U.S. Customs and Border Protection

HB 1400-05D

Information Systems Security Policies and Procedures Handbook

Office of Information and Technology

Version 2.0

July 27, 2009

DOCUMENT CHANGE HISTORY

Version	Date	Description
1.0	07/27/2009	Agency IT Security Policy. Reformated to follow the DHS 4300A document structure including policy statement boxes with policy # and mapped NIST 800-53 security controls (if applicable). Also added the following DHS 4300A, Version 7.0 changes including, Section 2.0: redefining the DAA as the Authorizing Official (AO); creating Risk Executive (CBP CISO); Section 3.9 Updated CISO Council and added Social Media Section; Section 4.0 added maintenance activities; and Section 5.0 introducted Policy Enforcement Points (PEPs).
1.1	12/07/2009	Updated Section 5.4.7 to reflect revision in the CBP Rules of Behavior (ROB) Attachment G that specifically prohibits the use of webmail or other personal email accounts on CBP information systems and Section 5.4.8 prohibits providing personal or official DHS information solicited by e-mail; Updated handbook to reflect consistent definition of AO as authorizing official; miscellaneous identified minors edits; and added Attachments TOC as requested by CBP ISSO and CA community.
2.0	10/01/2010	Updated to reflect recent policy changes driven by FIMP Project and recent changes in the DHS 4300A Policy and Handbook documents (versions 7.2 and 7.2.1). Changes include the following: (a) Created a new sub-section for Servers (including special servers) Section 4.8.1 and 4.8.1.1 respectively. These two-sub-sections were generated from FIMP work. Renumbered pre-existing 4.8 sub-sections and references; (b) Created new sub-section 5.4.3.3 for Domain Membership under 5.4.3 Network Connectivity. No impact on numbering or existing references. New sub-section generated from FIMP; (c) sub-section 3.16.1 Adjustment to definition of PII and the introduction of formal definition of SPII; (d) section 1.10 - DHS requirement that CBP Privacy Officer approve and sign waivers/exception requests related to CBP privacy designated system; (e) adopt new section 1.11 from DHS on Info Sharing and Communications Strategy; (f) adopt new subsection 1.12 that explains how to make policy change recommendations; (g) new policy statement (2.2.2c/15) that requires administrative privelges to be reviewed and approved; (h) adding new policy statement (2.11.a) for CBP Privacy Officer; (g) revised desktop configuration management guideline (3.7e); (h) Many additions and additional references and

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000002

Version	Date	Description
		policy statements within the 3.16 Privacy and Data Security Section; (i) (4.1.4b-d) new policy statements regarding administrator priveleges; (j); clarity on SMS-MMS prohibition; (k) requires maintenance personnel to be 'cleared' and not just 'trusted'; (l) (5.4.3) clarifies definition of network connectivity; (m) added clairification on interconnections between DHS components and ISA requirements (5.4.3f/m/n); (l) (5.4.7.jj) common naming conventions required for DHS email systems; (m) (5.7.3.f) clearly prohibts sharing of private keys; (n) (1.10.3k) waiver/exception approval and reporting requirements; (o) (2.2.2) AO must be fed and senior manager; (p) (2.7) CO must be a fed and senior manager; (q) (3.2) added language to Capital Planning and Investment Control; (r) (3.5.2.h) CP testing coordinating with DHS components for Mod/High systems; (s) (2.3.3 and 3.17) Financial System Owners ensure key controls assessed annually; (t) (3.19) Possible new section related to HIPPA; (u) (4.1.1) contractor positions assessed for sensitivity rating annually; (v) (5.2) limit to 1 concurrent session for High systems; (w) (5.4.2) limits to network monitoring; (x) (5.7.3) DHS PKI MA responsible for Human Subscriber Forms; (y) (2.5.1) creating new sub-section for CBP ISSMs; (z) Figure 2.0

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000003

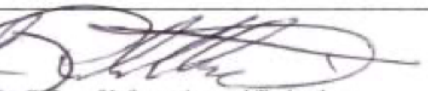
FOREWORD

This version of the U.S. Customs and Border Protection (CBP) Information Systems Security Policies and Procedures Handbook (HB 1400-05D) is formatted to be consistent with the Department of Homeland Security 4300A Sensitive System Handbook (DHS 4300A) The objective is to provide the CBP community with DHS and CBP information security policies in one location. This is intended to enhance CBP user awareness and compliance with DHS and CBP information security policies. The HB 1400-05D formatting also enhances CBP's ability to document and implement future DHS 4300A information security policy changes.

HB 1400-05D, July 27, 2009, supersedes the CBP Information Systems Security Policies and Procedures Handbook, HB 1400-05C, October 18, 2006. The revised policies in HB 1400-05D apply to Sensitive-But-Unclassified (SBU) systems. CBP policy for National Security Systems is contained in CBP National Security Systems Handbook, February 7, 2005, which is a companion document to HB 1400-05D. The intended audience for both documents includes all authorized users of CBP information systems. The policy contained in HB 1400-05D aligns with DHS Sensitive Systems Policy Directive 4300A, October 31, 2008, which implements DHS Management Directive 4300. CBP information security policy supports the business mission of the organization as well as federal mandates to protect critical national infrastructure.

Security of information and information systems has taken on new urgency in the globally computer-enabled world of the 21st century. We must exercise vigilance to protect our information resources. Owners, operators, developers, and users of information systems each have a personal responsibility to protect these resources. Managers and supervisors are personally responsible for understanding the sensitivity and criticality of their data as well as the damage that could occur to unprotected resources. It is their responsibility to provide appropriate security controls for the resources entrusted to them. CBP certification and accreditation authorities have the weighty responsibility to ensure that all systems presented for certification and accreditation have adequately addressed threats and vulnerabilities to minimize security risks of operating in the production environment.

The ***value*** of this information security policy is in its ***execution*** by all CBP system owners, operators, administrators, developers, interconnecting trade partners, government agencies, and system users. The ***goal*** of executed information security policies is to reduce the risks posed to CBP information and information systems by unauthorized access or disclosure. The ***result*** of well-executed information security policies is consistent application of security countermeasures enterprise-wide that provide defense-in-depth for all CBP systems and data.

7-27-09	
Date	Deputy Assistant Commissioner, Office of Information and Technology

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000004

CONTENTS

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000005

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000007

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000008

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000009

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000010

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000011

TABLE OF CONTENTS - FIGURES

TABLE OF CONTENTS - TABLES

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000012

TABLE OF CONTENTS - ATTACHMENTS

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000013

1.0 INTRODUCTION

Customs and Border Protection (CBP) must incorporate security safeguards within its information systems to support the Department of Homeland Security (DHS) mission. This handbook serves as an aid to CBP IT users to achieve confidentiality, integrity, availability, and non-repudiation within CBP Information Technology (IT) infrastructure and operations.

The purpose of this document is to provide specific techniques and procedures for implementing the requirements of the CBP Information Security Program for Sensitive Systems. These baseline security requirements (BLSRs) are generated by the DHS IT security policies published in DHS Sensitive Systems Policy Directive 4300A. The BLSRs included in 4300A (see Attachment A, Requirements Traceability Matrix) must be addressed in the IT security documents prepared by CBP.

This handbook incorporates DHS 4300A information security policies and procedures. In addition, it implements as requirements many of the guidelines contained in various National Institute of Standards and Technology (NIST) publications, Office of Management and Budget (OMB) direction and Congressional as well as Executive Branch mandates. Due to its business mission, CBP systems may require policies and procedures that are more stringent than those required by federal or DHS security policy.

The intended audience includes all elements of CBP using information systems and networks within CBP. Specific procedures supporting these policies may be found in the attachments. The scope and contents of this handbook will change over time as new capabilities are added to CBP systems, as security standards are upgraded, and as a result of user experience and comment.

This handbook is issued as implementation guidance under the authority of the Chief Information Officer (CIO) through the Office of the Chief Information Security Officer (CISO). This handbook addresses IT security only. However, those aspects of personnel, physical, information and industrial security; investigations; emergency preparedness; and counterterrorism that relate to IT security are addressed in this handbook.

1.1 Security Objectives

Confidentiality, availability, integrity, and non-repudiation are the CBP primary security objectives. These provide a framework to develop security policies and procedures for CBP. Risk management is another key objective, which is addressed in more detail in Section 3.8. The weighing of risks associated with each primary security objective may not be equal, nor will it be assessed in the same way for classified and Sensitive-But-Unclassified (SBU) information and information systems at CBP. Federal Information Processing Publication (FIPS) -199, Standards for Security Categorization of Federal Information and Information Systems, offers guidance to categorize information systems based on the priority of each of the security objectives. CBP follows this guidance in categorizing its SBU information and information systems.

1.2 IT Security Program Policy and Implementation Guidelines

This handbook provides procedures and techniques necessary to implement the BLSRs relating to management, operational, and technical controls that provide the foundation necessary to

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000014

ensure confidentiality, integrity, availability, authenticity, and non-repudiation within the CBP IT infrastructure and operations.

This handbook addresses the procedures necessary for implementing security requirements for sensitive IT systems. A CBP system is any information system that transmits, stores, or processes data or information and is (1) owned, leased, or operated by CBP, (2) operated by a contractor on behalf of CBP, or (3) operated by another Federal, state, or local Government agency on behalf of CBP. CBP policy mandates that all CBP computing resources be individually accounted for as part of an IT system. IT systems encompass major applications and general support systems.

The CBP Information Security Program does not apply to any IT that processes, stores, or transmits foreign intelligence information pursuant to Executive Order (E.O.) 12333, to Director of Central Intelligence directives governing the protection of intelligence information, and to other applicable orders.

Policy elements are effective when issued. Any policy elements that have not been implemented within 90 days shall be considered a weakness. Either a system or program Plan of Action and Milestones (POA&M) must be generated for the identified weaknesses. After 90 days, any new policy elements that have not been implemented shall be considered a weakness. When DHS Security Compliance tools [Risk Management System (RMS) and TrustedAgent FISMA (TAF)] are required to be updated to reflect policy element changes, tool changes shall be available to CBP within 45 days of the policy changes.

1.3 Applicability

This handbook applies to all CBP personnel, contractors acting for CBP, and all authorized users who access CBP information systems. The CBP Information Systems Security Policies and Procedures Handbook applies to all CBP information systems used to process, store, transmit, or receive any CBP data.

CBP Mission Statement

Information security principles and practices in this document support the basic CBP mission stated below:

We are the guardians of our Nation's borders. We are America's frontline.

We safeguard the American homeland at and beyond our borders.

We protect the American public against terrorists and the instruments of terror.

We steadfastly enforce the laws of the United States while fostering our Nation's economic security through lawful international trade and travel.

We serve the American public with vigilance, integrity, and professionalism.

1.4 Authorities

DHS established a department-wide Information Technology (IT) security program presented in DHS 4300A Sensitive Systems Handbook and DHS 4300B National Security Systems

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000015

Handbook for classified systems. This policy and authority extends to CBP, a component of DHS.

Applicable Executive orders, public laws, and national policy for this handbook include the following:

- 5 Code of Federal Regulations (CFR) §2635, Office of Government Ethics, Standards of Ethical Conduct for Employees of the Executive Branch
- Department of Homeland Security Acquisition Regulation (HSAR), June 2006
- Department of State 12 Foreign Affairs Manual (FAM) 600, *Information Security Technology*, June 22, 2000
- DHS Management Directives (e.g., MD 0470.1, MD 140-01, MD 1030, MD 4400.1, MD 4500.1, MD 4600.1, MD 11042.1, MD 11050.2)
- Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, dated April 3, 1984
- Executive Order 12656, *Assignment of Emergency Preparedness Responsibilities*, dated November 18, 1988, as amended
- Federal Financial Management Improvement Act of 1996 (FFMIA), P.L. 104-208
- Federal Managers' Financial Integrity Act of 1982 (FMFIA), P.L. 97-255
- Homeland Security Presidential Directive 12, *Policy for a Common Identification Standard for Federal Employees and Contractors,* August 27, 2004
- National Institute of Standards and Technology (NIST) Special Publications (e.g., 800-16, 800-34, 800-37, 800-50, 800-53 Revision 1) and Federal Information Processing Standards (FIPS) (e.g., FIPS 199, 200)
- NIST Federal Information Processing Standards (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems*
- Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*
- OMB Bulletin 06-03, Audit Requirements for Federal Financial Statements August 23, 2006
- OMB Circular A123, Management's Responsibility for Internal Control, Revised, December 21, 2004
- OMB Circular A-127, *Financial Management Systems*, Revised December 1, 2004
- Privacy Act of 1974, As Amended. 5 United States Code (U.S.C.) 552a, Public Law 93-579, Washington, D.C., July 14, 1987
- Public Law 104-106, Clinger-Cohen Act of 1996 [formerly, Information Technology Management Reform Act (ITMRA)], February 10, 1996
- Public Law 107-296, Homeland Security Act of 2002
- Public Law 107-347, E-Government Act of 2002, including Title III, Federal Information Security Management Act (FISMA)

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000016

- The National Security Act of 1947, dated July 26, 1947

1.5 Document References

Applicable documents used in the preparation of this handbook are listed below

Public Law

Public Law 100-235, Computer Security Act of 1987, January 8, 1988

Public Law 101-576, Chief Financial Officers (CFO) Act of 1990

Public Law 104-106, Information Technology Management Reform Act of 1996, Section 5131

Public Law 106-398, National Defense Authorization Act of 2001

Public Law 107-347, E-Government Act of 2002 (includes FISMA, Title III)

Public Law 107-347, Federal Information Security Management Act of 2002, Title III – Information Security

Executive Orders

Executive Order 13200, President's Information Technology Advisory Committee, Further Amendment to Executive Order 13035, as Amended, Signed: February 11, 2001

Executive Order 13215, President's Information Technology Advisory Committee, Further Amendment to Executive Order 13035, as Amended, Signed: May 31, 2001

Executive Order 13228, Establishing the Office of Homeland Security and the Homeland Security Council, Signed: October 8, 2001

Executive Order 13231, Critical Infrastructure Protection in the Information Age, October 16, 2001

Homeland Security Presidential Directive 7, Critical Infrastructure Identification, Prioritization, and Protection, December 17, 2003

Federal Guidance

OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources

OMB Memorandum M-06-16, Protection of Sensitive Agency Information, June 23, 2006

OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, September 26, 2003

OMB Memorandum M-04-04, E-Authentication Guidance for Federal Agencies, December 16, 2003

OMB Memorandum M-07-16 Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007

9/11 Act of 2007, Increased Mission Requirements for Chief Privacy Officer

OMB Circular A-123, Management's Responsibility for Internal Control, Revised, December 21, 2004

OMB Circular A-127, Financial Management Systems, Revised December 1, 2004

OMB Bulletin 06-03, Audit Requirements for Federal Financial Statements, August 23, 2006

OMB Bulletin 01-02, Audit Requirements for Federal Financial Statements, October 19, 2000

FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004

FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, May 2006

FIPS 140-1 (January 1994) and FIPS 140-2 (May 2001), Security Requirements for Cryptographic Modules

NIST SP-800-18, Guide for Developing Security Plans for Information Technology Systems, Revision 1, February 2006

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000017

NIST SP-800-21, Guideline for Implementing Cryptography in the Federal Government, Revision 1, December 2001

NIST SP-800-30, Risk Management Guide for Information Technology Systems, July 2002

NIST SP-800-37, Rev. 1, DRAFT Guide for the Security Authorization of Federal Information Systems: A Security Life Cycle Approach, August 2008

NIST SP-800-47, Security Guide for Interconnecting Information Technology Systems, August 2002

NIST SP-800-48, Wireless Network Security for IEEE802.11 a/b/g and Bluetooth, August 2, 2007

NIST SP-800-53, Recommended Security Controls for Federal Information Systems, Revision 1, December 2006

NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems, 6/2008

NIST SP-800-55, Security Metrics Guide for Information Technology Systems, July 2003

NIST SP-800-55, Performance Measurement Guide for Information Security, Revision 1, July 2008

NIST SP-800-65, Integrating IT Security into the Capital Planning and Investment Control Process, January 2005

NIST SP-800-63, Electronic Authentication Guidelines, Draft, February 20, 2008

NIST SP-800-61, Computer Security Incident Handling Guide, March 2008

NIST SP-800-98, Guidelines for Securing Radio Frequency Identification (RFID) Systems, April 2007

CNSS Instruction No. 4009, National Information Assurance Glossary, Revised June 2006

CNSS Instruction No. 1001, National Instruction on Classified Information Spillage, February 2008

Code of Federal Regulations (CFR) §2635, Office of Government Ethics, Standards of Ethical Conduct for Employees of the Executive Branch

Departmental/Agency Policy

DHS, Sensitive Systems Handbook 4300A, Version 6.1.1, October 31, 2008

DHS, IT Security Procedural Guide, Developing a Contingency Plan (Appendix 1 of DHS Security Program Handbook)

CBP, System Life Cycle Handbook, CIS HB 5500-07B, Version 1.2, October 16, 2008

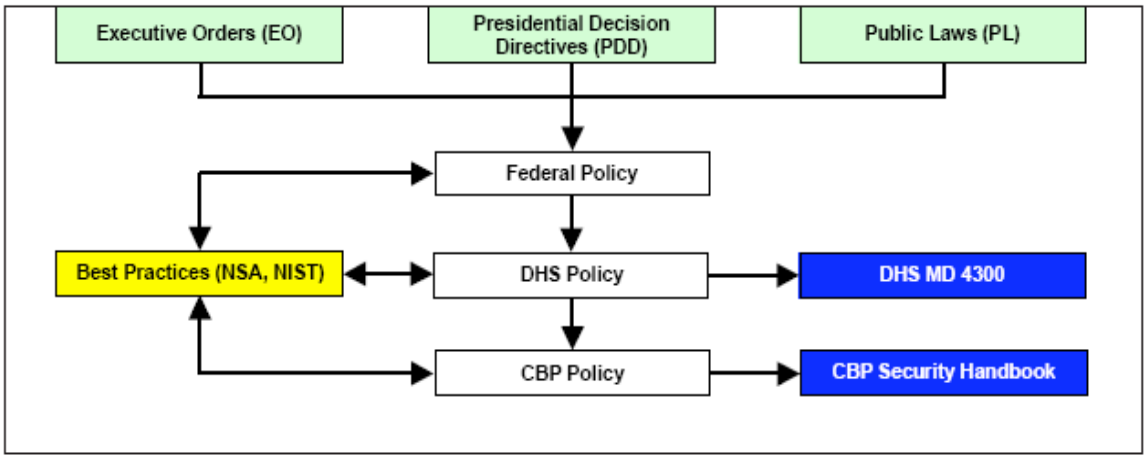
Department of Defense Directive 8100.2, April 14, 2004, Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)

1.6 Information Systems Security Policy Hierarchy

Federal security policy flows from the executive level and Public Law to Department and Bureau levels. Development of policy at the national level generally begins with the creation of an Executive Order (EO), a Presidential Decision Directive (PDD), or a Public Law (PL). Other organizations such as the National Security Agency (NSA), the National Institute of Standards and Technology (NIST), and the Office of Management and Budget (OMB) also provide guidance and directives for policy development. Federal agencies use these orders, directives, laws, and guidance to generate policies and practices applicable to their organizations. Figure 1.6, Security Policy Development depicts the flow of points of policy origination for CBP.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000018

Figure 1.6: Security Policy Development



1.7 Policy Overview

Security of federal information systems is mandated by law. (See Section 1.5) Information security policy regulates how an organization protects and assigns resources to achieve its security objectives. Security safeguards and countermeasures are selected as a result of risk assessment activities. The overall CBP information technology security program encompasses the architectural framework that contains applications, networks, hardware, software, services, processes, policies, documentation, and resources that assist in accomplishment of the CBP mission. Funding of CBP is closely tied to the robustness of its security program, which must be reported annually to the Office of Management and Budget (OMB). Great importance is given to security certification and accreditation of applications and systems. Security status of a project is weighted heavily in Congressional funding considerations. (Refer to Section 3.2.1 Investment Management Process.) Section II.B of the OMB Exhibit 300 annual report requires detailed reporting on the security program.

The statement that security is everyone's responsibility is absolutely true. System owners, operators, developers, and users of information systems each have a responsibility to protect IT data and resources. Managers and supervisors should provide appropriate security controls for any information resources entrusted to them. Managers and supervisors must be aware of the sensitivity and criticality of their data. In order to protect this data, managers should ensure that all IT users are aware of required security practices and procedures. Users of CBP systems have the responsibility to learn and follow the policies and procedures governing the use of CBP resources.

CBP IT security policies delineate the security management structure and foundation to measure progress and compliance. Policies in this document are organized under three areas: management, operational, and technical.

- **Management Controls** – Focus on managing both the IT security system and system risk. These controls consist of risk mitigation techniques and concerns normally addressed by management.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000019

- **Operational Controls** – Focus on mechanisms primarily implemented and executed by people. These controls are designed to improve the security of a particular system, or group of systems. These controls require technical or specialized expertise and often rely on management and technical controls.
- **Technical Controls** – Focus on security controls executed by IT systems. These controls provide automated protection from unauthorized access or misuse. They facilitate detection of security violations, and support security requirements for applications and data.

1.8 General CBP Security Policy

All information technology that generates, stores, processes, transfers, or communicates sensitive information shall be protected at a level commensurate with the threat. The following security practices, therefore, are necessary.

1. New system acquisitions, system development, and modifications to existing systems must be coordinated with the Security and Technology Policy (STP) Branch.

2. It is recommended that a label be affixed to media containing Sensitive-But-Unclassified (SBU) information, especially in environments where both sensitive information and classified information are processed. Labels stating "this medium is unclassified" are available from General Services Administration (GSA) [Standard Form (SF) 710]. Unless otherwise specified, SBU data should be labeled as "For Official Use Only" and safeguarded against unauthorized disclosure, modification, access, use, or destruction. (See Section 4.3 media controls for details.)

3. All Major Applications (MAs) and General Support Systems (GSSs) must be certified and accredited to comply with required security controls.

4. Connections between CBP information systems and any other systems or networks not under CBP authority are unauthorized, unless documented by a formally approved Interconnection Security Agreement (ISA) signed by the Deputy Director, Enterprise Data Management and Engineering Division (EDME)/Office of Information and Technology (OIT). If the system or network not under CBP authority is owned by another DHS component, an ISA is still required. The non-CBP system representatives must have the authority to represent their organization, when defining security requirements to be included in the ISA. (See Attachment N)

5. The non-CBP signatory representative(s) must have the authority to accept the system risk incurred by the connection to CBP. One non-CBP signatory authority would belong to the organization owning the information system at the point of connection to CBP. The organization that owns the data to be transferred through the interconnection may also be a stakeholder in the interconnection. Therefore, an individual from one or more organizations participating in the interconnection (e.g., the system owner and the data owner) may be the signatory authorities representing the non-CBP side of the connection. Because non-CBP organizations are participants in the ISA and are required to sign the agreement, CBP may have to be somewhat flexible in adhering to

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000020

the ISA Template. The Information Systems Security Officer (ISSO) assigned to the system should be contacted before any modifications to the template are made.

6. CBP information systems are for authorized CBP business only. "Limited Personal Use" is authorized under the conditions specified in Section 4.8.9.

7. Appropriate physical, administrative, and technical safeguards will be implemented and maintained to ensure the most cost-effective security safeguards exist. These safeguards will be consistent with the approved CBP enterprise architecture to ensure proper integration and interoperability.

8. Installation of assistive software, hardware, or other adaptive devices is subject to standard CBP security testing and change request processes before introducing these products to the production environment. Such adaptive devices and/or software must not degrade or circumvent established system security controls.

9. The requirement to protect Privacy Information is a federal law. CBP systems of record will be afforded the level of security protection commensurate with the level of safeguards required by Federal Privacy Law. For more information on Privacy Law implementation within CBP, contact the CBP Privacy Law Advocate within the Office of Regulations and Rulings (OR&R).

10. Users have no expectation of privacy when using CBP network resources, including the use of electronic messaging, Internet, and other CBP applications and systems. Acceptance of this condition is positively validated when users log onto the network

1.8.1 Security of Non-CBP Sites

Organizations providing contracted services to CBP at other than CBP facilities must adhere to the security policies described within this document to include federal policies and regulations. Services provided by non-CBP sites are integral parts of CBP Major Applications (MAs) or General Support Systems (GSSs) and must be considered within the system boundaries of the Certification and Accreditation (C&A) of the applicable information system.

All CBP information systems must be properly accredited. The Assistant Commissioner, OIT must certify and accredit information systems that are functionally owned and managed by CBP. Any CBP information system operating without the approval of the Assistant Commissioner, OIT is not considered accredited, regardless of any other accreditation, unless there is an explicit written Memorandum of Understanding that provides different policy.

Non-CBP sites are subject to the same security review as government owned or controlled sites. The reviews are conducted in accordance with the Federal Information Security Management Act (FISMA) of 2002, which states in the relevant section:

"The head of each agency shall be responsible for providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of the agency." (H.R. 2458—51, section 3544).

