.04.b RFID • DHS SSH, 4.08.01.c Unattended Workstations • DHS SSH, 4.08.04.b System Access • DHS SSH, 4.08.05.c Privacy • DHS SSH, 4.08.05.d Consent to Monitor • DHS SSH, 4.09.a Monitoring • DHS SSH, 5.02.a Access Controls • DHS SSH, 5.02.b Access Controls • DHS SSH, 5.02.d Temp Access • DHS SSH, 5.02.e Account Identifiers • DHS SSH, 5.02.01.a Failed Logon Attempts • DHS SSH, 5.02.01.b Account Lockout

epic.org EPIC-18-07-31-CBP-FOIA-20190618-2ndInterim-Production-pt3 000810

- DHS SSH, 5.02.01.c Account Reset
- DHS SSH, 5.02.02.a Session Inactivity
- DHS SSH, 5.02.02.b Session Lockout
- DHS SSH, 5.02.02.c Session Inactivity II
- DHS SSH, 5.04.01.a Modem Usage
- DHS SSH, 5.04.01.b Remote Access
- DHS SSH, 5.04.01.c Remote Access of PII
- DHS SSH, 5.04.01.d Remote Access of PII 2
- DHS SSH, 5.04.01.f Remote Access PSTN
- DHS SSH, 5.04.03.a Network Security
- DHS SSH, 5.04.04.a Restrict Firewall Access
- DHS SSH, 5.04.04.b Strong Firewall I&A
- DHS SSH, 5.04.04.c Firewall Maintenance
- DHS SSH, 5.04.05.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 SSH, 5.3.a Audit Trail Content
- DHS SSH, 5.3.b Financial/PII Audit Review
- DHS SSH, 5.3.c Audit Records and Logs Protection
- DHS SSH, 5.3.e Risks from PII
- DHS SSH, 5.3.f Threat-specific logging
- Identifier Management (IA-4)
- Authenticator Management (IA-5)
- DHS SSH, 3.14.07.a E-Auth
- DHS SSH, 3.14.07.b E-Auth
- DHS SSH, 3.14.07.c E-Auth
- DHS SSH, 4.03.01.d Encryption

epic.org EPIC-18-07-31-CBP-FOIA-20190618-2ndInterim-Production-pt3 000811

- DHS SSH, 4.06.b Wireless PKI
- DHS SSH, 4.06.04.f RFID
- DHS SSH, 5.1.c Disable USERID
- DHS SSH, 5.1.d I & A
- DHS SSH, 5.01.01.a Strong Passwords
- DHS SSH, 5.01.01.b Password Aging
- DHS SSH, 5.01.01.c Password Sharing
- DHS SSH, 5.01.01.d Group Passwords
- DHS SSH, 5.01.01.e Scripted Passwords
- DHS SSH, 5.01.01.f Encrypted Passwords
- DHS SSH, 5.01.01.03 Account Name Restriction
- DHS SSH, 5.01.01.03 Account Validation
- DHS SSH, 5.01.01.03 Guest Account
- DHS SSH, 5.01.01.03 Initial Password
- DHS SSH, 5.01.01.03 No Null Passwords
- DHS SSH, 5.01.01.03 Password Storage
- DHS SSH, 5.01.01.03 Privileged Accounts
- DHS SSH, 5.02.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 SSH, 3.14.06.c Privacy Inc. Reporting
- DHS SSH, 3.14.06.d Privacy Inc. Reporting
- DHS SSH, 3.15.g CFO Incident Response
- DHS SSH, 3.15.h CFO Incident Reporting
- DHS SSH, 4.09.b SOC
- DHS SSH, 4.09.01.a Incident Response