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000021

The goal of the information system security review effort is to ensure that sensitive CBP information being processed at non-CBP facilities is appropriately protected commensurate with federal law, CBP policies, DHS regulations, and security best practices. The objectives of the security reviews are to assess the effectiveness of security controls in place at all facilities, identify areas of strength and weakness, assist in corrective measures, and issue resolution where necessary.

Guidance for a self-evaluation of the security controls implemented to protect CBP information systems (i.e., Major Applications [MAs] and General Support Systems [GSSs] as listed in the CBP system inventory) compliance with CBP security policy. The self-assessment used by CBP is found in the NIST SP 800-53, which provides a detailed checklist for 17 security areas. STP staff, namely the Information Systems Security Officers (ISSOs) will complete the self-assessment templates generated by the DHS Risk Management System (RMS) tool. Based on DHS requirements, artifacts produced by security reviews of government or contractor/consultant facilities will be completed for each MA or GSS system, but not necessarily for each individual site. Independent audit agencies may validate the results of the completed self-assessments of CBP information systems.

1.9 Penalties and Offenses

All users authorized to access CBP systems are responsible for reading and complying with the policies in this handbook, as well as other CBP policies that govern standards of behavior within CBP. Failure to comply with these policies subjects a violator to the published penalties. These are available on the CBPnet using the following link:

http://www.cbp.gov/xp/cgov/careers/neo_kit/additional_info/standards_of_conduct/

Supervisors and managers are responsible for determining appropriate disciplinary action and applicable penalties for violations. Although some infractions may incur progressive disciplinary actions, others may be serious enough to warrant removal.

1.10 Waivers and Exceptions

Waivers from or exceptions to CBP or DHS policy may be requested from DHS or CBP policy requirements.

All waivers and exception requests for a specific system shall include the system name and system TrustedAgent FISMA (TAF) Inventory ID.

Any waiver or exception request should be handled at the same classification level as the system, either unclassified or classified. For an unclassified waiver or exception, which includes the identification of system vulnerabilities, the request should be marked “For Official Use Only.”

Any waiver or exception request from DHS policy shall be made to the Certifying Agent (CA) through the Information Systems Security Officer (ISSO) with the concurrence of the business owner and system owner. The request is then vetted through the appropriate Security and Technology Policy (STP) Team. The formal request is submitted through the Chief Information Security Officer (CISO) to the DHS CISO.

Any waiver or exception request from CBP policy shall be submitted to the Certifying Agent (CA) through the Information Systems Security Officer (ISSO) with the concurrence of the

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000022

business owner and system owner. The request is then vetted through the appropriate STP Team. The formal request is submitted through the CISO to the AO for final approval.

1.10.1 Waivers

A request for a waiver to any portion of DHS or CBP policy may be made, for up to 6 (six) months, any time DHS or CBP policy requirements cannot be achieved. Waiver requests shall include the operational justification, risk acceptance, risk mitigation measures, and a plan for bringing the system into compliance.

If a Material Weakness is reported in an Audit Report, and the control weakness is not scheduled to be remediated within twelve months, a waiver request must be submitted as described above.

If the Material Weakness is against a financial system, the CFO must also approve the waiver request before sending it to the CISO or through the CISO to the DHS CISO.

The Commissioner shall approve any waiver request that results in a total waiver time exceeding 12 months before sending it to the DHS CISO and the waiver must be reported as a material weakness in the Federal Information Systems Management Act (FISMA) report.

All waiver requests must identify the POA&M for bringing the system procedures or control weakness into compliance. In all cases waivers should be requested for an appropriate period based on a reasonable remediation strategy.

1.10.2 Exceptions

Exceptions may be requested whenever an office is unable to bring a system control weakness into compliance or requires a permanent exception to DHS or CBP policy. Exceptions are generally limited to systems that are unable to comply due to detrimental impact to mission, excessive costs, and/or clearly documented end of platform life for non-essential systems within 18 months, commercial-off-the-shelf (COTS) products that cannot be configured to support the control requirement, etc.

This request shall include the operational justification, risk acceptance, and risk mitigation measures.

The resulting risk also must be approved and accepted by the Authorizing Official (AO) and by the CFO if the system is a financial or mixed financial system.

1.10.3 Waiver or Exception Requests

For waivers to or exceptions from DHS policy, the Waiver or Exception Request Form, located in Attachment B of the DHS 4300A Sensitive Systems Handbook shall be used. For waivers to or exceptions from CBP policy, a memorandum, which is located as an asset in the OIT PAL shall be used. A Privacy Threshold Assessment (PTA) may be required as part of this process as well.

ISSOs, audit liaisons, and others may develop the waiver or exception request, but the CA must submit the request through the CISO.

Justification for the waiver request should document mission impact by the operational system, as well as efforts to mitigate the risk based on descriptions of counter measures or compensating controls currently in place.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000023

Any waiver or exception requests for Chief Financial Officer (CFO) designated systems must additionally be submitted to and approved by the CFO.

Any waiver or exception requests for Privacy Sensitive Systems must additionally be submitted to, and approved by, the Privacy Officer in writing. Justification for the exception requests should include cost trade off justification and/or system lifecycle considerations.

All approved waiver and exception requests must be directed to the CISO, and if the waiver and exception request is from DHS policy, from the CISO to the DHS CISO.

Policy ID	CBP Policy Statements	Relevant Controls
1.10.3.a	Systems without an ATO when this policy is issued shall comply with all of its policy statements or obtain appropriate waivers and/or exceptions.	PL-1
1.10.3.b	Systems with an ATO when this policy is issued shall comply with all of its policy statements within ninety (90) days or obtain appropriate waivers and/or exceptions. (A new ATO is only required for significant changes.)	PL-1
1.10.3.c	Each waiver or exception request shall include the system name, and system TrustedAgent FISMA (TAF) Inventory ID, operational justification, and risk mitigation.	CM-3
1.10.3.d	System Owners shall request a waiver whenever they are *temporarily* unable to comply fully with any portion of this policy.	CA-4
1.10.3.e	All waiver requests shall identify the POA&M for bringing the system or program into compliance.	CA-5
1.10.3.f	CISO shall approve all waiver requests prior to submitting them to the DHS CISO.	CA-6
1.10.3.g	Requests submitted without sufficient information will be returned for clarification prior to making a decision.	CA-6
1.10.3.h	A waiver shall be issued for six (6) months or less. The DHS CISO reserves the right to issue waivers for longer than six (6) months in exceptional situations. Waivers may be renewed by following the same process as in the initial request.	CA-4
1.10.3.i	The Assistant Commissioner must approve any waiver request that results in a total waiver time exceeding twelve (12) months before sending it to the DHS CISO. The waiver must also be reported as a material weakness in the Component's FISMA report.	---
1.10.3.j	CBP shall request an exception whenever they are permanently unable to comply fully with any portion of this policy.	CA-4

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000024

Policy ID	CBP Policy Statements	Relevant Controls
1.10.3.k	All such waivers shall be reported in the Component's FISMA report.	CA-6
1.10.3.l	The DHS CFO must approve all requests for waivers and exceptions for financial systems prior to their submission to the DHS CISO.	CA-6
1.10.3.m	The DHS Chief Privacy Officer must approve all requests for waivers and exceptions for designated privacy systems prior to their submission to the DHS CISO.	CA-6

1.10.4 U.S. Citizen Exception Requests

Special procedures apply for exception to the requirement that persons accessing DHS systems be U.S. Citizens (see Section 4.1.1). Under normal conditions, only U.S. Citizens are allowed access to DHS systems and networks, however, at times there is a need to grant access to foreign nationals. Access for foreign nationals is normally a long-term commitment, and exceptions to appropriate policies are treated separately from standard exceptions and waivers. The approval chain for an exception to the United States (U.S.) Citizenship requirement flows through the CISO to the DHS CISO. Attachment J to the DHS 4300A Sensitive Systems Handbook provides an electronic form for requesting exceptions to the U.S. Citizenship requirement.

Policy ID	CBP Policy Statements	Relevant Controls
1.10.4.a	Persons of dual citizenship, where one of the citizenships includes U.S. Citizenship, shall be treated as U.S. Citizens for the purposes of this directive.	---
1.10.4.b	The System Owner shall submit each request for exception to the United States Citizenship policy to the CISO. The CISO shall obtain concurrence from the DHS CISO.	PS-3
1.10.4.c	Additional compensating controls shall be maintained for foreign nationals, based on nations lists maintained by the DHS CISO.	---

1.11 Information Sharing and Communication Strategy

The DHS Enterprise Operations Center (EOC) exchanges information with CBP and other Component SOCs and Network Operations Centers (NOCs), the Homeland Secure Data Network (HSDN) SOC, the Intelligence Community, and with external organizations in order to facilitate the security and operation of the DHS network. This exchange enhances situational awareness and provides a common operating picture to network managers. The operating picture is developed from information obtained from "raw" fault, configuration management, accounting, performance, and security data. This data is monitored, collected, analyzed, processed, and reported by the NOCs and SOCs.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000025

The DHS EOC is responsible for communicating other information such as incident reports, notifications, vulnerability alerts and operational statuses to the Component SOCs, Component CISOs/ISSMs or other identified Component points of contact.

The DHS EOC portal implements role-based user profiles that allow Components to use the website's incident database capabilities. Users assigned to Component groups shall be able to perform actions such as:

- Entering incident information into the DHS EOC incident database
- Generating preformatted incident reports
- Initiating queries of the incident database
- Viewing FISMA incident reporting numbers
- Automating portions of the Information Security Vulnerability Management (ISVM) program
- Automating portions of the vulnerability assessment program

Policy ID	CBP Policy Statements	Relevant Controls
1.11.a	For DHS purposes, electronic signatures are preferred to pen and ink or facsimile signatures in all cases, except where pen and ink signatures are required by public law, Executive Order, or other agency requirements.	
1.11.b	Components are encouraged to use electronic signatures whenever possible.	
1.11.c	Components shall accept electronic signatures whenever the signature's digital certificate is current, electronically verifiable, and issued by a medium or high assurance DHS Certification Authority or other medium or high CA under the FBWG or Common Authority.	

1.12 Changes to Policy

DHS 4300A Policy and DHS 4300A Sensitive Systems Handbook serve as the foundation for the security policies contained in this Handbook. However, there may be additional policy areas that addressed within the 1400-05D that were not addressed by DHS or are addressed more strictly than the DHS 4300A documents.

For interpretation or clarification of CBP information security policies found in this policy document, contact the CBP CISO or the CBP Security Policy Team at SecurityPolicy@cbp.dhs.gov.

Changes to this policy and to the handbook may be requested by submitting an email request to the Security Policy Team at SecurityPolicy@cbp.dhs.gov.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000026

Policy ID	DHS Policy Statements	Relevant Controls
1.12.a	The CBP CISO shall be the authority for interpretation, clarification, and modification of the CBP 1400-05D *Handbook* (inclusive of all appendices and attachments).	PL-1
1.12.b	The CBP CISO shall update the CBP 1400-05 at least annually.	PL-1

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000027

2.0 ROLES AND RESPONSIBILITIES

Designated personnel play a major role in the planning and implementation of IT security requirements. Security is an inherently governmental responsibility. Contractors and other sources may assist in the performance of security functions, but a government individual must always be designated as the responsible agent for all security requirements and functions.

All personnel who manage, design, develop, program, and operate the CBP infrastructure have responsibilities that contribute toward CBP success. All personnel must be aware of their roles and corresponding responsibilities in maintaining information security. This section describes key roles with their associated responsibilities. Additional responsibilities for each of the roles are provided in Section 3.0 (Management Controls), Section 4.0 (Operational Controls), and Section 5.0 (Technical Controls). Key roles include:

Principal Authorizing Official (PAO)

Authorizing Official (AO)

Chief Financial Officer (CFO)

Chief Information Security Officer (CISO)/Certifying Official (CO)

Certification Agent (CA)

Information Systems Security Officer (ISSO)

Supervisors and Managers

System Administrators and Network Administrators

End Users

Figure 2.0 depicts security responsibility relationships and key roles within the CBP Information Security Program.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000028

Figure 2.0: Security Management Roles and Responsibilities

2.1 Commissioner/Principal Authorizing Official

The Commissioner of CBP is the Principal Authorizing Official responsible for all CBP systems. The title of Principal Authorizing Official and the associated responsibility cannot be delegated. However, the Commissioner's operational authority for the CBP Information Security Program is delegated to the Assistant Commissioner, Office of Information and Technology (OIT). The Assistant Commissioner, OIT is the Authorizing Official (AO), described in Section 2.2.2 below. The Commissioner's responsibility includes ensuring that all information, classified or unclassified, and all CBP automated information systems and their data are protected in accordance with congressional and presidential directives.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000029

Policy ID	CBP Policy Statement	Relevant Controls
2.1	The Commissioner of CBP shall ensure that information systems and their data are sufficiently protected.	PL-1

Within the DHS security structure, the CBP Commissioner will:

1. Establish, maintain, and oversee the CBP Information Security Program including its Certification and Accreditation (C&A) program. This responsibility includes the highest level of security management oversight of the development and implementation of all new or substantially modified CBP systems.

2. Appoint the Assistant Commissioner, OIT as the Authorizing Official (AO) of CBP. Delegate the authority in writing to the AO to approve or disapprove the operation of all systems functioning within CBP.

3. Appoint Chief Information Officers (CIOs), as documented in DHS security policy.

4. Appoint in writing the Director, Security and Technology Policy (STP) Branch, Enterprise Data Management and Engineering Division (EDME) as the Chief Information Security Officer (CISO) of CBP.

5. Certify and report annually the adequacy of the CBP Information Security Program to the DHS CISO.

6. Ensure that security of CBP information systems is an integral part of the life cycle management process.

7. Ensure that performance measurement requirements are implemented into management of the CBP security program.

8. Establish a Computer Security Incident Response Center (CSIRC) with an interface to appropriate national-level CSIRC, DHS Computer Emergency Readiness Team (CERT) and US-CERT.

9. Establish a centralized program for information systems security education, training, and awareness.

10. Ensure that organizations plan, budget, allocate, and spend adequate resources in support of information systems security.

11. Ensure data for IT systems are entered into the appropriate DHS Security Management Tool to support DHS IT security oversight and FISMA reporting requirements.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000030

2.2 Assistant Commissioner, Office of Information Technology

The Assistant Commissioner, Office of Information and Technology (OIT) is the AO who is appointed in writing by the Commissioner. The Assistant Commissioner, OIT has the authority to assume formal responsibility on behalf of the Commissioner for operating all CBP systems at an acceptable level of risk. The Assistant Commissioner, OIT has authority to accredit all CBP information systems and to accept risk for the security posture of the data and systems. Within the DHS security structure, the OIT Assistant Commissioner is also the Chief Information Officer (CIO) for CBP.

2.2.1 Chief Information Officer

The CIO is responsible for CBP information systems and their security as well as for ensuring FISMA compliance within the CBP.

Policy ID	CBP Policy Statement	Relevant Controls
2.2.1.a	The Component CIO shall develop and maintain the Component Information Security Program.	PL-1

The responsibilities of the Chief Information Officer (CIO) include the following:

1. Establish and oversee the CBP Information Security Programs.
2. Ensure appointment of a CISO and ensure that the CISO has resources to assist in ensuring compliance with DHS and CBP Policy:
3. Ensure that an Authorizing Official (AO) has been appointed for all CBP IT systems and serve as the AO for all IT systems.
4. Ensure that IT security concerns are addressed by Configuration Control Boards, the Architecture Review Board, and the Investment Review Board.
5. Ensure that an accurate IT systems inventory is established and maintained.
6. Ensure that an IT security performance metrics program is developed, implemented, and funded.
7. Advise the DHS CIO of any issues regarding infrastructure protection, vulnerabilities or issues that may cause public concern or loss of credibility.
8. Ensure that incidents are reported to the SOC within required reporting times as defined in Attachment F of the this handbook.
9. Work with the DHS CIO and Public Affairs Office in preparation for public release of security incident information. The DHS CIO, or designated representative, has sole responsibility for public release of security incident information.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000031

10. Ensure compliance with CBP and DHS IT policy.

11. Ensure that all IT systems acquisition documents, including existing contracts, include appropriate information security requirements and comply with CBP information security policies.

12. Ensure that system owners understand and appropriately address risks, including interconnectivity with other programs and systems outside their control.

2.2.2 Authorizing Official

The AO formally assumes responsibility for operating an information system at an acceptable level of risk. He or she shall be a senior management official and a Federal employee or military member.

Policy ID	CBP Policy Statements	Relevant Controls
2.2.2.a	The CIO shall act as the AO for CBP enterprise information systems or shall designate one in writing.	CA-6
2.2.2.b	An AO may be responsible for more than one system.	CA-6
2.2.2.c	The AO shall review and approve any individual requiring administrator privileges. The AO may delegate this duty to the appropriate system owner or Program Manager.	AC-2

The responsibilities of the Authorizing Official (AO) include the following tasks:

1. Grant the formal accreditation or Approval-To-Operate (ATO) for a CBP information system.

2. Approve/disapprove system accreditation, or issue an Interim Authorization to Operate (IATOs may be issued only for systems in development testing or for prototypes).

3. Terminate system operation if security conditions warrant such action.

4. Ensure key control compliance is well-documented and annually tested as part of the accreditation of systems supporting: 1) FISMA, 2) Privacy Sensitive Systems, and 3) Chief Financial Officer designated Financial Systems.

5. Require security safeguards, if necessary, greater than the safeguards specified in the accreditation package submitted for approval. This determination will be based on the sensitivity or classification level of the data and the operating environment of an information system.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000032

6. Withdraw accreditation and suspend operations when necessary. Grant waivers and exceptions to CBP policy when circumstances warrant and waivers are not in violation of applicable regulations. The AO can grant waivers and exceptions to CBP policy.

7. Complete the following steps before authorizing an information system that does not include all the security requirements specified in this handbook:

    a. Provide written notification to other Assistant Commissioners owning the data and information system of any security requirements that have not been implemented, their residual risks, and mitigating safeguards. Review and approve corrective actions necessary to mitigate residual risk.

    b. Provide the Authorizing Official and/or an individual with the authority to accept the risk of a non-CBP system connected to a CBP system with a written list of any security requirements that are not implemented, their residual risks, and mitigating safeguards.

    c. State in the accreditation document that the Assistant Commissioner, OIT, understands and accepts responsibility for the residual risk, if any, of operating the system.

8. Task the CISO with the development, implementation, and maintenance of an adequate CBP-wide Information Security Program. Within this security program, include the development of procedures necessary to implement applicable security regulations, directives, and publications.

9. Task the Deputy Director, EDME, to formally review and approve all Interconnection Security Agreements (ISAs) that permit the interconnection of CBP-owned systems with any non-CBP-owned systems.

10. Ensure that operational information systems security policies are promulgated for each system for which the Assistant Commissioner, OIT has approval authority.

11. Establish, implement, and maintain an information system security education, training, and awareness program.

12. Report security discrepancies, vulnerabilities, and threats, when applicable, to the non-CBP authorizing official of interconnected systems.

13. Approve incident-reporting procedures.

14. Ensure technically qualified personnel perform security functions.

15. Ensure any individual requiring administrator privileges is reviewed and approved. The AO may delegate this duty to the appropriate system owner or Program Manager.

16. Incorporate security throughout the system life cycle (SLC) process.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000033

17. Ensure data ownership is established for each information system, to include accountability and access rights.

18. Review Notices of Findings and Recommendations (NFR) and Plans of Action and Milestones (POA&M).

19. Review and approve corrective actions necessary to mitigate residual risks.

2.3 Chief Financial Officer Designated Financial Systems

CBP maintains systems defined by the DHS Chief Financial Officer (CFO) as financial systems based on OMB Bulletin No. 06-03, Audit Requirements for Federal Financial Statements, and (b) (7)(E), Cross Servicing Assertion, and Draft OMB Bulletin 01-02. The DHS CFO identifies financial systems subject to OMB A-123 and Internal Controls over Financial Reporting (ICOFR) requirements ("CFO-designated financial systems"). These designated financial systems require additional management accountability and effective internal control over financial reporting. For CFO-designated financial systems, additional CBP specific roles and responsibilities are summarized in this section.

For CFO-designated financial systems, additional roles and responsibilities are summarized in this section. *(NOTE: The DHS CFO-designated financial systems require additional management accountability and effective internal control over financial reporting, as outlined in Section 3.18)*

2.3.1 Chief Financial Officer

The Assistant Commissioner of the Office of Finance is the Chief Financial Officer (CFO) within CBP. The CFO is mandated with the authority to serve as the Authorizing Official for all CBP systems that were designated financial systems by the DHS CFO. The Assistant Commissioner's CFO operational authority for the designated financial systems may be delegated in writing to the Deputy AC of the Office of Finance. The CFO, working with the respective system owners, is responsible for overseeing implementation and compliance of IT controls for DHS CFO-designated financial systems. The CFO:

1. Works with the CIO and owners of all designated financial systems to help ensure the reliability of financial data processing through the systems.

2. Develops and establishes policies and procedures regarding automated application controls for software processing of financial data.

3. Remediates automated application controls deficiencies.

4. Works with system owners to designate an Information System Security Officer (ISSO) for each of the designated financial systems as defined in Section 2.8.1.

5. Tracks and monitors progress of automated application controls remediation efforts.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000034

6. Works with system owners of designated financial systems to ensure remediation of IT general controls (ITGC) deficiencies related to IT policies and procedures.

7. Approves accreditation of enterprise designated financial systems, if not already identified as the Authorizing Official (AO). In this role, accept security risk identified during audits of designated financial systems, on behalf of CBP.

8. Works with CIO to incorporate user requirements for new financial applications or upgrades to existing financial applications.

9. Works with the CIO to integrate and test CBP-wide business continuity plan.

10. Coordinates with the CIO to identify the financial data needed to be backed up and recovered.

2.3.2 Chief Information Officer

The Chief Information Officer (CIO) is responsible for overseeing implementation and compliance of CFO-designated financial systems. The CIO shall:

1. Review and evaluate the CFO-designated financial systems to ensure ITGCs are in place and working effectively.

2. Work with the system owners to ensure remediation of ITGC deficiencies related to CFO-designated financial systems.

3. Track and monitor progress of ITGC POA&Ms and remediation efforts.

4. Ensure completion of Memorandums of Understanding (MOUs) and Interconnection Security Agreements (ISAs) for CFO-designated financial system interconnections with any system not owned by DHS; ensure that they include appropriate security clauses; and monitor service provider for compliance with MOUs and ISAs.

5. Implement the CBP-wide system development lifecycle methodology and monitor user compliance with this methodology.

6. As part of developing new financial applications or updating existing applications, integrate CFO feedback to ensure user requirement are adequately addressed.

7. Develop and test CBP-wide disaster recovery plan. Coordinate with the CFO to incorporate business continuity requirements and test on a periodic basis.

8. Based on CFO requirements, execute policies for the routine backing up and recovery of financial data. Implement policies and procedures for rotating back-up media off-site.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000035

2.3.3 Financial System Owners

Systems owners are responsible for implementing and monitoring CBP policies, processes, and procedures related to the integrity of the data processed through the application and ongoing business processes. They are required to maintain the security of the technical and operational environment hosting the financial applications. Owners of CFO-designated financial systems:

1. Work with the CISO to ensure designated financial systems are properly secured.
2. Designate an ISSO for each of their respective designated financial systems as defined in Section 2.8.1.
3. Ensure ITGCs are implemented and tested as required in DHS and CBP policy.
4. Develop, implement, and test application controls, as appropriate.
5. Ensure the completeness, accuracy, validity, and security of data inputs into, processed by, and output from the financial application.
6. Ensure that Interconnection Security Agreements (ISA) are completed and enforced.
7. Ensure that system POA&Ms are prepared and implemented with resources identified.
8. Ensure resources are available for correcting weaknesses.
9. Review and update the security of IT systems within their program area, in consultation with the CIO and CISO, at least annually.
10. Prioritize security weaknesses based on material weaknesses, external audits, and program assessments.
11. Comply with system development life cycle methodology for new system implementations or modifications to existing systems.
12. Participate in the developing and testing of disaster recovery/IT contingency plans for CFO-designated financial systems.
13. Ensure that security assessments of key security controls (i.e., ST&E, & SAR) for CFO Designated Systems are completed annually in Trusted Agent FISMA (TAF). This includes updating the ST&E and SAR annually.

2.4 Other Assistant Commissioners

The head of each CBP office shall support the CBP Information Security Program by participation in the activities listed below.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000036

1. Enforce the information systems security policies and procedures set forth in this handbook, including the appointment of the Information Systems Security Officers (ISSOs) in writing, as appropriate, who will report to the CISO.

2. Provide information to the CISO concerning the sensitivity of information under the Assistant Commissioner's purview. This information will assist in the decision regarding the security features that need to be operative, in order to protect the information within the application. This information should be provided during system development and updated whenever there is a change.

2.5 Chief Information Security Officer

The Chief Information Security Officer (CISO) is responsible for all aspects of FISMA compliance. This designation shall be made in writing by the Chief Information Officer, with the concurrence of the DHS CISO. The CISO must provide a SOC that complies with the DHS Security Operations Concept of Operations (CONOPS) (unclassified/classified). The CISO is the Chief of the Security and Technology Policy (STP) Branch and is appointed by the Commissioner. Specific duties are detailed below.

Policy ID	CBP Policy Statements	Relevant Controls
2.5.a	CISO shall develop and maintain a CBP-wide information security program in accordance with the DHS security program.	PL-1
2.5.b	Overall security management of the CBP enterprise is the responsibility of the CISO.	---

1. The CISO establishes and oversees the CBP Information Security Program and provides consulting assistance to all CBP offices for their individual programs.

2. Ensure that the CIO is kept apprised of all pertinent matters involving the security of IT systems.

3. Designate (as necessary) one or more subordinate Officials to support national infrastructures.

4. Develop, maintain, and disseminate CBP information security policy, which must align with the DHS Information Security Program and government-wide security regulations and directives.

5. Ensure that IT security-related decisions and information, including updates to the DHS 4300 and CBP 1400 series of IT security publications, are distributed to the ISSOs and other appropriate persons.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000037

6. Initiate new security policy change requests as necessary. Issue interim policy in the form of Interim Policy Letters. Such letters will be included into *the CBP Information Systems Security Policies and Procedures Handbook* upon its next publication.

7. Approve and/or validate all IT system security reporting.

8. Consult with the Privacy Office for reporting and handling of privacy incidents.

9. Manage IT security resources including oversight and review of security requirements in funding documents (e.g. OMB Exhibit 300).

10. Review and approve the security of hardware and software prior to implementation into the SOC.

11. Periodically test the security of implemented systems.

12. Implement and manage a Plan of Action and Milestones (POA&M) process for remediation.

13. Develop and publish procedures necessary to implement the requirements of DHS information security policy.

14. Ensure that ISSOs are appointed in writing for each Major Application (MA) and General Support System (GSS). Review and approve ISSO appointments.

15. Ensure that weekly incident reports are submitted to the DHS SOC.

16. Acknowledge receipt of Information Security Vulnerability Management (ISVM) messages, report compliance with requirements or notify the granting of waivers.

17. Manage CBP firewall rule sets.

18. Ensure that Interconnection Security Agreements (ISAs) are maintained for all connections that do not share the same security policy.

19. Ensure adherence to the DHS Secure Baseline Configuration Guides.

20. Ensure reporting of vulnerability scanning activities to the DHS SOC.

21. Develop, implement, and maintain an information security program in accordance with DHS and CBP policies and guidance.

22. Ensure training and oversight for personnel with significant responsibilities for information security.

23. Oversee the Certification and Accreditation process for major applications and general support systems.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000038

24. Maintain an independent CBP-wide System Test and Evaluation (ST&E) Program to ensure a consistent approach to testing of effectiveness of controls.

25. Ensure that the SOC performs an independent network assessment as part of the ST&E process for each application that is accredited.

26. Ensure that the C&A documentation is recorded in the DHS C&A Tool and FISMA Reporting Tool.

27. Exercise oversight over all security operations functions, including the SOC.

28. Serve as the Certifying Official for CBP.

29. Ensure that certification is accomplished for each MA and GSS and that the test results are documented. Review the C&A package (SSP, Security Assessment Report, and POA&M) and provide the AO with written recommendations for accreditation

30. Ensure all security-related vulnerabilities and incidents are recorded and serious or unresolved security violations are reported to the Assistant Commissioner, OIT and DHS.

31. Advise the Assistant Commissioner, OIT of vulnerabilities, residual risks, and use of special security features and mechanisms for each MA and GSS operating on the system. Develop a POA&M to mitigate residual risks.

32. Ensure that rules of behavior and security procedures/guides are developed.

33. Ensure that the results of annual security assessments (e.g., NIST SP 800-53) of MAs or GSSs are properly addressed in funding requests to mitigate identified risks, or carry out the POA&M.

34. Assess the system during the continuous monitoring phase of the Certification and Accreditation (C&A) process, including modifications to the system, its environment, and operational needs that could affect the security posture of the system and its accreditation status.

35. Ensure the appropriate ISSO prepares all Interconnection Security Agreements (ISAs) that permit the interconnection of a CBP-owned system with any non-CBP-owned system or external systems. For each ISA submitted for approval, establish proof of adequate information system security measures and recommend approval or disapproval to the signatory authority.

36. Ensure proper protective or corrective measures are taken when an incident or vulnerability is discovered within a system.

37. With the concurrence of the Director, EDME, approve or disapprove all requests submitted from any source that lead to internal or external penetration testing; bypassing, straining or testing security mechanisms; performing target monitoring;

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000039

keystroke monitoring; or any other functions that may infringe on the performance of either the organization or an individual.

38. As a member of the Technology Review Committee (TRC), review requirements for adding commercial technologies to the CBP Technical Reference Model (TRM). Ensure that a security evaluation of the product has been conducted before it is added to the TRM.

39. Serve as a member of the Configuration Management (CM) Board, and ensure CM of security-related software and hardware is maintained and documented.

40. Provide oversight of the Continuity Of Operations Plans (COOPs) of the OIT. Ensure that a contingency plan is prepared and tested annually.

41. All general support systems shall be under the direct oversight of the CISO, with support from the SOC. All general support systems must have one or more ISSO assigned.

42. Ensure execution of the DHS Logging Strategy.

43. Designate one or more CBP Information System Security Managers (ISSMs), as necessary, to serve in a supervisory capacity within the program offices and significant and complex IT systems.

2.5.1 Information System Security Manager

Through the authority granted by DHS to develop and maintain a Component-wide security program in accordance with the DHS security program, the Chief Information Security Officer may designate one or more CBP Information System Security Managers (ISSMs), as necessary, to serve in a supervisory capacity within the program offices and significant and complex IT systems. The ISSM would serve as the coordinator for the CBP information security ogreram within the Program Offices on behalf of the CISO.

As the Certifying Official (CO), the CISO reserves the sole authority to certify IT systems within CBP for the Authorizing Official. Although the ISSM ensures that ISSOs are appointed for each system, the CISO retains veto and approval authority over the hiring or assignment of all ISSOs.

The ISSM are delegated with the authority to perform the following activities within their program office:

1. Oversee the information security program.
2. Ensure that the CBP CISO is kept apprised of all pertinent matters involving the security of information systems.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000040

3. Ensure that information security-related decisions and information, including updates to either the DHS 4300A or CBP 1400-05 series of information security publications, are distributed to their ISSOs and other appropriate persons.
4. Validate all Program Office information system security reporting.
5. Consult with the CBP CISO and the CBP Privacy Officer or Privacy Point of Contact for reporting and handling of privacy incidents.
6. Coordinate information security resources including oversight and review of security requirements in funding documents with the CBP CISO.
7. Periodically test the security of operational IT systems.
8. Implement and manage a Plans of Actions and Milestones (POA&M) process for remediation all program office security issues.
9. Ensure that weekly incident reports are forwarded to the CBP CISO.
10. Acknowledge receipt of Information Security Vulnerability Management (ISVM) messages, report compliance with requirements or notify the granting of waivers to the CBP CISO.
11. Ensure adherence to the DHS and CBP Secure Baseline Configuration Guides.
12. Develop and publish procedures necessary to implement the requirements of CBP information security policy within the appropriate Component.
13. Implement information security policies, procedures, and control techniques to address all applicable requirements
14. Ensure that ISSOs are appointed for each information system managed at the Component level.
15. Ensure training and oversight for personnel with significant responsibilities for information security
16. Oversee the C&A process for all IT systems in use, including taking an active role in reviewing security documents to ensure that all C&A packages are thorough and accurate and that all NIST 800-53 controls are answered as required by the RTM questions *prior* to being submitted to Security and Technology Policy (STP) Branch for CBP CISO approval.
17. Ensure that security controls are ALL answered as required by the RTM and address the following four areas: (1) What is the security solution or countermeasure that is in place? (2) Who is responsible for enacting and/or maintaining the solution? (3) How often is the solution implemented/reviewed/updated? and (4) How does the identified solution satisfy the requirements of the particular control?
18. Ensure that the Plan of Execution (POE) is determined and approved and then executed as scheduled and agreed upon.
19. Ensure that all policy waiver and/or exception requests, POA&M extension requests, MOUs, and ISAs are reviewed and approved *prior* to being submitted to STP for CBP CISO approval.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000041

20. Ensure that all POA&Ms are managed and all milestones are met.
21. Ensure that all system self assessments are completed on schedule
22. Represent security at IT security system audits, critical control or program reviews, and other CBP-level reviews
23. Ensure that all system connectivity is identified and documented in the system security plans and also addressed with a memorandum of understanding and/or interconnection security agreement (ISA) as necessary
24. Work with the STP FISMA Compliance Team (FCT) to ensure that all FISMA requirements are met and that the FISMA scorecard reflects the goals set by the CBP CISO.

2.6 Risk Executive

A Risk Executive ensures that risks are managed consistently across the organization. In keeping with its organizational structure, DHS has two levels of Risk Executives – Departmental and Component.

Policy ID	CBP Policy Statements	Relevant Controls
2.6.a	The DHS CISO shall be the DHS Risk Executive.	PL-1
2.6.b	CBP CISO is the Risk Executive within CBP.	PL-1

The CBP Risk Executive is responsible for the following:

- Ensure that managing information system-related security risks is consistent across the CBP, reflects CBP risk tolerance, and is performed as part of an CBP-wide process that considers other CBP risks affecting mission/business success
- Ensure that information security considerations for individual CBP information systems, including the specific authorization decisions for those systems, are viewed from an CBP-wide perspective with regard to the overall strategic goals and objectives of the organization
- Provide visibility into the decisions of the authorizing official and a holistic view of risk to the CBP beyond the risk associated with the operation and use of individual information systems
- Facilitate the sharing of security-related and risk-related information with the AO and other senior leaders within the CBP in order to help these officials consider all types of risks that may affect mission and business success and the overall interests of the organization at large

The DHS Risk Executive (the DHS CISO) develops information security policy, establishes the standards for system security risk, oversees risk management and monitoring, and approves all waivers and exceptions to DHS policy.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000042

The CBP Risk Executive may establish standards for system security risk more stringent than the DHS standard. They implement the system security risk management and monitoring program and submit requests for higher-risk deviations from the enterprise standard.

2.7 Certifying Official

The Certifying Official (CO) is a senior management official who certifies the results of the security assessment. A Certifying Official is assigned in writing to each information system by the CIO. He or she shall be a Federal employee.

The Certifying Official and the team conducting a certification must be impartial, that is, free from any perceived or actual conflicts of interest with respect to the developmental, operational, and/or management chain of command associated with the information system or to the determination of security control effectiveness.

For systems with low impact, a Certifying Official and/or certifying team do not need to be independent so long as assessment results are carefully reviewed and analyzed by an independent team of experts to validate their completeness, consistency, and veracity.

The AO decides the required level of certifier independence based on the criticality and sensitivity of the information system and the ultimate risk to organizational operations, organizational assets, and individuals. The AO determines if the level of certifier independence is sufficient to provide confidence that the assessment results produced are sound and can be used to make credible, risk-based decisions.

Policy ID	CBP Policy Statements	Relevant Controls
2.7.a	The CBP CISO shall serve as Certifying Official.	CA-4
2.7.b	The Certifying Official may be responsible for more than one system.	CA-4

The Certifying Official will:

1. The Certifying Official must be a Federal employee and must be designated in writing for each IT system. The Designation letter shall be signed by the Commissioner.
2. Ensures that the required Certification and Accreditation (C&A) activities are completed, and that the test results are documented.
3. Ensures that a risk analysis is performed and that it identifies risks, determines their magnitude, and identifies areas needing safeguards.
4. Ensures that a system test and evaluation is conducted and the results of such tests are documented or updated annually.
5. Ensures that rules of behavior and security procedures/guides are developed.
6. Ensures that a contingency plan is prepared and tested annually.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000043

7. Ensures that the C&A documentation is recorded in the DHS C&A Tool and FISMA Reporting Tool

8. Reviews the C&A package (SSP, Security Assessment Report, and POA&M) and recommends to the AO whether or not the system should be accredited.

9. Prepares the security accreditation decision letter for the AO's signature.

2.8 Certification Agent

The Certification Agent (CA) is a technically qualified security professional that reports to the CISO and provides a level of independent evaluation that is required by the Certification and Accreditation (C&A) process. The CA provides an independent assessment of the security plan to ensure it provides a set of security controls for the information system that is adequate to meet all applicable security requirements. In addition, the CA is responsible for a comprehensive assessment of the management, operational, and technical controls of the information system to determine if they are implemented correctly, operating correctly, and meeting the security requirements. The CA recommends corrective actions to reduce or eliminate security vulnerabilities. The results of the assessment of the security controls are documented in the Security Assessment Report (SAR) along with a list of recommended corrective actions and a plan of action and milestones (POA&M) to ensure their implementation. The SAR is the certification agent's statement regarding the security status of the information system.

The Certification Agent will:

1. Assist with information systems security audits and reviews, as appropriate. With the appropriate ISSO, determine the priority level associated with audit findings.

2. Validate that the information system design meets a specified set of managerial, operational, and technical security requirements and that it includes the implementation of an adequate audit trail capability of security-related activities as prescribed in Attachment T of this handbook.

3. Determine, with the data owner(s) and ISSO(s), the minimum-security features for each unique application.

4. Ensure security plans are developed for all information systems. Ensure that the application is certified and the certification documentation is developed using the DHS C&A tool, Risk Management System (RMS)

5. Review and evaluate security impact of changes to the applicable IT system, including interfaces with other networks.

6. Observe the testing of security controls for assigned MAs and GSSs.

7. Provide written justification, when appropriate, to the CISO for approval by the Assistant Commissioner, OIT to obtain a written waiver of or exception to the policy for mandated security features.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000044

8. Review C&A Packages and work with the assigned ISSOs and system owner to ensure that the security requirements of the system have been documented, tested, and implemented. Write the Security Assessment Report (SAR) and include the Certification Statement as part of the SAR. The final Plan of Actions and Milestones (POA&M) and a list of residual risks must also be included in the C&A Package. Forward the C&A Package to the CISO and AO for approval.

9. CAs represent the STP Branch at key project meetings, as directed by the CISO.

10. Validate TrustedAgent FISMA (TAF) submissions for FISMA compliance.

11. Maintain an on-line copy of the following documents and ensure the documents are current: annual security self-assessment (i.e., NIST SP 800-53), System Assessment Report (SAR), System Security Plan (SSP), Security Risk Assessment Report, Contingency Plan and Test Results, Security Test Plan and Evaluation, Vulnerability Scan Results, signed POA&M, Signed Accreditation Transmittal Letter.

2.9 Information Systems Security Officer

The Information Systems Security Officer (ISSO) serves as the subject matter expert (SME) for security and is assigned to Major Applications (MAs) and General Support Systems (GSSs). Given the broad scope and dynamic nature of the IT security discipline, each system needs an SME within STP to provide security consultation and interpretations of security policies as they relate to specific architectures and projects. In CBP, ISSOs are responsible for ensuring the implementation and effectiveness of security controls in accordance with Department policies. The ISSOs ensure a system is adequately protected while also addressing the legitimate needs of the user community for access and availability. System Owners/Managers will provide the majority of ISSOs and the CISO will appoint all ISSOs in writing using the DHS 4300A, *Sensitive Systems Handbook, Attachment C – Information Systems Security Officer (ISSO) Designation Letter*. ISSOs report to the CISO and are responsible for providing the CISO with the security documentation for the information system to which they are assigned. An ISSO can be either a government employee or a support contractor with an appropriate Background Investigation and security clearance. ISSO duties shall not be assigned as a collateral duty unless approved by the CISO. Any collateral duties shall not interfere with their ISSO duties.

Policy ID	CBP Policy Statements	Relevant Controls
2.9.a	An ISSO shall be designated for every information system and serve as the point of contact (POC) for all security matters related to that system.	PL-1
2.9.b	An ISSO shall ensure the implementation and maintenance of security controls in accordance with the System Security Plan (SSP) and CBP/DHS policies.	PL-1
2.9.c	An ISSO may be a CBP employee or a contractor.	PL-1

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000045

Policy ID	CBP Policy Statements	Relevant Controls
2.9.d	An ISSO may be assigned to more than one system.	PL-1
2.9.e	ISSO duties shall not be assigned as collateral duties unless approved by the CISO.	PL-1

Specific ISSO duties are detailed below.

1. Ensure that systems are operated, maintained, and disposed of in accordance with internal CBP security policies, practices, and procedures outlined in this handbook.

2. Determine the appropriate levels of security required to protect integrity, availability, and confidentiality of the information system data, and verify these levels with the Certification Agent (CA) and/or CISO.

3. Conduct an information system security analysis to determine and document appropriate security requirements during the design stage of an application.

4. Assist developers to incorporate security requirements into their applications that comply with all laws, regulations, and security policies. Verify that these requirements are appropriate, sufficient, and comply with organizational infrastructure standards.

5. Develop and maintain all Certification and Accreditation (C&A) Packages generated for assigned systems and coordinate each accreditation package with the appropriate personnel. Forward the hard copy of the signed accreditation package to the Certification Agent (CA) for further review and approval.

6. Develop and maintain all Interconnection Security Agreements (ISAs) that permit the interconnection of CBP owned systems with any non-CBP owned systems. Coordinate each ISA with appropriate personnel and forward the hard copy of the signed ISA to the Certification Agent for further review and approval.

7. Provide an assessment of security effectiveness of proposed hardware and software.

8. Ensure that all reported security-related incidents are immediately reported to the CSIRC. (See Section 4.9) Investigate security incidents to support the CSIRC, if directed, and report findings to the CISO.

9. With the concurrence of the CISO, initiate protective or corrective measures when a security incident or vulnerability is discovered.

10. Ensure Configuration Management (CM) for security-related software and hardware is maintained and documented. If a CM board exists, the ISSO may serve as a member of the CM board if so designated by the CISO.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000046

11. Ensure system security requirements are addressed during all phases of the system life cycle.

12. Ensure security features are properly restored and procedures are followed during system recovery processes.

13. Ensure all information system security-related documentation is current and accessible to authorized individuals.

14. Ensure a virus-free environment by coordinating with systems operations to maintain current anti-virus engines and signature files on all workstations and servers.

15. Ensure that requests to bypass, strain, or test security mechanisms are forwarded in advance to the CISO for review and approval.

16. Certify that appropriate procedures are used to cleanse system components before they are released. (See Section 4.3 and Attachment Y)

17. Notify the responsible CA and CISO when changes occur that might affect accreditation. This includes the recommendation to rescind any accreditation when systems are no longer used or fail to maintain the required security posture.

18. Inspect information systems to ensure the absence of unapproved software (including shareware and copyrighted software) and ensure the presence of the approved Department Security Warning Banner.

19. Ensure that security training programs applicable to all assigned security personnel are developed and maintained for applications and systems assigned to them.

20. Using the Security Operations Center (SOC) audit tools, ensure that audit logs for assigned systems are reviewed for security anomalies.

21. Develop a test plan and test the security controls that have been developed for assigned information systems. The CA should also observe the testing of the security controls.

22. Provide system owners and developers with appropriate budgetary inputs to ensure that information security features and operations are adequately funded. (See Section 3.2 and 3.6.) Assist system owners and developers to ensure that results of periodic security self-assessments, risk assessments, and independent audits are reflected in subsequent program funding requests.

23. Maintain a file (on-line or hardcopy) of the following documents and ensure the documents are current:

    a. Copies of all accreditation packages developed for assigned systems.

    b. Copies of all security policy documents.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000047

c. Copies of security risk assessments performed on assigned applications and/or information systems including vulnerability assessments for the same.

d. A copy of the last information system Security Self-Assessment or NIST SP 800-53 for each assigned Major Application (MA) or General Support System (GSS).

24. Serve as the principal points of contact for all IT security aspects pertaining to their systems.

25. Work closely with the DHS and CISO staff to interpret and apply IT security policies and implementing procedures.

26. Serve as liaison between system owners and the CISO.

27. Work with system owners to document weaknesses in POA&Ms and initiate corrective action.

28. Employ automated tools (approved by the DHS CISO) such as the Risk Management System (RMS) and TrustedAgent FISMA (TAF).

2.9.1 Information System Security Officers supporting Privacy Sensitive Systems:

1. Update system Security Plans documenting the implementation of all key Privacy controls.

2. Update risk assessments to address risks associated with Data Transport and Off-site storage, Remote Access to Personally Identifiable Information (PII) Data and Remote Storage.

3. Monitor key operational Privacy Controls to ensure controls remain in compliance.

4. Verify erasure of any expired PII extracts.

5. Obtain System Owner and CBP Privacy Officer's approvals to extract PII computer-readable data extracts that are outside of a system security plan.

6. Perform or oversee performance of day-to-day security operations of the system.

7. Develop or assist in development of the system security policy.

8. Ensure compliance with system security policy.

9. Assess security impact of system changes.

10. Develop and update the system security plan.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000048

2.9.2 Information System Security Officers supporting Chief Financial Officer-Designated Financial Systems

1. Update System Security Plans documenting the implementation of all key financial and financial internal controls.

2. Update Risk Assessments to address risks and potential impacts to the financial statement associated with security control weaknesses.

3. Monitor key operational Financial Controls to ensure controls remain in compliance.

4. Perform annual NIST SP 800-53 assessments for all required controls (100% coverage).

5. Provide support to annual financial systems audits as directed by the system owners and the CISO.

2.10 Supervisors and Managers

Each supervisor or manager is responsible for maintaining information system security within his or her specific work environment. Supervisors or managers may be located within an office at CBP Headquarters, the National Data Center (NDC), or other field locations. The responsibilities of supervisors and managers include the following:

1. Protect sensitive information system data and resources within their area of responsibility with appropriate security safeguards.

2. Verify that subordinates have access to only those information system applications and data necessary to perform authorized tasks (principle of least privilege). DO NOT authorize more than one account on the same system for an individual.

3. Conduct an annual review of current access lists for each system accessed by subordinates and revalidate their access requirements.

4. Report any changes in employee access requirements to the appropriate ISSO, System Administrator (SA), or Security Control Officer (SCO) as appropriate. In addition, coordinate with appropriate management when employee or management transfers occur that could affect information system access.

5. Ensure that proposed acquisitions of information system-related hardware, software, communications, applications, and equipment satisfy information system security requirements, meet security Technical Reference Model (TRM) architecture standards, and receive ISSO concurrence before acquisition. As part of the investment management program (See Section 3.2.), security requirements must be developed and funded in accordance with OMB budget request guidelines.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000049

6. Ensure that subordinates receive information system security training relevant to their assignments, as required by law, regulations, Memorandums of Understanding (MOUs) or other agreements.

7. Attend information system security training as required by law, regulations, MOUs, or other agreements.

8. Execute limited personal use policy for CBP employees and vendor support personnel using CBP-owned office equipment in accordance with U.S. Customs Directive 5230-031, Limited Personal Use Of Government Office Equipment Including Information Technology, January 19, 2001:

    a. Obtain, review, and enforce compliance with the "Limited Personal Use Policy" stated within the directive.

    b. Review and approve/disapprove each employee's request for personal use of CBP-owned systems. If there are any questions, contact the CISO.

    c. Respond to employee questions regarding acceptable use of government office equipment for personal reasons.

    d. Once approved, determine employee need for personal use annually, monitor for inappropriate usage, and reinforce this policy to restrict, suspend, or refuse the privilege of personal use when appropriate. Notify the CISO of violations of this policy.

    e. Revoke or limit the privilege to use such equipment for non-government purposes as necessary. All revocations will be reported as a security incident.

2.11 Privacy Officer

The Privacy Officer will be assisted by the DHS Chief Privacy Officer (CPO) to comply with Federal laws and DHS privacy policy. The Privacy Office will work with the CIO and DHS CPO to maintain privacy requirements. The SOC shall work with the Privacy Office, or with the DHS CPO to address suspected or confirmed privacy incidents (PI) or incidents involving PII.

Policy ID	CBP Policy Statements	Relevant Controls
2.11.a	The Privacy Officer shall review program and system Privacy Threshold Analyses (PTA), Privacy Impact Assessments (PIA), and System of Records Notices (SORN), providing approval as appropriate.	PL-1, PL-5

The Privacy Office is responsible to the DHS CPO and shall:

1. Advise the CIO and management regarding privacy issues.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000050

2. Review Privacy Threshold Analysis (PTAs) prior to submission to the DHS CPO for accuracy, and provide any additional information needed after submission to assist the DHS CPO with a determination as to whether it is a privacy sensitive system.

3. Work with system owners who maintain privacy sensitive systems to complete required Privacy Impact Assessments (PIAs) and System of Records Notices (SORNs) and review documentation for mitigating possible privacy risks.