epic.org EPIC-18-07-31-CBP-FOIA-20190618-2ndInterim-Production-pt3 000812

- DHS SSH, 4.09.01.b Incident Response
- DHS SSH, 4.09.01.c HSDN Incidents
- DHS SSH, 4.09.01.d Minor Incidents
- DHS SSH, 4.09.01.e Incident Reporting
- DHS SSH, 4.09.01.f Incident Reporting
- DHS SSH, 4.09.01.k SOC/CSIRC
- DHS SSH, 4.09.01.r Incident testing
- DHS SSH, 4.09.02.a External law enforcement
- DHS SSH, 4.09.02.b LE/CI Incident Handling
- DHS SSH, 5.04.04.e Security ops
- Media Access (MP-2)
- Media Storage (MP-4)
- DHS SSH, 4.03.01.a Media
- DHS SSH, 4.03.01.c Removable Media
- Physical Access Authorizations (PE-2)
- Physical Access Control (PE-3)
- Visitor Control (PE-7)
- Delivery and Removal (PE-16)
- DHS SSH, 4.02.01.c Security Controls
- DHS SSH, 4.02.01.d Visitor Access
- DHS SSH, 4.02.01.e Physical Controls
- DHS SSH, 4.02.02.a Facility Protection
- Boundary Protection (SC-7)
- Protection of Information at Rest (SC-28)
- *WITHDRAWN: Transmission Preparation Integrity (SC-33)*
- DHS SSH, 4.05.02.a Fax Controls
- DHS SSH, 4.05.03.b Teleconference
- DHS SSH, 5.04.03.i Policy Enforcement Points
- DHS SSH, 5.04.04.d Quarterly Firewall Testing
- DHS SSH, 5.04.04.f Firewall Administration

epic.org EPIC-18-07-31-CBP-FOIA-20190618-2ndInterim-Production-pt3 000813

- DHS SSH, 5.04.04.g Policy Enforcement Points (PEP)
- DHS SSH, 5.04.04.h Protocols and Services
- DHS SSH, 5.04.05.a Internet Connectivity
- DHS SSH, 5.04.05.c Mobile code

Vulnerability Assessment

Minimum required tests for CFO Designated Systems:
Configure testing tools to verify that:

- Firewalls, routers, or 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, webservers, etc are not in use
- 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 mechanism 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

epic.org EPIC-18-07-31-CBP-FOIA-20190618-2ndInterim-Production-pt3 000814

(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/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 to facility/data center: List of all personnel granted physical access, including the date access was granted and the areas/facilities authorized for access
  - Physical access request/authorization forms (Examples and for specific

epic.org EPIC-18-07-31-CBP-FOIA-20190618-2ndInterim-Production-pt3 000815

users)

- Emergency exit and re-entry procedures for the data center

2.3 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 procedures,
- 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, and
- 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 SSH, 4.04.01.a PBX • DHS SSH, 4.05.01.a Telecomm Protection • DHS SSH, 4.06.03.a Wireless Security • DHS SSH, 4.08.01.a Workstations • DHS SSH, 4.08.04.c CM • DHS SSH, 4.08.04.d Risk Mgmt • DHS SSH, 4.10.b Documentation • DHS SSH, 5.04.03.l CCB • DHS SSH, 5.04.05.b Firewalls and PEPs • DHS SSH, 5.04.05.d Telnet • DHS SSH, 5.04.05.e FTP • Information System Documentation (SA-5) • User Installed Software (SA-7)

epic.org EPIC-18-07-31-CBP-FOIA-20190618-2ndInterim-Production-pt3 000816

- DHS SSH, 3.06.b Life-Cycle Documentation
- DHS SSH, 4.08.03.b Personal Equipment
- Flaw Remediation (SI-2)
- Security Alerts and Advisories and Directives (SI-5)
- DHS SSH, 3.07.c CM
- DHS SSH, 5.04.02.a Network Continuous Monitoring
- DHS SSH, 5.04.08.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:*

epic.org EPIC-18-07-31-CBP-FOIA-20190618-2ndInterim-Production-pt3 000817

- 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 (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 testing of the contingency plan, with appropriate adjustments to the plan based on the testing.

epic.org EPIC-18-07-31-CBP-FOIA-20190618-2ndInterim-Production-pt3 000818

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 SSH, 3.15.f Contingency Planning • DHS SSH, 4.11.c Backup Procedures • Security Categorization (RA-2) • DHS SSH, 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:*
  o Contingency Plan
  o Annual Contingency Plan Test Results
  o Annual Disaster Recovery Exercise Results (for high availability systems)
• *Documents to be Managed by ISSO:*
  o Backup and restoration test results
• *Documents to be Monitored by ISSO:*
  o None

epic.org EPIC-18-07-31-CBP-FOIA-20190618-2ndInterim-Production-pt3 000819

2.5 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 SSH, 4.01.04.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:* o SSP • *Documents to be Managed by ISSO:* o None • *Documents to be Monitored by ISSO:* o List of users and their positions o Copies of all position descriptions

epic.org EPIC-18-07-31-CBP-FOIA-20190618-2ndInterim-Production-pt3 000820