4. Coordinate with program managers, CISO, CSIRC, or SOC in evaluating and reporting suspected or confirmed privacy incidents.

5. Implement the Privacy Incident Response Plan as outlined in the DHS Privacy Incident Handling Guidance (PIHG).

6. Periodically review logs maintained by system owners, program managers, or supervisors for computer-readable PII data extracts not covered by a system security plan.

7. Implement Privacy Awareness training and education as directed by the DHS CPO.

2.12 Program Manager

Program Managers are responsible for ensuring compliance with applicable Federal laws, directives and DHS and CBP policy governing the security, operation, maintenance and privacy protection of IT systems, information, projects and programs under his or her control.

Policy ID	CBP Policy Statements	Relevant Controls
2.12.a	Program Managers shall ensure that program POA&Ms are prepared and maintained.	CA-5
2.12.b	Program Managers shall prioritize security weaknesses for mitigation.	CA-5
2.12.c	Program Managers shall provide copies of program POA&Ms to affected System Owners.	CA-5

Program Managers shall:

1. Work with system owners, CISO, and their staffs to ensure information systems are properly secured.

2. Understand how to recognize and respond to suspected or confirmed security incidents, privacy incidents or incidents involving PII.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000051

3. Consult with the privacy office concerning privacy incidents and other privacy issues affecting IT systems and programs under his or her control.

4. Prepare and transmit written Privacy Event Notification (PEN) simultaneously to the privacy office, the CIO and CISO.

5. Supplement privacy incidents reports to the SOC and US-CERT as information becomes available.

6. Prepare and submit to the Privacy Office for approval of PTA for systems or programs, and Privacy Impact Assessments and System of Records Notices, as required and provide additional information to the Privacy Officer in order to finalize the required documents. In some instances changes to the system or the standard operating procedures may be required to reduce the impact on privacy and receive approval of the program from the DHS Chief Privacy Officer.

7. Develop standard operating procedures to handle routine computer-readable PII data extracts that are removed from the system security boundaries of the SSP of the C&A'd system. Computer-readable PII data extracts that are not covered by an appropriate SSP must be logged and may be reviewed periodically by the DHS Privacy Office or the Privacy Officer for compliance.

2.13 United States Computer Emergency Readiness Team

The United States Computer Emergency Readiness Team (US-CERT) is designated as the central reporting organization within the Federal Government and serves as the central repository for Federal incident data. The DHS SOC will report security incidents to the US-CERT. The US-CERT may notify law enforcement, the Identity Theft Task Force, the Social Security Administration, and the Executive Office of the President, as appropriate.

2.14 Information System Owners and Information Owners

In the context of this handbook, system owners and information owners are responsible for categorizing the security of data and/or systems in accordance with FIPS PUB-199, in addition to other role-based responsibilities. The distinction between system owners and information owners is not immediately obvious, and the roles may fall to different individuals, depending on the life cycle of the system. A single information system may process data from multiple information owners. Likewise, an information owner's data may reside on or be processed across multiple information systems. The information owner is responsible for ensuring the integrity and confidentiality of the information/data.

In the CBP environment, for example, an organization that owns development of a new application must coordinate with information owners in order to define the security categorization and requirements of the data processed by the application. In the production environment, system owners must identify and maintain the security level of the servers, LAN, and other devices, which support operation of one or many applications. All systems require a System Owner designated in writing for proper administration of security.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000052

Policy ID	CBP Policy Statements	Relevant Controls
2.1.4.a	The System Owner shall ensure that each of their systems is deployed and operated in accordance with this policy document.	PL-1
2.1.4.b	The System Owner shall ensure that an ISSO is designated in writing for each information system under their purview.	PL-1

System owner responsibilities may include the following[1]:

1. Prepare, develop, integrate, modify, operate or maintain an information system.
2. Develop the system security plan in coordination with information owners, the system administrator, the ISSO, the CISO and the functional "end users".
3. Maintain the system security plan and ensure that the system is deployed and operated according to the agreed-upon security requirements.
4. Ensure that a system security plan is developed and updated annually and a yearly security self-assessment (NIST SP 800-53) is conducted for each system (i.e., MA or GSS).
5. Provide an ISSO for each system under his/her responsibility or ensure that one is assigned.
6. Inform agency officials of the need for C&A (or re-certification/re-accreditation) and ensure appropriate resources are available.
7. Ensure that system POA&Ms are prepared and maintained and points of contact and resources are identified.
8. Ensure that a final accreditation package is signed by the AO before the system is implemented in production.
9. Ensure that an ISSO is formally assigned to each IT system under their control and that this assignment is appropriately documented.

[1] *NIST Special Publication 800-37Rev 1, DRAFT* Guide for the Security Certification and Accreditation of Federal Information Systems, *states that these roles are agency officials. CBP may incorporate the responsibilities of system owner and information owner under other job titles that have adjunct security responsibilities.*

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000053

10. Ensure that required computer security functions and documentation are included in system life cycle planning and budgets and appropriate resources are available for the security certification and accreditation.

11. Work closely with the CIO and other program and IT managers to ensure a complete understanding of risks, especially the increased risks resulting from interconnectivity with other programs and systems.

12. Document and manage accepted security risks in risk assessments.

13. Update the security of IT systems within their program area annually.

14. Prioritize security weaknesses for mitigation based on material weaknesses, external audits and program assessments and ensure mitigation funding is made available or is requested.

15. Ensure that all reported security-related incidents are immediately reported to the CSIRC. (See Section 4.9.6.) Investigate security incidents to support the CSIRC, if directed, and report findings to the CISO.

16. Work with the Privacy Office to Conduct Privacy Impact Assessments (PIA).

17. Report Privacy and Computer Security incidents as appropriate, in coordination with the CISO and Program Manager.

18. Develop Privacy Impact Assessments and obtain PIA approvals from the DHS Privacy Office for privacy systems.

19. Ensure PII identified systems implement all necessary NIST SP 800-53 controls as identified in OMB M-06-16.

20. Ensure necessary resources are allocated to remediate any areas of privacy sensitive systems that are non-compliant with key privacy controls.

21. Provide necessary system-related documentation to the certification agent.

22. Take appropriate steps to reduce or eliminate system vulnerabilities identified in the security certification and accreditation process.

2.15 Users of Supplied Computing Resources

CBP employees, contractors, and vendors working on behalf of CBP, are responsible for reporting suspected or confirmed computer security incidents to the CSIRC, in accordance with the incident response procedures. (See Attachment F for details on incident reporting procedures and definitions of incidents.)

Successful situational awareness depends on effective security awareness and incident handling. CBP will review its security awareness training requirements annually to ensure they reflect the evolving and changing nature of incidents.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000054

2.16 All Users

All CBP and vendor support personnel who are authorized access to CBP information systems are responsible for protecting that data.

Policy ID	CBP Policy Statement	Relevant Controls
2.16.a	CBP users shall follow prescribed rules of behavior.	PL-4

User responsibilities are detailed below.

1. Have completed a favorable adjudicated Background Investigations (BI). Hold appropriate CBP security clearances and have access approvals equal to or exceeding the maximum classification of information processed on any system to which he/she is granted access.

2. Access only data, control information, software, hardware, and firmware for which he/she is authorized access and has a need to know; and assume only those roles and privileges for which he/she is authorized.

3. Know the classification level of the data he/she handles or has access to and take appropriate measures to safeguard that data.

4. Comply with CBP security policies in the use of workstations, laptops, and other electronic devices.

5. Immediately report a suspected or confirmed security incident to the CSIRC and notify your supervisor/manager if it is a significant incident. (See Attachment F for details on incident reporting procedures and definitions of incidents.)

6. Complete initial and yearly refresher security awareness training courses. Training shall be specific to user security responsibilities.

7. Comply with identification and authentication guidance, specifically pertaining to password management.

8. Ensure encryption technology has been installed and in use on your laptop computer. Encryption validated under FIPS 140-2 is required. (See your LAN administrator to ensure validated FIPS 140-2 encryption was installed.) Assume responsibility for the security and protection of the laptop and information systems and data accessed.

9. Do not download or open files from unknown or un-trusted sources. All such files should be scanned by antivirus software before opening them. Do not open suspicious email, mailed from an unknown source, nor open attachments from Internet mail unless for official business.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000055

2.17 Additional Personnel

Other personnel throughout DHS are responsible for various aspects of the IT security program. Contracting Officers and their Technical Representatives, project managers, system and network administrators, managers, supervisors, and users all play a role in helping to ensure the security of the Department's IT systems. The DHS 4300A Sensitive Systems Handbook provides a description of the roles and responsibilities of these additional personnel.

In implementing DHS information security policy, the Commissioner will include these additional personnel in their security plans.

2.17.1 System Administrators - Network Administrators

System Administrators (SAs) and Network Administrators are responsible for daily operation and maintenance of systems. SAs keep systems and LANs operating and in service for the users. Where information security is concerned, any resource that performs the duties of an SA has the following responsibilities:

1. System administrators, who have a need for and have been granted root access, are responsible for protecting the root, administrator or super user authenticator at the highest sensitivity level it secures. These SAs should not share the authenticator and/or account.

2. Report all suspected information system security-related problems, security anomalies, system vulnerabilities or suspicious activities of authorized users to the ISSO assigned to the system.

3. Notify the ISSO and the change control board of any major system changes or system configuration changes that might adversely affect systems security.

4. Use special access or privileges granted to perform only authorized tasks and functions.

5. Notify the CSIRC of any detected violations of user access to assure timely detection of suspicious, inappropriate, or unauthorized activity.

6. Establish audit trails. Facilitate their review when required.

7. Maintain configuration control of the system and its application software.

8. Notify the ISSO when feasible security safeguards and features are not implemented on the information system or network.

9. Do not attempt to strain or test security mechanisms without authorization from the CISO or perform target or keystroke monitoring of an individual without written authorization from Internal Affairs (IA). Request permission for such testing or monitoring through the ISSO.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000056

10. Under the direction of the ISSO and with written approval from IA, perform authorized target monitoring of an individual using approved software in accordance with CBP security policy.

11. Assist the ISSO in developing and maintaining the accreditation package for the LAN system defined as a General Support System (GSS).

12. Participate in computer security incident reporting in accordance with Section 4.9.

13. Support compliance with functional security requirements as requested by the ISSO for locally developed, sensitive information system products, as appropriate.

14. Distribute initial passwords to the system user equivalent to the password distribution policy cited, as contained in Section 5.1 Identification and Authentication Policy and in Attachment L: Identification and Authentication - Password Management.

15. Deactivate unused accounts monthly. For systems with a low impact for the confidentiality security objective, consider an account unused if no login has occurred in 90 days. For systems with a moderate or high impact for the confidentiality security objective, consider an account unused if no login has occurred in 45 days.

2.17.2 System Control Officer

Certain administrators have unique security related duties and responsibilities. System Control Officers (SCOs) are appointed by local management (e.g., Directors, Field Operations, Port Directors). For AES, the Office of Field Operations, Headquarters (HQ) appoints officers in Outbound Operations HQ to be AES SCOs. SCOs have the following responsibilities:

1. Providing and removing access to assigned systems. (e.g., ACE, ACS, AES, TECS, SEACATS, etc)
2. Assigning and removing privileges based upon Supervisor/Manager written (e.g., e-mail) authorizations.
3. Revoking or suspending application access when a user separates from CBP or is transferred.
4. Documenting and retaining the authorization in accordance with procedures identified for each system.
5. Providing the ISSO and auditors with authorization documentation when requested.
6. Reporting user provisioning issues to the ISSO or a SCO chain ending with the National SCO as needed.

SCOs shall not grant or revoke system access or privileges to individuals without written authorization. To do so is a security violation and it may result in disciplinary action.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000057

2.17.3 OneNet Steward

The Customs and Border Protection (CBP) Technology Operations Division serves as the OneNet Steward and is responsible for daily operations and management of the DHS SOC. The DHS Configuration Governance Board provides management guidance. The SOC Steward is responsible for informing the DHS CIO, the DHS CISO, and senior management of significant incidents, and providing the status and outcome of ongoing investigations. The Steward is also responsible for distributing reports to the DHS and CBP CIOs, the DHS CISO, and to the CBP CISO. The OneNet Steward shall implement Trust Zones.

2.18 Security Operations Center

The Security Operations Center (SOC) serves as the first tier for security monitoring, incident response and vulnerability management of CBP information assets. The SOC administers, monitors, respond to, and reports on security devices, events and incidents involving networks or devices within their watch areas.

CBP will develop and publish internal computer security incident response plans and incident handling procedures, and provide copies to DHS CSIRC. These procedures will include a detailed configuration management process for security devices.

The CSIRC will most often initiate incident evaluation processes in accordance with CBP's incident response or evaluation plan. The CSIRC shall report incidents to the DHS CSIRC and not to any other external agency or organization. For events involving devices on other local area networks (LAN), CBP is responsible for notifying the LAN owner and the DHS CSIRC.

The CSIRC shall have the ability to respond 24 hours a day, 7 days a week or will outsource this capability to the DHS CSIRC. CBP will maintain an accurate list of key points of contact (POC) and provide a listing to the DHS SOC. POC changes will be reported as part of the weekly report.

The Incident Response team(s) shall catalog CBP capabilities (forensic, malware, analytical, etc) and points of contact so that CBP can be leveraged appropriately in the event of a national level cyber incident. Incident response personnel will have a background investigation and clearance commensurate with the classification level of the information with which they are working and viewing.

CBP will compile and maintain a list of mission-critical systems and applications which will assist in determining the classification and prioritization of security incidents and in developing vulnerability scan schedules. CBP will provide the DHS SOC with daily updates of scheduled scans and quarterly updates of asset classification and prioritization.

1. The SOC should include access to Homeland Secure Data Network (HSDN).

2. The SOC will monitor HSDN and react to threat information on a continuous basis.

3. The SOC shall maintain an area cleared for open storage of classified information to the SECRET level continuously.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000058

4. The DHS SOC and SOC shall have the ability to process SECRET level information continuously.

5. All SOC personnel shall be cleared to the SECRET level.

The SOC will maintain an updated TAF inventory list for their financial systems and report incidents to the DHS SOC using a TAF name and ID.

The SOC responsibilities include:

1. Keeping CBP leadership informed of matters concerning DHS OneNet security.

2. Maintain robust, continuous CBP-wide security situational awareness

    a. Includes an operational intelligence capability for ensuring appropriate situational awareness across the IT enterprise, including the ability to operate continuously in the collateral secret environment.

3. Administering and monitoring CBP IDS sensors and security devices.

4. Reporting and responding to detected faults, attacks, events or incidents.

5. Coordinating and overseeing the DHS incident and outage escalation process for all computer security incidents.

6. Coordinating and overseeing the CBP incident and outage escalation process for all computer security incidents.

7. Coordinating with the privacy offices/PPOC for reporting of suspected or confirmed privacy incidents or incidents involving PII.

8. Maintaining an up-to-date system inventory list based on the TrustedAgent FISMA (TAF) inventory report.

9. Providing the following reports to CBP leadership:

    a. Vulnerability Scanning Schedules

    b. Vulnerability Scan Reports

    c. Intrusion Detection Reports

    d. Computer Security Incident Reports.

10. Maintaining a current point of contact list to quickly notify appropriate parties based on incoming calls. Points of contact that shall be maintained by the DHS SOC include but are not limited to:

    a. The CIO, and CISO,

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000059

b. Program managers for CBP financial systems and high FIPS 199 categorization systems

c. ISSOs for all CBP systems

d. Chief Privacy Officers

e. Chief Security Office

f. Chief Financial Office

g. All Site Security Officers (SSO).

11. Any time the SOC experiences a reduction of capabilities, the CBP management and the DHS SOC shall be notified within 60 minutes.

12. Maintain a CBP-wide incident reporting, handling and response capability.

13. Implement both general and threat-specific IT logging requirements, as outlined in Management Directive 4300 and as amplified by the DHS SOC.

14. Deploy a CBP-wide network scanning program.

15. Oversee the implementation of a CBP-wide Security Content Automation Protocol (SCAP) compliance program.

16. Follow guidance and direction from the DHS SOC.

17. Respond to Information Security Vulnerability Management (ISVM) alerts and resolve major vulnerabilities as they become known.

18. Provide oversight of CBP-level Policy Enforcement Points (PEP).

19. Maintain a Backup Center, capable of assuming all SOC roles and responsibilities when required.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000060

3.0 MANAGEMENT CONTROLS

Management controls focus on management of the IT system (major application or general support system) itself and management of risk to that system. Examples include conducting risk assessments, developing rules of behavior, and ensuring that security is an integral part of the System Life Cycle (SLC) and the Capital Planning and Investment Control (CPIC) processes. Management controls consist of techniques and concerns that are normally addressed by management personnel as indicated in the following sections.

3.1 Basic Requirements

All security reports regarding CBP IT systems (major applications and general support systems) shall be submitted by the CISO to the Assistant Commissioner or a designated representative. The CISO shall interpret and manage CBP security policies and procedures to meet Federal, Departmental, and other CBP requirements. The CISO shall also answer data queries from the Compliance and Oversight Program Director and develop and manage information security guidance and procedures unique to CBP's requirements. ISSOs are the primary points of contact for the security of the IT systems assigned to them. They develop and maintain System Security Plans and are responsible for overall system security.

Policy ID	CBP Policy Statements	Relevant Controls
3.1.a	Every CBP computing resource (e.g., desktops, laptops, servers, portable electronic devices) shall be individually accounted for as part of a recognized IT system.	CM-8
3.1.b	The DHS CIO, in cooperation with each CBP senior official, shall be responsible for ensuring that every CBP computing resource is designated as a part of an IT system (major application or general support system).	CM-8
3.1.c	A System Security Plan shall be prepared and accurately maintained for each CBP IT system.	PL-2, PL-3
3.1.d	An ISSO shall be designated for every CBP IT system.	PL-1
3.1.e	The CBP Information Security Program shall be structured to support DHS and applicable FISMA, OMB, and other federal requirements.	PL-1
3.1.f	Information security reports regarding CBP IT systems shall be submitted to the CBP senior official or designated representative.	---
3.1.g	The ISSO for each IT system shall serve as the POC for all security matters related to that system.	PL-1

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000061

Policy ID	CBP Policy Statements	Relevant Controls
3.1.h	The CISO shall ensure that CBP IT systems comply with the CBP/DHS Enterprise Architecture (EA) and Security Architecture (SA) or maintain a waiver or exemption, approved by the CISO and AO or DHS CISO and CIO as appropriate. See Waivers and Exceptions Section 1.10.	CM-2, CM-6
3.1.i	The CISO shall implement DHS information security policies, procedures, and control techniques to address all applicable requirements.	PL-1
3.1.j	The CISO shall develop and manage information security guidance and procedures unique to CBP requirements.	PL-1

Basic IT security responsibilities are provided below.

Basic Requirements Responsibilities
System Owners • Appoint an ISSO for each IT system **CISO** • Structure the CBP Information Security Program to support DHS requirements. • Report all pertinent matters involving the security of IT systems to the AO or a designated representative. • Interpret, tailor, implement, and manage CBP security policies and procedures to meet the Federal, Departmental, and other CBP requirements. • Develop, disseminate, implement, and manage information security guidance and procedures unique to CBP's requirements. **ISSOs** • Account for every CBP computing resource as part of a recognized IT system. • Develop and maintain a System Security Plan for each assigned IT system. • Serve as the POC on all security matters for each assigned IT system.

3.2 Capital Planning and Investment Control

Information security is a business driver and any risks found through security testing are ultimately business risks. Information security personnel should be involved, to the maximum extent possible, in all aspects of the acquisition process, including drafting contracts, and procuring material. Consult the DHS CPIC Guide for more information.

Two critical and complementary processes, Capital Planning and Investment Control (CPIC), and the Systems Engineering Life Cycle (SELC) govern information system management. Senior managers must ensure that information security is adequately addressed throughout all phases of systems engineering and investment lifecycles.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000062

In accordance with the requirements of the Federal Information Security Management Act of 2002 (FISMA), annual Department budgets must address the adequacy and effectiveness of information security policies, procedures, and practices. This implies that security controls must be included in both capital planning and IT procurement actions for the current budget year and for the Future Years Homeland Security Program (FYHSP).

Protecting computer systems, networks, and data is essential to effective management of information resources. Programs that have not met the standards and criteria may be denied funding.

Policy ID	CBP Policy Statements	Relevant Controls
3.2.a	System owners shall include information security requirements in their capital planning and investment control (CPIC) business cases for the current budget year and for the Future Years Homeland Security Program (FYHSP).	SA-1
3.2.b	System owners or the AO shall ensure that information security requirements and POA&Ms are adequately funded, resourced and documented in accordance with current OMB budgetary guidance.	SA-2
3.2.c	The CBP Investment Review Board (IRB) shall not approve any capital investment in which the information security requirements are not adequately defined and funded.	SA-2
3.2.d	The DHS CISO shall perform security reviews for planned information system acquisitions over $2.5 million and additional selected cases.	SA-1
3.2.e	CBP shall ensure that information security requirements as described within this policy document are included in the acquisition of all DHS information systems and services used to enter, process, store, display, or transmit sensitive information.	SA-4
3.2.f	CBP procurement authorities shall ensure that Homeland Security Acquisition Regulation (HSAR) provisions are fully enforced.	SA-1, SA-4
3.2.g	For CBP IT projects, computer security costs must appear in the initial investment management business case and also in subsequent cost benefit analyses throughout the SLC. At a minimum, the system design and functional requirements documents must include computer security requirements.	SA-2 SA-4 SA-5

Capital planning and investment control (CPIC) responsibilities are provided below.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000063

Capital Planning and Investment Control Responsibilities
DHS CIO • Coordinates the review of an independent evaluation of the DHS annual budget submission to ensure that information security requirements are adequately addressed. **CIO/AO** • Coordinate and advocate resources for IA enterprise solutions. • Ensure that funding for implementation of information security is included in project life cycle planning. **CISO** • Ensure that information security requirements are included in the organization's capital planning and investment management planning processes. **System Owners** • Ensure that funding for implementation of information security is included in project life cycle planning.

Two critical and complementary processes govern the management of IT within the CBP: Investment Management Planning (IMP) and System Life Cycle (SLC). A typical CPIC process is discussed in this section. SLC processes and responsibilities are described in Section 3.6 below.

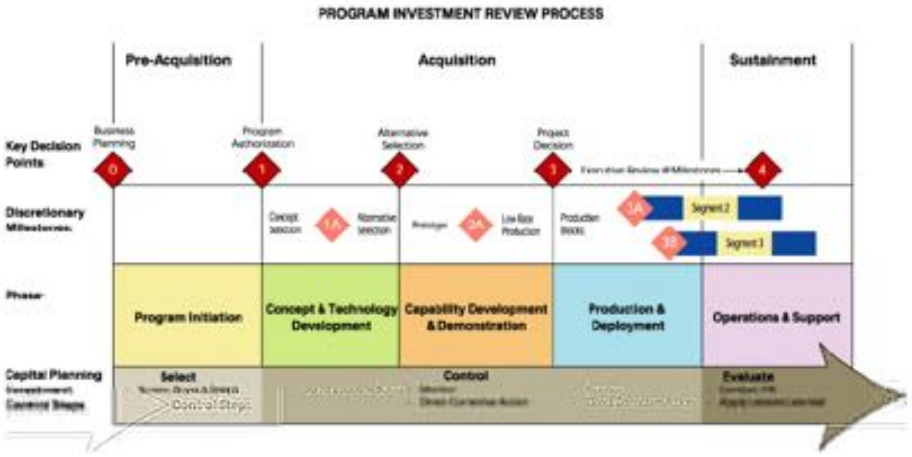
The protection of computer systems, networks, and data is essential to the effective management of IT resources. CBP security professionals thus play a key role in implementing both of these management processes. Senior managers must ensure that security considerations are adequately addressed in all aspects of CBP IT activities. This is accomplished by requiring all projects and programs to demonstrate through the SLC documentation that they have met all appropriate security standards and criteria at specific points in their development and investment lifecycles as defined by the CPIC process. Programs that have not met the standards and criteria can be denied funding.

Capital Planning and Investment Control Process

DHS investment management is governed by DHS Management Directive 1400, *Investment Review Process*. This directive requires that all IT investments be reviewed by the DHS Enterprise Architecture board at each of 4 Key Decision Points (KDPs), Program Authorization, Alternative Selection, Project Decision, and Executive Review. Figure 3.2 shows how these KDPs are related to the CPIC phases and the SLC phases.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000064

Figure 3.2: Program Investment Review Process



Program Authorization: At this KDP, programs are responsible for demonstrating the results of operational analysis and identification of program requirements developed to define the new capability required to satisfy a mission. With approval at KDP1, the initiative is (1) designated as a Level 1 acquisition, (2) directed to charter a major acquisition Integrated Product Team (IPT), (3) authorized to commence the Concept & Technology Development phase, and (4) entered into the budget process. Typically, the initiative will enter the Fiscal Year (FY) +2 budget to provide staff and funding to proceed.

Alternative Selection: At this KDP, the program is evaluated on the feasibility of the alternative solution it has selected. The program will present its evaluation of the feasibility of alternatives and provide a basis for assessing the relative merits of alternatives (e.g., advantages and disadvantages, degree of risk, life cycle cost, and cost benefit). Promising alternative solutions are defined in terms of cost, schedule, and performance objectives; identification of interoperability, supportability, and infrastructure requirements; opportunities for tradeoffs; an overall acquisition strategy; and a test and evaluation strategy (including Development Test and Evaluation [DT&E], and Operational Test and Evaluation [OT&E]).

The Program Manager will submit an updated Exhibit 300 containing or based on items identified above. This information and associated presentations are used to monitor initiatives, direct corrective actions, and determine when the investment is ready to proceed to the next phase.

Project Decision: At this KDP, the review is focused on the feasibility of the preferred alternative and refining the solution prior to a full production commitment.

In preparation for KDP 3, the Program Manager will review and update documents prepared during previous phases and develop: (1) proposed Exit Criteria for the Production and Deployment Phase. The Program Manager will submit an updated Exhibit 300. This information and associated presentations are used to monitor initiatives, manage risks, and determine when the investment is ready to proceed to the next phase.

With approval at KDP 3, the investment is authorized to commence the Production and Deployment Phase, and the future year's program plan must be fully funded.

Executive Review: At KDP 4, a project is reviewed against its performance and costs goals. The results of this review will form the basis for decisions on whether the project should be enhanced, reengineered, or retired.

At each of these KDPs, the security function has a formal role as a specialty reviewer, advising the EAB on whether the project should be allowed to proceed based on how well security is addressed at each lifecycle phase.

3.2.1 Investment Management Process

The information security program of CBP is funded primarily through budget requests for individual systems and applications. To that end, key portions of each program and/or system's OMB Exhibit 300 (Section II.B) reflect both specific and general information security considerations. The formal CBP System Life Cycle (SLC) and the Investment Management Process (IMP) facilitate the development of the OMB Exhibit 300 submission.

During the SLC, security requirements are identified based on the appropriate security inputs from key project personnel (primarily the System Owner, the ISSO and the assigned Certification Agents (CAs), with review and approval from the CISO). These are provided to program managers who are responsible for drafting the budgetary requests. These inputs include both specific security requirements such as particular software and hardware required to mitigate a distinct risk or set of risks, as well as ongoing operational requirements such as staffing of security operations and incident response capabilities.

Additionally, under FISMA, the ongoing select, control, evaluate management model interacts with the continuing security assessment program as reflected in the annual completion of security self-assessments (NIST SP 800-53) for every MA or GSS.

Security deficiencies identified in annual self-assessments, periodic risk assessments, and independent audit reviews are incorporated into the Plan of Action and Milestones (POA&Ms), which then provides input to the next budget request. It is, therefore, imperative for IT security requirements to be identified and adequately defined or otherwise documented for each SLC stage of development (especially ongoing operations) to ensure program funding and to meet the requirements of OMB budgetary reporting processes.

Further detail on this methodology can be found in the CBP Investment Management Process as well as NIST SP 800-65.

Figure 3.2.1 – CBP Program Funding Process provides a high-level view of how security requirements identified through projects/programs and the SLC process are submitted as input to the agency budget request. Agency executive management prioritizes security requests/requirements before the budget request is submitted to OMB.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000066

Figure 3.2.1: CBP Program Funding Process

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000067

3.3 Contractors and Outsourced Operations

Computer security requirements must be incorporated in contractual documents involving the acquisition, development, and/or operations and maintenance of computer resources. This applies at the beginning of a project or acquisition and in all follow-on contracts or purchasing agreements involving the acquisition of computer resources. This includes hardware, software, maintenance, and other associated IT products and services.

Contractors fill a vital role in the daily operations of CBP. They have a responsibility to protect the information they possess and process. To ensure the security of the information in their charge, contractors must adhere to the same rules and regulations as Government employees.

Policy ID	CBP Policy Statements	Relevant Controls
3.3.a	All statements of work and contract vehicles shall identify and document the specific security requirements for IT services and operations required of the contractor.	SA-4
3.3.b	Contractor IT services and operations shall adhere to all applicable CBP and DHS information security policies.	SA-9
3.3.c	Requirements shall address how sensitive information is to be handled and protected at the contractor's site, including any information stored, processed, or transmitted using the contractor's computer systems, the background investigation and/or clearances required, and the facility security required.	SA-9
3.3.d	Statements of work and contracts shall require that at the end of the contract, the contractor must return all information and IT resources provided during the life of the contract and must certify that all CBP information has been purged from any contractor-owned system used to process CBP information.	SA-4
3.3.e	The Security and Technology Policy Branch shall conduct reviews to ensure that the information security requirements are included within the contract language and are implemented and enforced.	SA-1
3.3.f	Security deficiencies in any outsourced operation shall require creation of a program-level POA&M.	SA-9
3.3.g	CBP Procurement authorities shall ensure that HSAR provisions are fully enforced.	SA-1, SA-4
3.3.h	All companies providing services to CBP are required to comply with the CBP *Information Systems Security Policies and Procedures Handbook*.	SA-9
3.3.i	All support staff must be trained in basic network, hardware, and security principles of CBP.	PS-2
3.3.j	All CBP employees and contractors must be U.S. citizens and have a favorably	PS-3

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000068

Policy ID	CBP Policy Statements	Relevant Controls
	adjudicated Background Investigation (BI) completed.	

Responsibilities for contractors and outsourced operations are provided below.

Contractors and Outsourced Operations Responsibilities

CISO

- Establish and maintain a contractor and outsourced operations policy for CBP.

System Owners/IT Project Managers

- Ensure that computer security requirements are reviewed and included in all applicable statements of work and other contractual agreements throughout the System Life Cycle.
- Ensure that basic security requirements are integrated into the software and procurement life cycle for project development.
- Ensure that computer security requirements are specified in the system design and functional requirements documents, and other SLC documents, as required.

ISSOs

- Coordinate with the system owners to ensure that contractor and outsourced operations policy requirements are met.

System owners and IT Project Managers must review and include computer security requirements in the Solicitation document *prior to the acquisition of IT assets or services*. Information security must be a key factor in the source selection process and weighted commensurate with the sensitivity and criticality of the data to be processed. The Statement of Work (SOW) for all contracts (both initial and follow-on) must address computer security requirements. If the solicitation includes the purchase of a commercial off-the-shelf (COTS) application or if the system being developed has a COTS component, the security aspects of the COTS product must be analyzed and, if appropriate, must identify and include security requirements in the acquisition specifications.

Computer security costs must appear in the initial investment management business case and also in subsequent cost benefit analyses throughout the SLC. At a minimum, the system design and functional requirements documents must include computer security requirements.

Program Office information technology acquisition plans and solicitation documents (e.g. Requests for Proposal, Statement of Work, etc) must include at a minimum a description of the following information security requirements:

1. Requirements to Certify and Accredit the system in accordance with CBP and DHS policy.

2. Vendor documentation must detail all functional security controls in the system (what they are, how they operate, how to set configurations, etc) such that they can be analyzed and tested. Security configurations and implementation guidance must be consistent with NIST SP 800-70, Security Configuration Checklists Program for IT Products: Guidance for Checklists Users and Developers.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000069

3. Deliver sufficient system documentation for users and administrators that describes design and functional properties of the security controls and how to enable or set system security features and operate security features.

4. All statements of work and contract vehicles must identify and document the specific security requirements for IT services and operations that are required of the contractor. At a minimum, such security requirements must be consistent with Federal and Departmental security policies and processes.

Each Program Office must define and document acquisition plans and procedures to acquire or procure IT systems and services. These plans must meet Federal Acquisition Regulations (FAR), in particular, those requirements identified in sub-sections 7.1 and 39.00 for acquisition of information systems and the Department of Homeland Security Acquisition Regulation (HSAR), June 2006. Additionally, acquisition of commercial products must be consistent with NIST SP 800-23, *Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products.*

3.3.1 Non-Disclosure Agreements

All active Contractor Officer's Technical Representatives (COTRs) must have signed Non-Disclosure Agreements on file for all contractors that access the information systems. All contractor employees must be made aware of the need to protect sensitive DHS and CBP information/information systems.

All OIT COTRs for active contracts are required to:

1. Obtain a signed Non-Disclosure Agreement (NDA) from all current contractors. All contractor employees are required to have a signed NDA on file with the COTR.

2. Form DHS 11000-6, Non-Disclosure Agreement must be used and the COTR shall maintain these signed forms in the COTR contract file.

3. SOWs must include language that requires a signed NDA from each of the contractor's employees working under the contract in all future SOW's.

   Example of language: "Upon award, the contractor shall provide to the COTR a signed DHS 11000-6 Standard Non-Disclosure Agreement Form for each employee working under the contract. The contractor shall also provide this signed form each time a new employee is assigned to the contract."

4. The NDA should only apply to moderate and high level risk contractor positions. It is assumed that any contractor who accesses the CBP information system is, at minimum, a moderate risk.

3.4 Performance Measures and Metrics

CBP is participating in the DHS initiated balanced scorecard security performance measures.

Information security performance measurement is basic to CBP structure and mission. Implementing and maintaining an information security measures program enhances compliance

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000070

with good management guidelines for performance improvement. Within CBP, measures determine whether a program meets or fails to meet security objectives. Performance measures evaluate critical success factors within an application or system, such as those discussed in the Federal Enterprise Architecture Performance Reference Model. In an application that reports on financial data or uses financial data, a metric for security might include frequency of access or method used to validate totals or data integrity of totals. For a network application, measuring the level and frequency of improper login attempts might be of concern.

NIST SP 800-55, Security Metrics Guide for Information Technology Systems, Revision 1, July 2008, provides guidance on how an organization, through the use of metrics, can identify the adequacy of in-place security controls, policies, and procedures. NIST 800-55 describes an approach to assist management in determining where to invest resources in additional security protection or where to discontinue nonproductive controls. It explains a process to develop and implement metrics and how these metrics can be used to justify security control expenditures.

A security metrics program within an organization should be built with four interdependent components:

1. Strong upper-level management support;
2. Practical security policies and procedures;
3. Quantifiable performance metrics, and
4. Results-oriented metrics analysis.

Information security performance goals and objectives must be the basis for the security metrics that are established. Information security metrics monitor the success of these goals and objectives by quantifying the level of compliance of the security controls. NIST SP 800-55 provides examples of metrics.

When implementing an information security metrics program, the metrics must yield information that can be quantified for comparison purposes, in order to track progress using the same points of reference. Percentages or averages are common, and absolute numbers may be useful, depending on the activity being measured. Data required for calculating metrics must be easily obtainable, and the process that is under consideration must be measurable. To be measurable, a repeatable process is required. Only processes that are performed in a relatively formal manner should be considered for measurement. Metrics data must be easily obtainable to ensure that the cost of data collection does not exceed the benefits derived from the collection and assessment process.

Policy ID	CBP Policy Statements	Relevant Controls
3.4.a	Define performance measures to evaluate the effectiveness of CBP's information security program.	---

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000071

Policy ID	CBP Policy Statements	Relevant Controls
3.4.b	CBP shall provide OMB FISMA data at least monthly to the DHS Compliance Officer.	---
3.4.c	CBP shall utilize the automated tool directed for use by the DHS CISO for Performance Plan reporting	---

Performance measures and metrics responsibilities within CBP are provided below.

Performance Measures and Metrics Responsibilities
DHS CISO • Establishes an IT security metrics program for DHS. **CISO** • Define performance metrics to evaluate the effectiveness of the IT security program. • Provide semiannual data on CBP's progress in meeting DHS's performance measures to the DHS CISO. **ISSOs** • Provide input to the identification and selection of specific performance metrics for their systems. • Identify sources of metrics data and assign personnel to gather chosen data. • Monitor metrics data collection and integrate/analyze data for reporting purposes. • Provide performance metrics information to the CISO as required.

3.5 Continuity Planning for Critical CBP Assets

The Continuity Planning for Critical DHS Assets Program is vital to the success of the DHS Information Security Program and consists of two integrated elements:

1. Continuity of Operations (COOP) Planning
2. IT Contingency Planning (CP)

The COOP planning element requires CBP to develop, test, exercise, and maintain comprehensive plans so that essential CBP business functions can be continued following an emergency situation. COOP plans are business oriented and focus on sustaining an organization's essential functions at an alternate site until the primary site can be restored.

All CBP organizations and sites are responsible for developing, annual testing, and maintaining COOPs for their area of responsibility. Each organization must train personnel in COOP procedures specific to their areas of responsibility. Certain organizations will have specific pre-crisis monitoring responsibilities for the maintenance and execution of their COOP functions. For example, the Disaster Recovery Operations Center, Program Operations Division (POD) develops and maintains COOPs for the Office of Information and Technology (OIT). The CISO reviews plans to ensure that the COOP meets security requirements.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000072

The principal objectives of the COOP plan are to focus on CBP's ability to continue mission-essential functions without unacceptable interruption. These objectives are:

1. Overcome a crisis that renders a CBP location unusable by deploying pre-selected personnel to a safe alternate facility.
2. Ensure the ability to maintain or reestablish CBP control and direction at the affected site.
3. Prepare alternative courses of action to minimize or mitigate the effects of the crisis and shorten CBP crisis response times.
4. Identify critical duty functions that must continue during the first two days of a crisis.
5. Assess damages and losses and identify remaining resources.
6. Allocate surviving resources, in priority order, to resolve the crisis and perform critical functions.
7. As required, reconstitute key staff positions with successor personnel.
8. As required, regenerate full functions and resume normal operations.

The IT Contingency Planning element is designed to sustain and recover critical IT services following an emergency. IT contingency plans focus on sustaining the critical IT applications and general support systems needed to support essential operations. The thrust of IT contingency planning is to assure the continuous availability of critical IT systems, protect IT assets and vital records, mitigate disruptions to operations, provide maximum safety to personnel, minimize damage to assets, and achieve a timely and orderly recovery from a disruption to operations.

Good contingency plans address the possibility of catastrophic loss, but also address those less-than-cataclysmic events that can seriously impede normal operations. IT contingency planning includes emergency response, backup operations, and post disaster recovery operations. Small problems disrupt IT operations with a far higher frequency than do major disasters. The size or scope of a catastrophe and its impact on operations are often not proportional. In the absence of a good plan, minor damage can cause major problems. Conversely, with a good plan, even a major catastrophe may not result in serious losses.

The term "contingency planning" is often used interchangeably with disaster recovery, business continuity, continuity of operations, or business resumption planning. A disaster recovery plan for the CBP National Data Center incorporates many of the COOP plans developed by and pertinent to all CBP offices and systems, including Major Applications (MAs) or General Support Systems (GSSs).

3.5.1 Continuity of Operations Planning

DHS must have the capability to ensure continuity of essential functions under all circumstances. In support of DHS Strategic Goals, COOP planning policies are designed to support the DHS-

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000073

wide capability to react to emergency events **(response)**; restore essential business functions if a disruption occurs **(recovery)**; and achieve a resumption of normal operations **(reconstitution)**.

COOP planning focuses on sustaining an organization's essential business functions at an alternate site until the primary site can be restored. This requires that CBP develop, test, exercise, and maintain comprehensive plans to ensure that essential CBP business functions can be continued off site following an emergency. These plans address three essential phases:

1. Activation and Relocation (0-12 hours)
2. Alternate Facility Operations (12 hours to Termination)
3. Reconstitution (Termination to Return to Normal Operations)

Policy ID	CBP Policy Statements	Relevant Controls
3.5.1.a	When available, a DHS-wide process for continuity planning shall be used in order to ensure continuity of operations under all circumstances.	CP-2
3.5.1.b	Develop, test, implement, and maintain comprehensive COOP plans to ensure the continuity and recovery of essential CBP functionality.	CP-2, CP-4
3.5.1.c	All COOP plans shall be tested and exercised annually.	CP-4
3.5.1.d	All CFO designated systems requiring high availability shall be identified in COOP plans and exercises.	CP-1
3.5.1.e	All personnel involved in COOP efforts shall be identified and trained in the procedures and logistics of COOP development and implementation.	AT-3, CP-3
3.5.1.f	To ensure that accounts can be created in the absence of the usual account approval authority, CBP systems that are part of the Critical DHS Assets Program shall have provisions to allow the CISO or CIO to approve new user accounts as part of a COOP scenario.	AC-2
3.5.1.g	CBP shall compile and maintain a list of mission-critical information systems in support of COOP.	CM-8, CP-1
3.5.1.h	CISO shall ensure preparation and maintenance of plans and procedures to provide continuity of operations for information systems.	CP-1
3.5.1.i	CBP information systems that are part of the DHS Continuity Planning for Critical DHS Assets Program will be provided requirements for system-level contingency planning by a CBP Continuity Office or by a DHS Contingency Planning Program Office.	---

General COOP planning responsibilities are shown below. Specific COOP responsibilities for CBP are detailed in the DHS Headquarters Continuity of Operations Plan.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000074

Continuity of Operations Planning Responsibilities
DHS Continuity Planning Program Director • Administers the Continuity Planning for Critical DHS Assets Program. Develops, maintains, and promulgates requirements. • Provides oversight and ensures program compliance across DHS Components. • Provides COOP planning guidelines to the Components. • Facilitates the development and testing of COOP plans. • Approves DHS COOP plans and maintains COOP status. **CISO** • Identify and align office functions with DHS essential functions. • Identify vital records, IT, and personnel requirements needed to recover office functions. • Administer the CBP Continuity Planning program. • Ensure the development of the COOP plans. Ensure that COOP planning is implemented for each line of business. • Provide COOP status and strategy to the DHS Continuity Planning Program Director. • Develop and maintain a COOP Multi-Year Strategy and Program Plan. **ISSOs** • Comply with the CBP Continuity Planning program. • Perform continuity planning and testing and document results. • Assist in the development of the COOP Multi-Year Strategy and Program Plan. • Ensure operational security is maintained during any test or recovery activities.

3.5.1.1 Continuity of Operations Planning Requirement

COOP planning is required by Presidential Decision Directive 67. CBP is required to develop, test, exercise, and maintain Continuity of Operations (COOP) plans for the recovery of essential business functions identified in the DHS Headquarters COOP Plan. COOP plans are business oriented and thus focus on sustaining the essential functions of the organization (usually a headquarters element) and the supporting business functions (including those identified as national critical) at an alternate site and performing those functions for up to 30 days before returning to normal operations.

3.5.1.2 Continuity of Operations Planning Objectives

COOP planning is designed to achieve the following objectives:

1. Ensure the continuous performance of CBP essential functions/operations during an emergency
2. Protect equipment, vital records, and other assets to meet mission needs
3. Reduce or mitigate disruptions to operations

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000075

4. Reduce loss of life, minimizing damage and losses

5. Achieve a timely and orderly recovery from an emergency and resumption of full service to customers.

3.5.1.3 Continuity of Operations Plan Content

To facilitate their usefulness and acceptance by the users, COOP plans need to be brief and concise. COOP plans must encompass the following elements:

1. Essential functions (including IT requirements, vital records and databases, and functional recovery activities)

2. Essential personnel

3. Alternate operating facilities

4. Interoperable communications

5. Human capital issues (inclusion of occupant emergency planning)

6. Devolution of control (delegations of authority and orders of succession)

7. Reconstitution (return to normal operations).

Because Continuity of Operations emphasizes the recovery of an organization's operational capability at an alternate site, the COOP plan will not necessarily address IT operations. COOP plans normally focus on facility-level and organization contingency planning rather than IT contingency planning. IT requirements are considered in the COOP plan in terms of their support of essential functions and the supporting office functions and should be documented in the COOP Plan. Although IT contingency planning is a separate effort (see Section 3.5.2), these plans can be included in the COOP Plan as appendices. Close coordination with IT support operations is required to ensure IT availability at the alternate site(s).

3.5.1.4 Continuity of Operations Test, Training, and Exercise

The most important aspect of successful Continuity of Operations planning is the periodic testing and exercising of the COOP plan. To demonstrate a viable continuity of operations capability, COOP plans must be periodically tested and exercised, and COOP personnel must be trained. Tests and exercises serve to validate specific aspects of COOP plans, policies, procedures, systems, and facilities that would be used during an emergency event. CBP shall conduct periodic Test, Training, and Exercises (TT&Es), so that weaknesses in the COOP Plan can be identified and corrected. TT&E results must be documented.

3.5.2 IT Contingency Planning

IT contingency planning is an integral part of the Department of Homeland Security (DHS) Continuity Planning for Critical DHS Assets Program. Consequently, this policy supplements Continuity of Operations (COOP) Planning policy.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000076

IT contingency planning is designed to ensure the availability of critical IT support under all circumstances. CBP shall develop, test, and maintain IT Contingency Plans to ensure adequate IT is available to sustain CBP essential and supporting office functions in accordance with the requirements for the FIPS 199 potential impact level for the availability security objective. See Section 3.9.1, *FIPS 199 Categorization and the NIST SP 800-53 Controls*, for more information on DHS's approach to system categorization.

In support of DHS strategic goals, IT contingency planning is designed to establish a DHS-wide capability to react to emergency events **(response)**, restore essential business functions if a disruption occurs **(recovery)**, and achieve a resumption of normal operations **(reconstitution)**.

Policy ID	CBP Policy Statements	Relevant Controls
3.5.2.a	Guidance, direction, and authority for IT contingency planning activities for DHS Components are centralized in the DHS Office of the CIO.	CP-1
3.5.2.b	To ensure critical IT system availability under all circumstances, a standard DHS-wide process for IT contingency planning shall be developed, documented, and maintained. CBP shall provide IT contingency planning status and strategy to the DHS Continuity Planning Program Director.	CP-1, CP-2
3.5.2.c	Implement and enforce backup procedures for all sensitive IT systems, data, and information. Recommended intervals are daily for incremental data backups and weekly for full data backups. System and application software should be backed up whenever modifications to the software make backups necessary.	CP-9
3.5.2.d	The rigor of the IT system contingency planning, training, testing and capabilities shall be commensurate with the **availability** security objective. The minimum contingency capabilities for each impact level follow: **High** – System functions and information have a high priority for recovery after a short period of loss. **Moderate** – System functions and information have a moderate priority for recovery after a moderate period of loss. **Low** – System functions and information have a low priority for recovery after prolonged loss.	CP-1
3.5.2.e	Comprehensive IT Contingency Plans to continue and recover critical CBP major applications and general support systems shall be developed, tested, exercised, and maintained by CBP in accordance with the requirements for the FIPS 199 potential impact level for the **availability** security objective. These plans shall be based on three essential phases: Activation/Notification, Recovery, and Reconstitution. Components shall review the contingency plan for the information system at least annually and revise the plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.	CP-1, CP-5
3.5.2.f	IT Contingency Plans shall be tested in accordance with the **availability** security objective. The minimum contingency testing for each impact level	CP-4,

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000077

Policy ID	CBP Policy Statements	Relevant Controls
	follows: **High** – System recovery roles, responsibilities, procedures, and logistics in the CP shall be used to recover from a simulated contingency event at the alternate processing site within a year prior to accreditation. The system recovery procedures in the CP shall be used to simulate system recovery in a test facility at least annually. **Moderate** – The system recovery roles, responsibilities, and procedures in the CP shall be used to simulate system recovery in a test facility within a year prior to accreditation. System personnel shall review recovery procedures annually. **Low** – CP contact information shall be verified at least annually.	CP-7
3.5.2.g	All personnel involved in IT contingency planning efforts shall be identified and trained in the procedures and logistics of IT contingency planning and implementation in accordance with the **availability** security objective. The minimum contingency planning for each impact level follows: **High** – All personnel involved in contingency planning efforts shall be identified and trained in their contingency planning and implementation roles, responsibilities, procedures, and logistics. This training shall incorporate simulated events. Refresher training shall be provided at least annually. **Moderate** – All system personnel involved in contingency planning efforts shall be trained. Refresher training shall be provided at least annually. **Low** – There is no training requirement.	CP-3
3.5.2.h	CP testing and/or exercises with COOP related plans for systems with moderate and high availability FIPS-199 categorization shall be coordinated with other DHS components.	CP-4

IT contingency planning responsibilities are provided below.

IT Contingency Planning Responsibilities
DHS Continuity Planning Program Director • Administers the Continuity Planning for Critical DHS Assets Program. Develops, maintains, and promulgates program requirements. • Provides oversight and ensures program compliance across DHS Components. • Provides IT contingency planning guidelines to Component CISO/ISSMs • Facilitates the development and testing of IT Contingency Plans. • Approves DHS IT Contingency Plans and maintains status. **System/Network Administrators** • Participate in all phases of the IT contingency planning process. **Site Managers/System Owners** • Ensure that the system's FIPS 199 potential impact for the availability security objective is correct and maintained to be consistent with system information processing changes. • Ensure that adequate resources are budgeted for IT contingency planning, testing, and

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000078

IT Contingency Planning Responsibilities
training consistent with the availability objective of the system. • Ensure that adequate Contingency Plans are included in C&A documentation. **CISO** • Establish a CBP continuity planning program. • Provide IT contingency planning status and strategy to the CBP Continuity Planning Program Director. **ISSOs** • Comply with the CBP continuity planning program. • Ensure that the system's FIPS 199 potential impact for the availability security objective is consistent with the information types processed, stored, and transmitted by the system. • Ensure comprehensive IT Contingency Plans are developed, as required, for each major application and general support system under their purview. • Perform IT contingency planning, testing/exercising, and training, as required. For systems with moderate and high potential impact for availability, testing/exercising and training shall occur at least annually and when significant changes are made to the IT application or system, supported essential and office function(s), or the IT contingency plan. Examples of significant changes to information systems include installation of a new or upgraded operating system, middleware component, or application; modifications to system ports, protocols, or services; installation of a new or upgraded hardware platform or firmware component; or modifications to cryptographic modules or services. • Ensure operational security is maintained during any test or recovery activities.

IT contingency planning represents a broad scope of activities designed to sustain and recover critical IT services following an emergency and includes identification of procedures and capabilities for recovering major applications and general support systems.

IT contingency plans are IT oriented and therefore focus on sustaining an organization's critical IT services provided by the major applications and general support systems that sustain essential and supporting office functions.

3.5.2.1 IT Contingency Planning Requirement

IT contingency planning is directed by (1) NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*, (2) Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*, Appendix III, and (3) NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*.

Appendix III requires the development and maintenance of continuity of support plans for general support systems and IT Contingency Plans for major applications. NIST SP 800-34 considers continuity of support planning to be synonymous with IT contingency planning. Because an IT Contingency Plan should be developed for each major application and general support system, multiple Contingency Plans may be maintained within the organization's Continuity of Operations (COOP) Plan or Business Continuity Plan.

NIST SP 800-53 defines a family of security controls for contingency planning (CP). It identifies the level that these controls should be developed for high, moderate, and low potential

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000079

impact systems. DHS uses the FIPS 199 designation of the availability security objective to define the impact level applicable to contingency planning controls (see Section 3.9.1 for information on DHS guidance on FIPS 199 system categorization and implementation of the NIST SP 800-53 security controls).

3.5.2.2 IT Contingency Plan Development

IT contingency planning is designed to achieve the following objectives:

1. Ensure the continuous availability of the critical IT systems that support CBP essential functions during an emergency
2. Protect IT assets and vital records needed to support mission needs
3. Reduce or mitigate disruptions to operations
4. Reduce loss of life, minimizing damage and losses
5. Achieve a timely and orderly recovery from an emergency and the resumption of full IT service to customers.

3.5.2.3 IT Contingency Plan Format and Content

To facilitate their usefulness and acceptance by the users, IT contingency plans need to be brief and concise. The specific control requirements and level of effort are determined based on the IT system's security categorization. The level of resources for the contingency plan is based on the security categorization for the availability security objective. See Section 3.9.6, *Contingency Plan*, or see Appendix K for more information on the Contingency Plan template requirements.

IT contingency plans must encompass the following elements as required for the potential impact level for the system's availability security objective:

1. Disruption impacts and allowable outage times
2. Preventive controls and recovery strategies
3. Vital records
4. Responsible personnel
5. Alternate operating facilities
6. Devolution of control (delegations of authority and orders of succession)
7. Reconstitution (return to normal operations)

3.5.2.4 IT Contingency Plan Test and Exercise

Testing the IT contingency plan identifies planning gaps. Tests and exercises serve to validate specific aspects of IT contingency plans, policies, procedures, systems, and facilities to be used

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000080

during an emergency. Both activities improve plan effectiveness and overall Department preparedness.

Contingency Plan testing requirements for systems at each impact level for availability are described in Section 3.9.8.

3.5.2.5 IT Contingency Plan Training

Training prepares recovery personnel for plan activation and improves plan effectiveness for overall Department preparedness. The IT system personnel shall be trained on the IT contingency plan according to the potential impact level of the availability security objective.

1. High impact for availability – All personnel involved in IT contingency planning efforts shall be identified and trained in the procedures and logistics of IT contingency planning and implementation, as well as their roles and responsibilities in relation to contingencies. This training shall incorporate simulated events. Refresher training shall be provided

2. Moderate impact for availability – All system personnel involved in IT contingency planning efforts shall also be trained. Refresher training shall also be provided.

3. Low impact for availability – System personnel are not required to be trained.

3.6 System Life Cycle

The System Life Cycle (SLC) methodology provides a structured approach to managing IT projects. It also allows introduction of IT security planning, including budgeting, review, and oversight.

CBP follows a formal SLC to support its mission. The Systems Life Cycle Handbook (b)(7)(E) (b)(7)(E) is a component of official CBP policy. The SLC includes life cycle processes, and documentation requirements for various stages of the SLC. The SLC describes a project leader's responsibilities for all aspects of systems development including Project Planning and Management, Risk Management, Quality Assurance, Requirements Management, IT Security, Contract Management, and Configuration Management. Information security must become an integral part of all phases of system development, even as early as the project concept and business case stage. Proper adherence to this process is interrelated to the Investment Management Process and funding of the project/program.

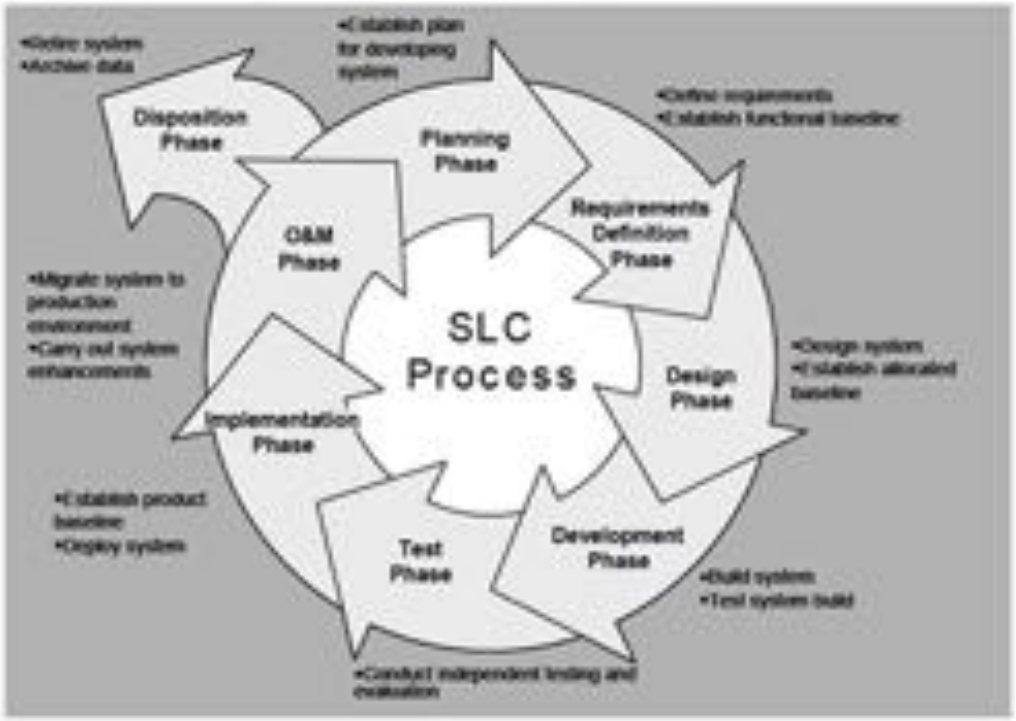
As part of the SLC for all CBP systems, each Major Application (MA) or General Support System (GSS) (e.g., mainframe, client-server, networks) developed or operating at any CBP location is required to produce security documentation as part of Certification and Accreditation (C&A).

The SLC process begins when the Program Authorization decision (discussed in Section 3.2) within the CPIC process that determines an IT project should be initiated.

There are eight distinct phases in the SLC as depicted in figure 3.6 below:

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000081

Figure 3.6: System Life Cycle Process



Policy ID	CBP Policy Statements	Relevant Controls
3.6.a	Ensure that system security is integrated into all phases of the SLC.	SA-3
3.6.b	Ensure that security requirements for sensitive IT systems are incorporated into system life-cycle documentation.	SA-3
3.6.c	All custom developed code shall be reviewed, approved and signed by the Program Manager prior to deployment into production environments. The Program Manager may delegate this authority to another CBP employee in writing. This authority shall not be delegated to contractor personnel.	RA-5

SLC responsibilities are provided below:

SLC Responsibilities
DHS CIO • Defines and promulgates the DHS SLC process. • Ensures that information security life cycle planning is integrated into DHS capital planning and investment control process. **DHS CISO** • Ensures that information security requirements are included in the DHS SLC. • Oversees proper implementation of security controls in system development.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000082

SLC Responsibilities
CISO • Establish procedures for reviewing compliance with SLC documentation requirements. • Participate in capital planning and investment management meetings involving SLC considerations for IT systems and networks. • Ensure that required information security documentation is produced and reviewed in accordance with SLC milestones. • Approve IT security documentation produced as part of the SLC process (except the C&A package). **ISSOs** • Participate in planning and executing the SLC process. • Provide information security expertise to system development project teams. • Review and comment on all SLC security documents. **System Owners/IT Project Managers** • Ensure required security documents and reviews are included in the SLC. • Ensure that adequate funding is available for implementation of security requirements. • Prepare required security documents.

3.6.1 Planning

The Planning Phase defines the system concept from the user's perspective and establishes a comprehensive plan for developing the system. Information security activities include the following:

1. Preparation of the initial risk assessment and security plan.
2. Ensuring that adequate budgetary resources for information security requirements are available.

3.6.2 Requirements Definition

During the Requirements Definition Phase, users and technical staff define detailed requirements to ensure that the system will meet user requirements. This results in the establishment of a Functional Baseline. Information security activities include:

1. Updating the risk assessment and security plan
2. Reviewing IT Baseline Security Requirements (See Attachment A)
3. Developing an initial Plan of Action and Milestones (POA&Ms)
4. Developing an initial Security Test and Evaluation (ST&E) Plan
5. Reviewing information security budget requirements

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000083

6. Preparing the initial security inputs to the IT Training Plan
7. Preparing the initial contingency plan.

3.6.3 Design

The system development then moves to the Design Phase, during which the requirements are transformed into detailed design specifications. During the Design Phase, an Allocated Baseline is established and documented in the System Design Document. Information security activities include the following:

1. Updating the risk assessment and security plan
2. Reviewing budget requirements
3. Developing Interconnection Security Agreements
4. Updating the security information in the IT Training Plan
5. Updating the contingency plan
6. Preparing the initial Certification and Accreditation (C&A) package.

3.6.4 Development

After formal approval of the design, the IT project enters the Development Phase. During this phase, the development team builds the system according to the design specified during the Design Phase and conducts development testing. The Development Phase represents an iterative process during which the development team builds the system, tests the system build, modifies the system based on any problems identified during Development Testing, and then tests the modified system build. Information security activities include the following:

1. Conducting the initial developmental Security Test and Evaluation (ST&E)
2. Updating the risk assessment and security plan
3. Developing the initial operational ST&E
4. Reviewing budget requirements
5. Updating the C&A package.

3.6.5 Test

When the developed system is fully functional and has successfully passed Development Testing, the system development project moves into the Test Phase. During this phase, Independent Testing and Evaluation is conducted to ensure that the developed system functions properly, satisfies the requirements (including security requirements) developed in the

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000084

Requirements Definition Phase, and performs adequately in the host environment. Information security activities include:

1. Conducting formal developmental ST&E
2. Reviewing budget requirements
3. Updating the risk assessment and security plan
4. Updating the C&A package.

3.6.6 Implementation

The system development project enters the Implementation Phase after the system has successfully passed testing and is ready for deployment. The output of this phase is the Product Baseline, which consists of the production system, databases, an updated data dictionary, associated infrastructure, and supporting documentation. During this phase the system is deployed to designated production sites. Information security activities include the following:

1. Conducting the operational ST&E on upgraded or new systems
2. Reviewing adequacy of budget requirements
3. Finalizing the security inputs in the IT Training Plans
4. Updating the risk assessment and security plan
5. Finalizing the Certification and Accreditation (C&A) package.

3.6.7 Operations and Maintenance

After the system has been successfully deployed, it enters the Operations and Maintenance (O&M) Phase. During this phase, the system becomes operational and any necessary system modifications are identified and documented as "System Change Requests." These changes must be formally approved before they can be implemented. Information security activities include the following:

1. Reviewing C&A status and maintaining the currency of the C&A documentation
2. Conducting annual user security awareness training and role-based training (e.g., training for ISSOs, AO, network and system administrators, managers)
3. Maintaining adequate budgetary resources.

3.6.8 Disposition

Finally, the system is retired from the operational environment during the Disposition Phase. Activities during this phase involve:

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000085

1. Terminating system operations
2. Removing the system from the production environment
3. Archiving the system components, data, and documentation
4. Disposing of equipment and media in accordance with security requirements.

3.7 Configuration Management

Configuration management (CM) relates to managing the configuration of all hardware and software elements within IT systems and networks. CM within DHS consists of a multi-layered structure – policy, procedures, processes, and compliance monitoring. CBP shall utilize appropriate levels of configuration management.

CM is vital in controlling and managing security of IT systems and, through change control, can reduce risk from unwanted or unmanaged change. Precise understanding of system components and configurations is very important; change must be accomplished through formal change control procedures.

Routine business actions or events can have a significant impact on security. Examples include the following:

1. A change in mission may change security requirements.
2. A change in an application may require a different security mode of operation.
3. Connection to any new external interface affects system security.
4. Changes in the operational environment (relocation, changes in external operational procedures) could impact security controls.
5. Security patches for newly identified vulnerabilities must be applied in a timely manner.

The CM program must be applied properly to protect security mechanisms and to ensure they are not compromised or rendered ineffective. The Office of Information Technology (OIT) configuration management program is an important component of our security program. CM will apply to all systems, subsystems, and components of the CBP enterprise, thereby ensuing implementation, and continuing life-cycle maintenance. CM begins with base lining of requirements documentation and ends with decommissioning of items no longer used for production or support.

The CM discipline will be applied to hardware, including power systems, software, firmware, documentation, test and support equipment, and spares. The Change Control Board (CCB) will ensure that documentation associated with an approved change to a CBP system is updated to reflect the appropriate baseline, including an analysis of any potential security implications. The initial configuration must be documented in detail and all subsequent changes must be controlled

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000086

through a complete and robust CM process. Configuration management has security implications in three areas:

1. Ensuring that the configuration of subordinate IT system elements are consistent with the certification and accreditation requirements of the parent system
2. Ensuring that any subsequent changes, including an analysis of any potential security implications, are approved
3. Ensuring that all recommended and approved security patches are properly installed

As new systems and newly modified systems proceed through the SLC, changes to these systems must be documented and tested prior to placing these systems into the operational environment. This includes the testing of security controls. The objective is to ensure that new vulnerabilities are not introduced during the change process. The same requirements apply to operational systems as they undergo periodic modifications. Changes must be documented and tested prior to placing the system back into the operational environment.

Configuration management policies must take into account and have provisions for quickly testing and approving time-sensitive changes that result from newly released vulnerability information. Often in today's climate, severe new vulnerabilities quickly present themselves and the risk of not immediately implementing the vendor-supplied patches exceeds the risk of installing an untested vendor patch. CBP must have provisions for reacting quickly as these critical patches are identified and released by the DHS Security Operations Center (SOC).

Policy ID	CBP Policy Statements	Relevant Controls
3.7.a	Configuration management plans (CMPs) for all IT systems shall be created as part of their System Security Plans (SSPs). All CBP systems shall be under the oversight of a Change Control Board (CCB).	CM-1
3.7.b	Configuration management controls shall be established, implemented, and enforced on all IT systems and networks in order to address significant deficiencies as part of a Plan of Action and Milestones (POA&M).	CA-5, CM-3
3.7.c	Information security patches must be installed in accordance with configuration management plans and within the timeframe or direction stated within the Information Security Vulnerability Management (ISVM) message published by the DHS Computer Security Incident Response Center (CSIRC).	SI-2
3.7.d	System Owners shall document the initial system configuration in detail and control all subsequent changes in accordance with the CMP.	CM-2, CM-3
3.7.e	Workstations shall be configured in accordance with DHS guidance on the Federal Desktop Core Configuration (FDCC). Configuration shall include installation of the DHS Common Policy OID, Common Policy Framework	CM-2, CM-6

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000087

Policy ID	CBP Policy Statements	Relevant Controls
	Root CA certificate, and the DHS Principal CA certificate.	
3.7.f	If the information system uses operating systems or applications that do not have hardening or do not follow configuration guidance from the DHS CISO, the System Owner shall request an exception, including a proposed alternative secure configuration.	CM-2, CM-6
3.7.g	CBP shall ensure that CM processes under their purview include and consider the results of a security impact analysis when considering proposed changes.	CM-4

Configuration management responsibilities are provided below.

Configuration Management Responsibilities
CISO • Ensure that security issues are being addressed in configuration reviews and the Change Control Board. **Certifying Officials** • Re-certify the system if significant configuration changes have been made. **AO** • Re-accredit systems if significant configuration changes have been made. • Ensure that IT Project Managers and Development/O&M Support Teams implement an effective configuration management process in accordance with SLC requirements. **Site Management** • Ensures that approved configuration changes are correctly implemented at the site. **IT Project Managers/ISSOs** • Ensure that configuration management procedures are documented and implemented for all proposed configuration changes to IT systems. • Ensure that all proposed configuration changes to operating systems and applications are analyzed prior to implementation to determine if the proposed change has security implications. • Maintain a capability to quickly approve and implement time-sensitive security patches in reaction to late-breaking security vulnerabilities identified by the DHS SOC. • Ensure that all proposed configuration changes to operating systems, operating system security features, applications, critical system files, and system devices are formally approved, tested, and documented prior to the change being implemented. • Ensure that all approved changes to the configuration baseline are documented, reviewed for accuracy, and that records are maintained for each IT system for both the current and all previous configurations. • Ensure that formal system configuration reviews are performed. • Ensure that accurate system documentation and configuration logs are maintained to reflect current and prior configuration baselines.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000088

Configuration Management Responsibilities
• Prepare and distribute a configuration management plan for each system under their authority. • Implement and enforce configuration management controls.
Project Team
• Understand and comply with the configuration management plan for the system. • Comply with configuration management controls and procedures.

The CISO will make determinations as to when time-sensitive system patches identified by the DHS SOC must be quickly implemented to protect the CBP infrastructure. The CISO, in cooperation with network operations leadership, will determine how quickly late-breaking patches must be expedited through the configuration management process and installed on CBP systems in order to protect mission accomplishment.

The ISSO and IT project manager work with the Development Team (for new development systems) or the Operations Support Team (for fielded systems) to ensure that all proposed changes to the configuration baseline are analyzed and tested to determine if the proposed changes have security implications. As new vulnerabilities are identified during the testing process, appropriate security software patches must be developed and installed prior to implementation of the proposed change.

Any changes that impact the security posture of the system must be brought to the attention of the Certification Agent and the Authorizing Official (AO). Further, all proposed configuration changes to operating systems, operating system security features, applications, critical system files, and system devices must then be formally approved and documented prior to the change being implemented. If the approved change is deemed to be significant, the C&A documentation must be updated.

This configuration management process continues throughout the life cycle of the system.

3.8 Risk Management

Risk management is a process that allows system owners to balance the operational and economic costs of protective measures to achieve gains in mission capability by protecting the IT systems and data that support their organization's missions.

The purpose of risk management is to identify risks, assess the impacts of the risks identified, and to take appropriate steps to reduce the identified risks to an acceptable level. An effective risk management process is a vital component of a successful Information Security Program. An organization's risk management process is designed to protect the *organization and its ability to perform its mission*, not just its IT assets.

Effective risk management enables an organization to accomplish its mission(s) by

1. Better securing the IT systems that store, process, or transmit organizational information

2. Enabling management to make well-informed risk management decisions to justify the expenditures that are part of an IT budget

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000089

3. Assisting management in authorizing IT systems on the basis of the supporting documentation resulting from the performance of risk management.

Policy ID	CBP Policy Statements	Relevant Controls
3.8.a	Establish a risk management program in accordance with National Institute of Standards and Technology Special Publication (NIST SP) 800-30, *Risk Management Guide for Information Technology Systems*.	RA-1
3.8.b	Conduct and document risk assessments every three years, when high impact weaknesses are identified, or whenever significant changes to the system configuration or to the operational/threat environment have been made, whichever occurs first. The risk assessment must consider the effects of the modifications on the operational risk profile of the information system. SSPs shall be updated and re-certification conducted if warranted by the results of the risk assessment.	RA-4
3.8.c	CISO shall establish a CBP-wide Security Test and Evaluation (ST&E) program to ensure a consistent approach to testing of effectiveness of controls.	RA-1
3.8.d	Risk Executives shall review recommendations for risk determinations and risk acceptability and may recommend changes to the CIO/AO.	RA-3
3.8.e	CBP SOC shall deploy a CBP-wide network scanning program.	RA-5
3.8.f	Special rules apply to CFO designated systems. See Section 3.18 for additional information.	---

Risk management responsibilities are provided below.

Risk Management Responsibilities
CISO • Establishes and enforces policy relating to the risk management process. **Certification Agents** • Evaluate the risk assessment document as part of the certification process. • Ensure that the risk assessment contains information required for C&A. • Recommend to the AO the possible implementation of additional risk mitigation actions that would mitigate existing residual risks. **AO** • Determine the overall degree of acceptable risk based on the CBP's mission requirements. • Determine whether the residual risk for the IT system being accredited is within tolerable limits. • Make a risk-based decision to (1) grant system accreditation, (2) grant an interim authorization to operate the system for a designated period of time (systems in development testing or prototypes only), or (3) deny system accreditation because the risks to the system

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000090

Risk Management Responsibilities
are not at an acceptable level. **System Owners** • Assist in determining the degree of acceptable residual risk based on the Department's mission requirements. • Review the Certification Package and ensure resources are provided to implement risk mitigation measures. **IT Project Managers/ISSOs** • Conduct the initial risk assessment. • Ensure that the system security plan and risk assessment contain information required by certification activities and address all appropriate management, operational, and technical controls. • Initiate follow-on risk assessments if any significant changes to the system configuration or to the operational/threat environment have occurred, or every three years, whichever comes first.

The risk management process described in NIST SP 800-30 contains three key elements: (1) risk assessment, (2) risk mitigation, and (3) evaluation and assessment. Risk management is an integral part of the Certification and Accreditation (C&A) process, which is discussed in Section 3.9.

3.8.1 Risk Assessment

Risk assessments are used to determine the extent of potential threats and risks associated with an IT system throughout its lifecycle. Based on the results of the risk assessment, appropriate security controls can be identified to reduce risks to an acceptable level during the risk mitigation phase. See Section 3.9.4 for more information on developing a risk assessment with the RMS automated tool.

NIST SP 800-30 identifies nine major activities to be conducted in the development of the risk assessment:

1. System Characterization
2. Threat Identification
3. Vulnerability Identification
4. Control Analysis
5. Likelihood Determination
6. Impact Analysis
7. Risk Determination
8. Control Recommendations

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000091

9. Results Documentation

Threats to CBP information systems may target communications networks, hardware devices, software applications, individuals, and physical attacks on CBP facilities. Potential threats to CBP include:

1. Disruption of voice communications
2. Disruption of internal communications
3. Insertion of 'Trojan horses', computer viruses, or other malware into the network environment of CBP
4. Unauthorized access to internal systems through 'social engineering' or by posing as a CBP official or authorized contractor

3.8.2 Risk Mitigation

The risk mitigation element occurs after the risk assessment phase is complete. Risk mitigation encompasses the prioritization, evaluation, and implementation of appropriate security controls identified during the risk assessment phase.

NIST SP 800-30 identifies seven major activities to be conducted as part of the risk mitigation phase:

1. Prioritize Actions
2. Evaluate Recommended Control Options
3. Conduct a Cost-Benefit Analysis
4. Select Appropriate Controls
5. Assign Implementation Responsibility
6. Develop an Implementation Plan
7. Implement Selected Controls.

Examples of security measures employed to reduce the risk of threats include:

1. Use of electronic badges for facility access (physical)
2. Deployment of firewalls to restrict network access
3. Use of anti-virus software

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000092

3.8.3 Evaluation and Assessment

Risk management is an ongoing process that will evolve over time as IT systems are updated and replaced with newer versions. New risks can surface and risks previously mitigated can re-surface as concerns.

For these reasons, CBP must conduct risk assessments whenever significant changes to the system configuration or to the operational/threat environment occur, or every 3 years, whichever comes first. The risk assessment is a key component of the C&A process discussed in the following section.

3.9 Certification and Accreditation, Remediation, and Reporting

FISMA directs that all Federal agencies develop and implement a Department-wide Information Security Program designed to safeguard IT assets and data. CBP bases its Certification and Accreditation (C&A) policy on DHS policy and the recommendations set forth in NIST SP 800-37, Rev. 1, DRAFT Guide for the Security Authorization of Federal Information Systems: A Security Life Cycle Approach, August 2008, and OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*.

Certification is the comprehensive testing and evaluation of the management, operational, and technical security features of an IT system. It primarily addresses software and hardware security safeguards; considers procedural, physical, and personnel security measures; and establishes the extent to which a particular design and implementation meets a specified set of security requirements.

Accreditation is the official management decision by the AO, that authorizes the operation of an IT system. It includes explicitly accepting the risk to Department operations, assets, or individuals, based on the implementation of an agreed-upon set of security controls. The AO accepts security responsibility for the operation of certified IT systems and officially declares that a specified IT system is approved to operate (ATO) based on these protections. The AO shall be identified in TrustedAgent FISMA (TAF). The CIO will serve as the AO.

NIST SP 800-37 describes the four phases of certification and accreditation. The artifacts required by the RMS automated C&A tool and by the TAF automated reporting tool are listed below by the phase in which each is generated:

- **Initiation Phase**

  FIPS 199 Categorization (Section 3.9.1)

  Privacy Impact Assessment (Section 3.9.2)

  E-Authentication (Section 3.9.3)

  Risk Assessment (Section 3.9.4)

  System Security Plan (Section 3.9.5)

  Contingency Plan (Section 3.9.6).

- **Certification Phase**

  Security Test and Evaluation (ST&E) Plan (Section 3.9.7)

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000093

Contingency Plan Testing (Section 3.9.8)

Security Assessment Report (SAR) (Section 3.9.9)

- **Accreditation Phase**

  Authorization to Operate (ATO) Letter (Section 3.9.10)—includes updated System Security Plan (SSP), Plan of Action and Milestones (POA&M), SAR

- **Continuous Monitoring Phase**

  Annual Self-Assessments (Section 3.9.11)

All production IT systems (major applications, general support systems) are to undergo C&A. In some situations, a common controls (type accreditation) approach may be used for authorizing a system as defined by CBP, DHS and NIST guidance. Prior to starting a common controls-based C&A, agreement should be reached with the AO to ensure a sufficient approach is performed. See Appendix D for more information on type certification/accreditation.

In accordance with approved DHS information security policy, the Risk Management System (RMS) automated tool developed by SecureInfo, Inc., shall be used to produce C&A packages for all IT systems. All IT systems shall be accredited using RMS. The NIST 800-53 controls must be applied. Applying the NIST 800-53 controls requires that systems be categorized.

Artifacts generated during the accreditation process are uploaded into TrustedAgent FISMA (TAF), which supports the remediation process with its capability to manage the POA&M process and which generates quarterly reports and the required annual self-assessment.

The artifacts required by the RMS and TAF automated tools are listed below:

1. FIPS 199 Categorization
2. Privacy Impact Assessment (PIA)
3. E-Authentication
4. Risk Assessment
5. System Security Plan (SSP)
6. Contingency Plan
7. Security Test and Evaluation (ST&E)
8. Contingency Plan Testing
9. Security Assessment Report (SAR)
10. Authorization to Operate (ATO)—includes updated System Security Plan (SSP), Plan of Action and Milestones (POA&M), SAR

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000094

11. Annual NIST SP 800-53-based Self-Assessments.

All certifications and accreditations for unclassified and collateral classified systems shall be done following DHS Management Directive 4300 series policies and procedures. SCI Systems are accredited by the DHS Office of Intelligence and Analysis (DHS I&A).

Policy ID	CBP Policy Statements	Relevant Controls
3.9.a	Assign an impact level (high, moderate, low) to each security objective (confidentiality, integrity, and availability) and apply NIST 800-53 controls specific to the security objective at the determined impact level. Impact levels shall be assigned according to the standards set in FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, and following the guidance from NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*. CBP C&A policy is based on DHS policy and on guidance from NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*.	RA-2
3.9.b	Implement NIST SP 800-53 security controls, using the FIPS Pub 200, *Minimum Security Requirements for Federal Information and Information Systems* methodology, based on the impact level established for each security objective (confidentiality, integrity, availability).	---
3.9.c	Pursue type C&A for IT resources that are under the same direct management control; have the same function or mission objective, operating characteristics, security needs, and that reside in the same general operating environment, or in the case of a distributed system, reside in various locations with similar operating environments. Type C&A shall consist of a master C&A package describing the common controls implemented across sites and site-specific controls and unique requirements that have been implemented at the individual sites.	---
3.9.d	The AO for a system shall be identified in Trusted Agent FISMA (TAF). The CIO shall serve as the AO.	---
3.9.e	The CISO shall ensure that all new or major upgrades of existing sensitive IT systems and networks are formally certified through a comprehensive evaluation of their management, operational, and technical security features.	CA-4
3.9.f	The certification, made as part of and in support of the accreditation process, shall determine the extent to which a particular design and implementation plan meets the DHS required set of security controls.	---
3.9.g	The CISO shall ensure that a risk assessment is conducted whenever any modifications are made to sensitive IT systems, networks, or to their physical environments, interfaces, or user community. SSPs shall be updated and re-certification conducted if warranted.	RA-4

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000095

Policy ID	CBP Policy Statements	Relevant Controls
3.9.h	Accredit systems at initial operating capability and every three years thereafter, or whenever a major change occurs, whichever occurs first. An ATO of six (6) months or less must receive an ATO accreditation period waiver from the DHS CISO before submission to the AO for a final accreditation decision.	CA-6
3.9.i	The AO may grant an Interim Authorization to Operate (IATO) for systems that are undergoing development testing or are in a prototype phase of development. A system must be certified and accredited in an Authorization to Operate (ATO) letter prior to passing the Key Decision Point 3 milestone in the development life cycle. IATOs are not appropriate for operational systems. The AO may grant an IATO for a maximum period of six months and may grant one six month extension.	PL-1
3.9.j	If the system is not fully accredited and has not received a full ATO by the end of the second and final IATO, the system shall not be deployed as an operational system.	PL-1
3.9.k	As a result of the Office of the Inspector General (OIG) auditing experience, CBP shall request concurrence from the DHS CISO for all accreditations for six months or less.	—
3.9.l	All CBP IT systems shall be accredited using the automated tools, TAF and RMS, approved by the DHS CISO.	CA-1
3.9.m	All certifications and accreditations for unclassified and collateral classified systems shall be done following DHS Management Directive 4300 series policies and procedures, in addition to CBP C&A process. SCI Systems are accredited by the DHS Office of Intelligence and Analysis (DHS I&A).	CA-1, CA-4
3.9.n	CISO shall ensure that enterprise security tools are used to manage C&A processing and FISMA reporting.	CA-1
3.9.o	CISO shall maintain a repository for all C&A documentation and modifications.	CA-1
3.9.p	CISO shall establish processes to ensure consistent C&A processing across all CBP IT systems.	CA-1
3.9.q	System Owners shall use the POA&M process to manage vulnerabilities, correct deficiencies in security controls, and remediate weaknesses in system security plans.	CA-5
3.9.r	CBP shall use the tools directed by the DHS CISO to document and maintain POA&Ms.	CA-5
3.9.s	The AO shall formally assume responsibility for operating an information system at an acceptable level of risk. System operation with sensitive	CA-6

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000096

Policy ID	CBP Policy Statements	Relevant Controls
	information is prohibited without an ATO.	
3.9.t	ATOs shall only be provided for systems that fully comply with policy or have been granted appropriate exceptions or waivers.	CA-6
3.9.u	Artifacts in support of *new* ATOs shall not be older than 13 months. Older artifacts remain valid during the life of a current ATO.	---
3.9.v	The DHS CIO may revoke any ATO of any DHS IT system.	CA-6
3.9.w	The CIO may revoke the ATO of any CBP IT system.	CA-6
3.9.x	The duration of an ATO must be at least six (6) months and shall be no longer than three (3) years. Concurrence from the DHS CISO shall be requested for all accreditations lasting less than six (6) months.	CA-6
3.9.y	CBP shall establish an information system security review and assistance program within their respective security organization in order to provide System Owners with expert review of programs, assist in identifying deficiencies, and provide recommendations for bringing systems into compliance. This security and review assistance is provided by Security and Technology Policy (STP).	CA-7, PL-1

Certification and accreditation responsibilities are provided below.

Certification and Accreditation Responsibilities
DHS CISO • Establishes and enforces policy relating to the C&A process. **AO** • Determine degree of acceptable residual risk based on Department's mission requirements. • Review the state of the security controls for the system and the mission requirements of the Department. • Assess the correctness and effectiveness of security controls and identify the level of risk remaining (residual risk) for the system in performing its operational mission. • Determine whether the residual risk is within tolerable limits. • Make a risk-based decision to (1) grant system accreditation, (2) grant an interim authorization to operate the system for a designated period of time (systems in development testing or prototypes only), or (3) deny system accreditation because the risks to the system are not at an acceptable level. **System Owners** Certification Responsibilities: • Ensure that adequate resources are budgeted for and allocated to the C&A process. • Review the results of the Initiation and Security Certification phases and ensure resources

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000097

Certification and Accreditation Responsibilities
are provided to identify and implement risk mitigation measures. Accreditation Responsibilities: • Assist in determining degree of acceptable residual risk based on agency's mission requirements. • Review the Certification Package and ensure resources are provided to implement risk mitigation measures. **IT Project Managers/ISSOs** • Ensure that the SecureInfo RMS automated tool is utilized to develop C&A packages. Certification Responsibilities: • Ensure that the SSP and risk assessment contain information required by certification activities. • Develop the ST&E plan, conduct the ST&E, and prepare the ST&E Report. Accreditation Responsibilities: • Complete the final risk assessment, update the security plan, prepare the certification findings, and prepare a Draft Certification Statement. • Complete the Certification Package and forward to the Certifying Official. • Maintain files of the Certification Package. • Initiate Re-Accreditation activities if any significant changes to the system configuration or to the operational/threat environment that might affect system security have occurred, or every three years, whichever comes first. **Certification Agent** • Participate in the early phase to assist the development team in identifying specific security requirements. • Validate the security design decisions of the development teams and the ISSOs. • Determine with the data owner(s) and ISSO(s), the minimum-security features for each unique application. • Observe the testing of security controls for assigned Major Applications (MAs) and General Support Systems (GSSs). • Ensure that the System Security Plan (SSP), Security Test & Evaluation (ST&E), Contingency Plan, and Risk Assessment contain the information required for C&A. • Ensure security plans are developed for all information systems. Ensure that the system is certified and the certification documentation is developed using the DHS C&A tool, Risk Management System (RMS) • Review the security documentation. • Write the System Assessment Report (SAR) and include the Plan of Actions and Milestones (POA&M) and a list of residual risks. • Write the Certification Statement, which reflects the state of the security controls, based on the results of the ST&E and review C&A Package and recommend approval to the Certifying Official.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000098

Risk Management System

Risk Management System (RMS) is an automated system that supports the established C&A process. RMS system is the DHS mandated solution for developing and maintaining C&A documentation. RMS bridges the gap between regulatory requirements, standards, and local security policies. This system provides C&A audit-readiness against mandated regulations and manages the security C&A compliance lifecycle with regulatory content updates. The use of RMS enables conformance and standardization of the DHS C&A process on CBP.

Through an interactive process, RMS aids security personnel (ISSOs) in identifying the minimum level of system security controls based on FIPS-200 (i.e., NIST SP 800-53) and DHS policy. This is accomplished by the completion of an RMS security questionnaire that generates required security document templates. RMS tracks this comprehensive list of security requirements through the development of the required security certification and accreditation documents.

For additional information, training or obtaining a log-on for this tool, contact the STP Branch at (b)(6) (b)(7)(C).

TrustedAgent FISMA

TrustedAgent FISMA (TAF) is a DHS enterprise-wide application that is a repository for system identification and security information. TAF also generates Federal Information Security Management Act (FISMA) reports in compliance with the OMB guidelines. System specific Plans of Action and Milestones (POA&Ms) are entered into TAF in order to capture and track the identified security weaknesses with their associated corrective milestones. TAF provides an automated capability to support required system self-assessment reviews utilizing the NIST SP 800-53. TAF contains data on the number of systems with contingency plans, tested contingency plans, system security plans, security tests and evaluations, identified weaknesses and accompanying POA&Ms, certifications and accreditations, IT security training, and incident response activities.

In addition to the primary tracking capability of TAF, CBP benefits by the accurate and current listing of operational systems and sub-systems that are recognized by DHS. This system inventory serves as a baseline for the security performance measures that TAF generates for component and departmental level security management officials. This data is used to generate the TAF measures and is reported to the DHS. The TAF data also serves as the basis for quarterly FISMA reports for OMB.

For additional information, training, or obtaining a log-on for this tool, contact the STP Branch at (b)(6) (b)(7)(C).

3.9.1 FIPS 199 Categorization and the NIST SP 800-53 Controls

For DHS, the high water mark requirement is amplified to reflect the actual security requirements for controls to meet. The high water mark is the concept that the highest impact level of any of the security objectives (confidentially, integrity, and availability) must be implemented for the system as a whole, based on the highest impact level of each of the individual security objectives.

At DHS, the necessary security controls, supporting the security objectives, required for an IT system will be implemented without the requirement to implement extra controls that may not be

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000099

necessary. This is the minimum DHS standard; however, any program that wishes to implement more than the minimum controls can still implement them when appropriate. This policy amplification is a Department-level risk-based decision that is consistent with FISMA policy which requires DHS to "cost-effectively reduce information security risks to an acceptable level." The tailoring of controls and use of compensating controls is also consistent with providing the safeguards necessary to reduce the risks in a specific operational environment.

This policy amplification is also consistent with the NIST information security guidance which promulgates the "concept of risk based decisions." The due diligence required by FIPS 199 of determining the exact impact level each type of information contained on the system, and each of the security objectives, will lead to well defined impact levels for confidentiality, integrity, and availability of the system as a whole. It is important, when using a risk-based decision to minimize the security controls, that all of the information and the risks to that information be clearly defined and documented. In that way, the AO can make an informed decision on the level of risk that is acceptable for the system and its information in the specific operational environment.

As a result, in the DHS FIPS 199 Workbook (developed from FIPS 199, NIST SP 800-60, and the DHS Business Reference Model), impact levels (high, moderate, low) can be assigned to each security objective. This means, for example, that a system with low risk availability, high risk integrity, and low risk confidentiality will not be required to implement all high controls across the board. Rather the controls that fall out of the analysis will be implemented (i.e., high levels for integrity controls, low for the confidentiality and availability controls). NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, should be applied specific to the security objective determined impact level.

For systems involving personally identifiable information, the confidentiality security objective shall be assigned an impact level of at least moderate. A risk-based assessment shall be performed to determine whether the confidentiality security objective warrants being assigned an impact level of high for such systems.

The table below identifies the security objective(s) (C = confidentiality, I = integrity, and A = availability) assigned to each NIST SP 800-53 control by impact level (L = low, M = moderate, and H = high; a bullet indicates the control is applicable, and a check indicates the enhancement to the control is applicable). See Attachment M for a listing of the NIST SP 800-53 controls by impact level and by security objective, and it provides information on the possible tailoring of these controls and on the use of compensating controls.

Table 3.9.1: NIST SP 800-53 Security Controls and DHS-assigned Security Objectives

800-53 Control and Enhancements		Security Objectives (C, I, A)	Security Impact Level		
			L	M	H
Access Control (AC)					
AC-1	Access Control Policy and Procedures	CIA	●	●	●
AC-2	Account Management	C	●	●	●
	E1: Automated mechanisms for management of	C	---	✓	✓

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000100

800-53 Control and Enhancements		Security Objectives (C, I, A)	Security Impact Level		
			L	M	H
	accounts				
	E2: Automatic termination of temporary and emergency accounts	C	---	✓	✓
	E3: Automatic disabling of inactive accounts	C	---	✓	✓
	E4: Automated mechanisms for auditing actions on accounts	C	---	✓	✓
AC-3	Access Enforcement	C	●	●	●
	E1: Access to security functions and information is restricted to authorized personnel	C	---	✓	✓
AC-4	Information Flow Enforcement	C	---	●	●
	E1: Explicit labels	C	---	---	---
	E2: Protected processing domains	C	---	---	---
	E3: Dynamic security policy mechanisms	C	---	---	---
AC-5	Separation of Duties	C	---	●	●
AC-6	Least Privilege	C	---	●	●
AC-7	Unsuccessful Login Attempts	C	●	●	●
	E1: Automatic locking of account/node	C	---	---	---
AC-8	System Use Notification	C	●	●	●
AC-9	Previous Logon Notification	C	---	---	---
AC-10	Concurrent Sessions Control	C	---	---	●
AC-11	Session Lock	C	---	●	●
AC-12	Session Termination	C	---	●	●
	E1: Local and remote session termination	C	---	---	✓
AC-13	Supervision and Review — Access Control	C	●	●	●
	E1: Automated mechanisms to facilitate review of user activities	C	---	✓	✓
AC-14	Permitted Actions without Identification or Authentication	CI	●	●	●
	E1: Actions permitted only to necessary extent	CI	---	✓	✓
AC-15	Automated Marking	C	---	---	●
AC-16	Automated Labeling	C	---	---	---
AC-17	Remote Access	C	●	●	●
	E1: Automated mechanisms for monitoring and control of remote access	C	---	✓	✓
	E2: Encryption for protecting confidentiality of remote access sessions	C	---	✓	✓

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000101

800-53 Control and Enhancements		Security Objectives (C, I, A)	Security Impact Level		
			L	M	H
	E3: Remote access controlled through a managed access control point.	C	---	✓	✓
	E4: Remote access for privileged functions	C	---	✓	✓
AC-18	Wireless Access Restrictions	C	●	●	●
	E1: Authentication and encryption for protecting wireless access to the information system	C	---	✓	✓
	E2: Scanning for unauthorized wireless access points	C	---	---	✓
AC-19	Access Control for Portable and Mobile Devices	C	---	●	●
AC-20	Use of External Information Systems	C	●	●	●
	E1: Prohibit use of external information system-to-access	C	---	✓	✓
Awareness and Training (AT)					
AT-1	Security Awareness and Training Policy and Procedures	CIA	●	●	●
AT-2	Security Awareness	CIA	●	●	●
AT-3	Security Training	CIA	●	●	●
AT-4	Security Training Records	CIA	●	●	●
AT-5	Contacts with Security Groups and Associations	CIA	---	---	---
Audit and Accountability (AU)					
AU-1	Audit and Accountability Policy and Procedures	CIA	●	●	●
AU-2	Auditable Events	CIA	●	●	●
	E1: Multi-component, system-wide audit trail	CIA	---	---	✓
	E2: Selected events audit	CIA	---	---	✓
	E3: Review and update auditable events	CIA	---	✓	✓
AU-3	Content of Audit Records	CIA	●	●	●
	E1: Detailed info. audit	CIA	---	✓	✓
	E2: Centrally managed audit	A	---	---	✓
AU-4	Audit Storage Capacity	IA	●	●	●
AU-5	Response to Audit Processing Failures	IA	●	●	●
	E1: Alert for max. capacity	A	---	---	✓
	E2: Real-time alert for audit failure events		---	---	✓
AU-6	Audit Monitoring, Analysis, and Reporting	CIA	---	●	●
	E1: Automated audit monitoring	CIA	---	---	✓
	E2: Alert for unusual activities	CIA	---	✓	✓
AU-7	Audit Reduction and Report Generation	IA	---	●	●

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000102

800-53 Control and Enhancements		Security Objectives (C, I, A)	Security Impact Level		
			L	M	H
	E1: Report select criteria	IA	---	✓	✓
AU-8	Time Stamps	I	●	●	●
	E1: Synchronization of internal clocks	I	---	✓	✓
AU-9	Protection of Audit Information	CI	●	●	●
	E1: Audit on write-once media	I	---	---	---
AU-10	Non-Repudiation	I	---	---	---
AU-11	Audit Record Retention	A	●	●	●
Certification, Accreditation, and Security Assessments (CA)					
CA-1	Certification, Accreditation, and Security Assessment Policies and Procedures	CIA	●	●	●
CA-2	Security Assessments	CIA	●	●	●
CA-3	Information System Connections	C	●	●	●
CA-4	Security Certification	CIA	●	●	●
	E1: Independent security control assessment	CIA	---	✓	✓
CA-5	Plan of Action and Milestones	CIA	●	●	●
CA-6	Security Accreditation	CIA	●	●	●
CA-7	Continuous Monitoring	CIA	●	●	●
	E1: Independent monitoring of security controls	CIA	---	---	---
Configuration Management (CM)					
CM-1	Configuration Management Policy and Procedures	CIA	●	●	●
CM-2	Baseline Configuration	IA	●	●	●
	E1: Update baseline at new installation	IA	---	✓	✓
	E2: Automated update of baseline configuration	IA	---	---	✓
CM-3	Configuration Change Control	CIA	---	●	●
	E1: Automated change control	CIA	---	---	✓
CM-4	Monitoring Configuration Changes	CIA	---	●	●
CM-5	Access Restrictions for Change	CIA	---	●	●
	E1: Automated access control	CIA	---	---	✓
CM-6	Configuration Settings	CI	●	●	●
	E1: Automated central configuration control	I	---	---	✓
CM-7	Least Functionality	CIA	---	●	●
	E1: Reviews functionality	CIA	---	---	✓
CM-8	Information System Component Inventory	CIA	●	●	●
	E1: Maintenance of information system components inventory	CIA	---	✓	✓

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000103

800-53 Control and Enhancements		Security Objectives (C, I, A)	Security Impact Level		
			L	M	H
	E2: Automated mechanisms to maintain inventory	CIA	---	---	✓
Contingency Planning (CP)					
CP-1	Contingency Planning Policy and Procedures	CIA	●	●	●
CP-2	Contingency Plan	A	●	●	●
	E1: Coordinated plans	A	---	✓	✓
	E2: Capacity planning	A	---	---	✓
CP-3	Contingency Training	A	---	●	●
	E1: Simulated events training	A	---	---	✓
	E2: Automated training	A	---	---	---
CP-4	Contingency Plan Testing and Exercises	A	●	●	●
	E1: Coordinated testing	A	---	✓	✓
	E2: Alternate processing site testing	A	---	---	✓
	E3: Automated testing	A	---	---	---
CP-5	Contingency Plan Update	A	●	●	●
CP-6	Alternate Storage Site	A	---	●	●
	E1: Geographically separate	A	---	✓	✓
	E2: Pre-configured storage	A	---	---	✓
	E3: Identified access problems	A	---	✓	✓
CP-7	Alternate Processing Site	A	---	●	●
	E1: Geographically separate	A	---	✓	✓
	E2: Identified access problems	A	---	✓	✓
	E3: Priority service contract	A	---	✓	✓
	E4: Pre-configured alternate site	A	---	---	✓
CP-8	Telecommunications Services	A	---	●	●
	E1: Priority service contract	A	---	✓	✓
	E2: No shared point of failure	A	---	✓	✓
	E3: Geographically separate	A	---	---	✓
	E4: Contingency plans for vendor services	A	---	---	✓
CP-9	Information System Backup	A	●	●	●
	E1: Backup tested	A	---	✓	✓
	E2: Backup restored in testing	A	---	---	✓
	E3: Separate backup facility or fire-rated container	A	---	---	✓
	E4: Protect from unauthorized modification	A	---	✓	✓
CP-10	Information System Recovery and Reconstitution	A	●	●	●

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000104

800-53 Control and Enhancements		Security Objectives (C, I, A)	Security Impact Level		
			L	M	H
	E1: Recovery and Reconstitution testing	A	---	---	✓
Identification and Authentication (IA)					
IA-1	Identification and Authentication Policy and Procedures	CIA	●	●	●
IA-2	User Identification and Authentication	C	●	●	●
	E1: Multifactor authentication	C	---	✓	---
	E2: Multifactor authentication for local system access	C	---	---	✓
	E3: Multifactor authentication for remote system access	C	---	---	✓
IA-3	Device Identification and Authentication	C	---	●	●
IA-4	Identifier Management	C	●	●	●
IA-5	Authenticator Management	C	●	●	●
IA-6	Authenticator Feedback	C	●	●	●
IA-7	Cryptographic Module Authentication	C	●	●	●
Incident Response (IR)					
IR-1	Incident Response Policy and Procedures	CIA	●	●	●
IR-2	Incident Response Training	CIA	---	●	●
	E1: Simulated events	CIA	---	---	✓
	E2: Automated response training	CIA	---	---	---
IR-3	Incident Response Testing and Exercises	CIA	---	●	●
	E1: Automated testing	CIA	---	---	✓
IR-4	Incident Handling	CIA	●	●	●
	E1: Automated handling	CIA	---	✓	✓
IR-5	Incident Monitoring	CIA	---	●	●
	E1: Automated tracking and analysis	CIA	---	---	✓
IR-6	Incident Reporting	CIA	●	●	●
	E1: Automated reporting	CIA	---	✓	✓
IR-7	Incident Response Assistance	CIA	●	●	●
	E1: Automated distribution	CIA	---	✓	✓
Maintenance (MA)					
MA-1	System Maintenance Policy and Procedures	CIA	●	●	●
MA-2	Controlled Maintenance	A	●	●	●
	E1: Maintenance logs	A	---	✓	✓
	E2: Automated schedules	A	---	---	✓
MA-3	Maintenance Tools	IA	---	●	●

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000105

800-53 Control and Enhancements		Security Objectives (C, I, A)	Security Impact Level		
			L	M	H
	E1: Inspection of tools	CIA	---	---	✓
	E2: Malicious code check of tools	CIA	---	---	✓
	E3: Equipment sanitized	C	---	---	✓
	E4: Automated personnel check	C	---	---	---
MA-4	Remote Maintenance	CIA	●	●	●
	E1: Audit and review	CIA	---	✓	✓
	E2: Diagnostics in SSP	CIA	---	✓	✓
	E3: Level of security equal for diagnostic service	CIA	---	---	✓
MA-5	Maintenance Personnel	C	●	●	●
MA-6	Timely Maintenance	A	---	●	●
Media Protection (MP)					
MP-1	Media Protection Policy and Procedures	CIA	●	●	●
MP-2	Media Access	C	●	●	●
	E1: Guards or automated access control to media storage	C	---	✓	✓
MP-3	Media Labeling	C	---	---	●
MP-4	Media Storage	C	---	●	●
MP-5	Media Transport	C	---	●	●
	E1: Protection of media during transport	C	---	✓	✓
	E2: Information system media transport activities	C	---	✓	✓
	E3: Custodian to transport information system media	C	---	---	✓
MP-6	Media Sanitization and Disposal	C	●	●	●
	E1: Sanitization and disposal activities	C	---	---	✓
	E2: Test sanitization equipment and procedures	C	---	---	✓
Physical and Environmental Protection (PE)					
PE-1	Physical and Environmental Protection Policy and Procedures	CIA	●	●	●
PE-2	Physical Access Authorizations	C	●	●	●
PE-3	Physical Access Control	C	●	●	●
	E1: Physical access to information system	C	---	---	✓
PE-4	Access Control for Transmission Medium	C	---	---	●
PE-5	Access Control for Display Medium	C	---	●	●
PE-6	Monitoring Physical Access	CIA	●	●	●
	E1: Intrusion alarms and surveillance	CIA	---	✓	✓
	E2: Response to alarms	CIA	---	---	✓

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000106

800-53 Control and Enhancements		Security Objectives (C, I, A)	Security Impact Level		
			L	M	H
PE-7	Visitor Control	C	●	●	●
	E1: Escort and monitor visitors	C	---	✓	✓
PE-8	Access Records	C	●	●	●
	E1: Automated review	CA	---	---	✓
	E2: Record of physical access	C	---	---	✓
PE-9	Power Equipment and Power Cabling	A	---	●	●
	E1: Redundant parallel cabling	A	---	---	---
PE-10	Emergency Shutoff	A	---	●	●
	E1: Accidental or unauthorized activation	A	---	---	✓
PE-11	Emergency Power	IA	---	●	●
	E1: Long-term alternate power	A	---	---	✓
	E2: Long-term, self-contained power	A	---	---	---
PE-12	Emergency Lighting	A	●	●	●
PE-13	Fire Protection	A	●	●	●
	E1: Suppression and detection	A	---	✓	✓
	E2: Alert responders	A	---	✓	✓
	E3: Automatic fire suppression	A	---	✓	✓
PE-14	Temperature and Humidity	A	●	●	●
PE-15	Water Damage Protection	A	●	●	●
	E1: Automatic water shut-off	A	---	---	✓
PE-16	Delivery and Removal	C	●	●	●
PE-17	Alternate Work Site	A	---	●	●
PE-18	Location of Information System Components	CIA	---	●	●
	E1: Location planning	CIA	---	---	✓
PE-19	Information Leakage	C	---	---	---
Planning (PL)					
PL-1	Security Planning Policy and Procedures	CIA	●	●	●
PL-2	System Security Plan	CIA	●	●	●
PL-3	System Security Plan Update	CIA	●	●	●
PL-4	Rules of Behavior	CIA	●	●	●
PL-5	Privacy Impact Assessment	C	●	●	●
PL-6	Security-Related Activity Planning	CIA	---	●	●
Personnel Security (PS)					
PS-1	Personnel Security Policy and Procedures	CIA	●	●	●

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000107

800-53 Control and Enhancements		Security Objectives (C, I, A)	Security Impact Level		
			L	M	H
PS-2	Position Categorization	CIA	●	●	●
PS-3	Personnel Screening	C	●	●	●
PS-4	Personnel Termination	CA	●	●	●
PS-5	Personnel Transfer	C	●	●	●
PS-6	Access Agreements	C	●	●	●
PS-7	Third-Party Personnel Security	CIA	●	●	●
PS-8	Personnel Sanctions	CIA	●	●	●
Risk Assessment (RA)					
RA-1	Risk Assessment Policy and Procedures	CIA	●	●	●
RA-2	Security Categorization	CIA	●	●	●
RA-3	Risk Assessment	CIA	●	●	●
RA-4	Risk Assessment Update	CIA	●	●	●
RA-5	Vulnerability Scanning	CIA	●	●	●
	E1: Scanning tools update vulnerabilities	CIA	---	---	✓
	E2: Updates to reported list	CIA	---	---	✓
	E3: Ensure adequate scan coverage	CIA	---	---	---
System and Services Acquisition (SA)					
SA-1	System and Services Acquisition Policy and Procedures	CIA	●	●	●
SA-2	Allocation of Resources	CIA	●	●	●
SA-3	Life Cycle Support	CIA	●	●	●
SA-4	Acquisitions	CIA	●	●	●
	E1: Details on functional properties of security controls	CIA	---	✓	✓
	E2: Details on design and implementation of security controls	CIA	---	---	---
SA-5	Information System Documentation	CIA	●	●	●
	E1: Details for analysis/testing	CIA	---	✓	✓
	E2: Details on interfaces	CIA	---	---	✓
SA-6	Software Usage Restrictions	IA	●	●	●
SA-7	User Installed Software	CIA	●	●	●
SA-8	Security Engineering Principles	CIA	---	●	●
SA-9	External Information System Services	CIA	●	●	●
SA-10	Developer Configuration Management	CIA	---	---	●
SA-11	Developer Security Testing	CIA	---	●	●

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000108

800-53 Control and Enhancements		Security Objectives (C, I, A)	Security Impact Level		
			L	M	H
System and Communications Protection (SC)					
SC-1	System and Communications Protection Policy and Procedures	CIA	●	●	●
SC-2	Application Partitioning	CI	---	●	●
SC-3	Security Function Isolation	I	---	---	●
	E1: Hardware separation	I	---	---	---
	E2: Divides security functions	I	---	---	---
	E3: Minimize non-security functions in isolation	I	---	---	---
	E4: Independent modules	I	---	---	---
	E5: Layered structure	I	---	---	---
SC-4	Information Remnance	CI	---	●	●
SC-5	Denial of Service Protection	A	●	●	●
	E1: Restriction of user launch	A	---	---	---
	E2: Limits info. flooding	A	---	---	---
SC-6	Resource Priority	A	---	---	---
SC-7	Boundary Protection	C	●	●	●
	E1: Separate subnets for public access	C	---	✓	✓
	E2: Prevent public access	C	---	✓	✓
	E3: Limit access points	C		✓	✓
	E4: Managed interface with external telecommunication service	C	---	✓	✓
	E5: Deny network traffic by default	C	---	✓	✓
	E6: Unauthorized release of information	C	---	---	✓
SC-8	Transmission Integrity	I	---	●	●
	E1: Cryptographic to ensure recognition of changes	I	---	---	✓
SC-9	Transmission Confidentiality	C	---	●	●
	E1: Cryptographic to prevent unauthorized disclosure	C	---	---	✓
SC-10	Network Disconnect	CIA	---	●	●
SC-11	Trusted Path	CI	---	---	---
SC-12	Cryptographic Key Establishment and Management	IA	---	●	●
SC-13	Use of Cryptography	CI	●	●	●
SC-14	Public Access Protections	I	●	●	●
SC-15	Collaborative Computing	C	---	●	●
	E1: Physical disconnect	C	---	---	---
SC-16	Transmission of Security Parameters	C	---	---	---

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000109

800-53 Control and Enhancements		Security Objectives (C, I, A)	Security Impact Level		
			L	M	H
SC-17	Public Key Infrastructure Certificates	CI	---	●	●
SC-18	Mobile Code	CIA	---	●	●
SC-19	Voice Over Internet Protocol	CIA	---	●	●
SC-20	Secure Name/Address Resolution Service (Authoritative Source)	CIA	---	●	●
	E1: Security status of child subspaces	CIA	---	---	---
SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver)	CIA	---	---	●
	E1: Data origin authentication and data integrity verification	CIA	---	---	---
SC-22	Architecture and Provisioning for Name/Address Resolution Service	CIA	---	●	●
SC-23	Session Authenticity	CIA	---	●	●
System and Information Integrity (SI)					
SI-1	System and Information Integrity Policy and Procedures	CIA	●	●	●
SI-2	Flaw Remediation	I	●	●	●
	E1: Central auto-updates flaws	I	---	---	✓
	E2: Remediation reports	I	---	✓	✓
SI-3	Malicious Code Protection	CIA	●	●	●
	E1: Central virus protection	I	---	✓	✓
	E2: Automatic updates	I	---	✓	✓
SI-4	Information System Monitoring Tools and Techniques	CIA	---	●	●
	E1: System-wide detections	CIA	---	---	---
	E2: Automated real-time analysis	CIA	---	---	✓
	E3: Automated reconfiguration	CIA	---	---	---
	E4: Monitor outbound traffic	CIA	---	✓	✓
	E5: Real-time alert for compromise	CIA	---	---	✓
SI-5	Security Alerts and Advisories	CIA	●	●	●
	E1: Automated advisories	CIA	---	---	✓
SI-6	Security Functionality Verification	IA	---	---	●
	E1: Alert of failed security test	CIA	---	---	---
	E2: Distributed security testing	I	---	---	---
SI-7	Software and Information Integrity	I	---	---	●
	E1: Integrity scans	I	---	---	✓
	E2: Automated tools	I	---	---	✓

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000110

800-53 Control and Enhancements		Security Objectives (C, I, A)	Security Impact Level		
			L	M	H
	E3: Verification tools	I	---	---	---
SI-8	Spam Protection	CIA	---	●	●
	E1: Centrally managed	IA	---	---	✓
	E2: Automated updates	IA	---	---	---
SI-9	Information Input Restrictions	C	---	●	●
SI-10	Information Accuracy, Completeness, Validity, and Authenticity	I	---	●	●
SI-11	Error Handling	CIA	---	●	●
SI-12	Information Output Handling and Retention	C	---	●	●

3.9.2 Privacy Impact Assessment

IT systems involving personally identifiable information are required by Section 208 of the E-Government Act to have a Privacy Impact Assessment (PIA). A Privacy Threshold Analysis (PTA) is first performed to determine whether potential privacy data is being processed or stored by the IT system. Systems that are determined to have privacy concerns require a formal PIA.

The template for the Privacy Threshold Analysis is available on the DHS CISO page of DHS Online; the template is also available through the DHS Privacy Office, and the DHS Compliance Help Desk (b)(6) (b)(7)(C) can also provide assistance in obtaining the template for the Privacy Threshold Analysis. The PTA template is also included in the RMS tool.

The PIA template for those systems involving privacy information and requiring a PIA is available in the RMS tool. A Microsoft Word template is also available by contacting the DHS Compliance Help Desk.

The DHS *Certification and Accreditation (C&A) Guidance for SBU Systems: Users Manual* provides detailed information on the Privacy Threshold Analysis and on the PIA process.

3.9.3 E-Authentication

E-Authentication security requirements must be applied to IT systems that allow online transactions. The first step is to determine whether Government e-authentication security requirements apply to the system. For those systems for which e-authentication security requirements apply, two additional steps are required:

1. Determine the potential impact of authentication errors.
2. Determine the required assurance level for authentication.

The E-Authentication Workbook and the instructions needed for completing the workbook (see *DHS Information Security Categorization Guide*) are available on the DHS CISO page of DHS Online. The DHS Compliance Help Desk (b)(6) (b)(7)(C) can also provide assistance in obtaining these documents.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000111

3.9.4 Risk Assessment

Risk Assessment is the process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact. An initial risk assessment is used to understand the unique system risks and to determine if any controls are required to address specific threats or weaknesses to the system. The initial risk assessment incorporates system characterization information, security categorization determination (see Section 3.9.1), privacy threshold analysis and Privacy Impact Assessment (PIA) (Section 3.9.2), and e-Authentication assessment (Section 3.9.3). CBP and DHS follows the overall risk process as described in NIST Special Publication 800-30, *Risk Management Guide for IT Systems*. The results of the risk assessment will be used to directly address the controls that will be documented in the SSP and implemented within the system.

The initial risk assessment is updated and revised and becomes the final risk assessment as part of the overall accreditation process after the controls are implemented and tested and the results/corrective actions are implemented. Through the development of the final risk assessment, the definition of the program residual risk can be determined for the AO's acceptance during accreditation.

An initial risk assessment document is generated within RMS when a C&A package is created and the questionnaire is run.

The DHS *Certification and Accreditation (C&A) Guidance for SBU Systems: Users Manual* provides detailed information on developing the risk assessment within RMS.

3.9.5 System Security Plan

The System Security Plan (SSP) provides a complete description of the information system, including purposes and functions, system boundaries, architecture, user groups, interconnections, hardware, software, encryption techniques, transmissions, and network configuration. The SSP also provides an overview of the security requirements of the system and describes the controls in place or planned for meeting those requirements. In addition, the SSP delineates the responsibilities and expected behavior of all individuals who access the system. The SSP, typically written in conjunction with the risk assessment, is refined throughout the accreditation process.

A template for the SSP is provided in RMS. The template and the RMS Requirements Traceability Matrix (RTM) provide a basic structure to ensure consistency and completeness in the finished document. The DHS *Certification and Accreditation (C&A) Guidance for SBU Systems: Users Manual* provides detailed information on completing the SSP within RMS.

3.9.6 Contingency Plan

A contingency plan documents the management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster (see Section 3.5 for more information). The specific control requirements and level of effort are determined based on the IT system's security categorization. The level of resources for the contingency plan is based on the security categorization for the availability security objective:

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000112

1. For systems with a **low impact for availability**, the system owner can determine the contingency plan format and content that is appropriate for the system and its environment. The contingency plan generated in RMS can also be used.
2. For systems with a **moderate impact level for availability**, the default contingency plan template in RMS should be used.
3. Systems with a **high impact level for availability** should develop a rigorous contingency plan. The DHS-developed high impact version of a contingency plan, *IT Contingency and Disaster Recovery Plan*, should be used. This template is found in the Additional Documents section of RMS. The high impact plan can be received in RMS when creating a package, by answering "Yes" to additional documents in the questionnaire. This template is also available in Attachment K.

The DHS *Certification and Accreditation (C&A) Guidance for SBU Systems: Users Manual* provides detailed information on developing the contingency plan within RMS.

3.9.7 Security Test and Evaluation Plan

The Security Test and Evaluation (ST&E) Plan outlines the plan, the process, and the procedures necessary to verify that the controls outlined in the SSP are in place and are operating as expected. The ST&E Plan template provided by RMS is the starting point for ensuring that there is a plan and methodology for testing and verifying that the management, operational, and technical controls are in place. The Requirements Traceability Matrix (RTM) generated by RMS when a C&A package is initiated is pre-populated with sample test procedures. However, the procedures will need to be tailored to the particular SSP, risks, and system environment, and they will need to be supplemented with detailed technical methods and procedures.

The complete ST&E Plan includes both the primary document as well as any supporting material. Typically, this material includes the documented test procedures contained with the RMS RTM by system.

The DHS *Certification and Accreditation (C&A) Guidance for SBU Systems: Users Manual* provides detailed information on developing the ST&E Plan within RMS. Once the Risk Assessment, SSP, and ST&E Plan are completed and approved by the System Owner and agreed to with the Certification Agent, the ST&E testing can be conducted as part of the certification process. The test methods and procedures are documented as part of the ST&E Plan. Results of the testing are documented in the Security Assessment Report (see Section 3.9.9).

3.9.8 Contingency Plan Testing

Contingency plan testing is the process of simulating an IT security event and the subsequent activities undertaken to restore and recover the system following the simulated event.

Contingency plan testing is required only for systems with a moderate or high impact for the availability security objective; it is optional for systems with a low impact for availability. Testing requirements for systems with high, moderate, and low impact for availability are provided in the subsections that follow.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000113

3.9.8.1 Systems with High Impact Availability — Testing required

IT systems with high impact availability shall provide an established alternate site. Resources for establishing an alternate site shall be identified and made available for systems assessed as high impact for availability.

For IT systems with high impact availability, a full-scale test of the contingency plan is preferred. In a full-scale test, the triggering incident shall be simulated, but the detection, containment, and recovery steps shall be executed in accordance with the plan. This test shall include coordination with the alternate site. The following objectives shall be achieved:

1. The test demonstrates that the system can be brought to an operational condition at the designated alternate site by following the procedures and instructions described in the plan.

2. It is important that the plan draw only on resources that are normally located away from the site where the incident occurs.

3. The test verifies that the organizational units responsible for the contingency plan fully understand their responsibilities and are able to carry them out in a timely manner.

4. The test verifies that the system is brought to an operational condition within the allotted recovery time.

5. The test verifies that system information is restored to the expected state, so that operations can resume in a synchronized manner.

6. The test verifies that access to the system information by authorized business area personnel has been reestablished.

In circumstances that preclude a full-scale test, a rigorous tabletop exercise, with a planned follow-on for a full test, shall provide an acceptable alternative. The tabletop exercise is described below in the section on moderate impact IT systems.

3.9.8.2 Systems with Moderate Impact for Availability — Testing required

For IT systems with moderate impact availability, a full-scale test of the contingency plan shall be encouraged, but not required. A tabletop exercise shall be acceptable for most moderate impact systems. The most important elements are that the actual individuals involved in the recovery process are involved in the exercise and that the exercise formally addresses all of the steps in the plan. The following objectives shall be achieved:

1. The exercise walks through the procedures and instructions described in the contingency plan.

2. Results for each step are simulated as rigorously as possible.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000114

3. The exercise makes reference only to personnel and other resources that will be located away from the site where the incident occurs.

4. The exercise requires each organizational unit to explain how they would carry out their responsibilities.

5. A timeline with reasonable times for events is used to illustrate that the system could be brought to an operational condition within the allotted system recovery time.

6. The exercise illustrates how access to the system information by authorized business area personnel would be reestablished.

7. The entire exercise is used as a tool to train the teams involved on their responsibilities during an emergency.

In a tabletop exercise, the triggering incident, detection, containment, and recovery are simulated. The contingency plan shall be used to walk though a prepared scenario in order to demonstrate how system recovery would be achieved. This exercise shall include personnel from the site(s) where the system would be recovered.

3.9.8.3 Systems with Low Impact for Availability — Testing optional

For IT systems whose availability is categorized as low impact, contingency plan testing is optional. As a minimum, the plan shall be reviewed and evaluated for feasibility every two years or whenever significant changes are made to the system. A memo shall be developed that indicates that "the system is a FIPS 199 low impact system; therefore, the system's contingency plan is not required to be tested."

The DHS *Certification and Accreditation (C&A) Guidance for SBU Systems: Users Manual* provides detailed information on developing the ST&E Plan within RMS.

3.9.9 Security Assessment Report

The Security Assessment Report (SAR) summarizes the results of the ST&E and the system's compliance with the defined security controls in the SSP. The findings in the SAR can state that the system is fully compliant with the stated SSP and risk assessment or can state that the testing could not verify the claims in the SSP and risk assessment. If the testing finds that the system is compliant with the SSP and risk assessment, but residual risk still remains, the SAR must document what risk and actions will result. The results of the ST&E (updated RTM) are attached to support the findings in the SAR.

A SAR template is available in RMS. The DHS *Certification and Accreditation (C&A) Guidance for SBU Systems: Users Manual* provides detailed information on developing the SAR within RMS.

3.9.10 Authorization to Operate Letter

The Authorization to Operate (ATO) letter or Denial to Operate letter is generated based upon the decision of the Authorizing Official (AO). The AO is given the accreditation package to review.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000115

A notebook for the AO's signature containing a printed copy of the C&A documentation must include the following documents.

1. Security Categorization (FIPS-199 Assessment)
2. Risk Assessment
3. System Security Plan (SSP)
4. Contingency Plan
5. Privacy Impact Assessment (PIA)
6. e-Authentication
7. Security Test and Evaluation (ST&E) Plan
8. Contingency Plan Test Results
9. Interconnection Security Agreement, if applicable
10. Security Assessment Report (SAR)/Security Certification Statement
11. Plan of Action and Milestones (POA&M)
12. Security Accreditation Letter (ATO)
13. Self-Assessment (NIST SP 800-53)

For operational systems, the AO makes a risk-based decision either to grant full authorization to operate or deny authorization to operate. Authorizations to operate certified and accredited systems can be granted for a maximum period of three (3) years. Should CBP require a system to operate in a production environment for six (6) months or less an ATO accreditation period waiver from the DHS CISO is required. For development testing or for prototype systems, the AO may grant an interim authorization to operate (IATO). An interim authorization provides a limited authorization to operate the IT system under specified terms and conditions and acknowledges greater risk to the organization's operations and assets for a limited period of time. A system undergoing development testing or a prototype system is *not* considered accredited during the period of limited authorization to operate.

Subsequent to the Key Decision Point 3 of the life cycle development and/or prior to allowing a system to become operational, the AO must sign a formal ATO letter authorizing the system for operation in the DHS environment.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000116

Decision	Criteria
Full Authorization to Operate (ATO)	After assessing the results of the security certification, if the Authorizing Official (AO) accepts the residual risk to the CBP's operations or assets, a full authorization to operate is issued for the IT system. The information system is accredited without any significant restrictions or limitations on its operation.
Interim Authorization to Operate (IATO) (for systems in development testing and prototype systems only)	After assessing the results of the security certification, the Authorizing Official may issue an interim authorization to operate (IATO) for systems in development testing and prototype systems. The IATO authorizes operation of the information system for up to 6 months. During this period, the effectiveness of security controls must be closely monitored. If the AO has not officially accredited the testing or prototype system by the end of the IATO, the AO may grant a second and final IATO for a period of up to 6 months. The information system must be fully accredited by the end of the second IATO in order for it to receive a full ATO and become operational.
Denial of Authorization to Operate	After assessing the results of the security certification, if the AO finds that the residual risk to the CBP's operations or assets is unacceptable, the authorization to operate the IT system is denied. The IT system is not accredited and should not be placed into operation. For an IT system currently in operation, all activity should be halted.

The Plan of Action and Milestones (POA&M) is another part of the accreditation package. Weaknesses that will be accepted and not mitigated are documented in the final SAR and agreed to by the AO prior to operation. Any weakness that is to be mitigated as part of the accreditation process must be documented in a Plan of Action and Milestones (POA&M). The POA&M documents the weaknesses of a system and the corrective actions that must be taken to address those weaknesses. The POA&M serves as a management tool for addressing and resolving security-related weaknesses. It details resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates. .For detailed guidance on the DHS POA&M process consult the POA&M Process Guide (Attachment H), or contact the DHS Compliance Help Desk (b)(6) (b)(7)(C).

The AO reviews the package and the Certifying Official's recommendation. In authorizing a system, the AO can stipulate conditions on the accreditation (e.g., certain POA&M activities may need to be completed within a specific timeframe, or additional compensating controls may need to be implemented). The AO writes the ATO letter (including any conditions) or Denial to Operate letter, signs the letter, and forwards it to the Certifying Official and System Owner.

The DHS *Certification and Accreditation (C&A) Guidance for SBU Systems: Users Manual* provides detailed information on the accreditation phase and on the ATO letter.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000117

3.9.11 Annual Self-Assessments

NIST Special Publication 800-53 Revision 2, *Recommended Security Controls for Federal Information Systems*, provides the IT security requirements that the DHS Information Security Program must satisfy for the FISMA annual review requirements. NIST SP 800-53 provides guidance for selecting and specifying security controls for information systems.

For FY 2008 and beyond, FIPS 200/NIST SP 800-53 must be used for the specification of security controls, and NIST SP 800-53A must be used for the assessment of security control effectiveness and for the annual FISMA reporting.

The annual assessments are performed within the Continuous Monitoring Phase of the accreditation, the purpose of which is to provide ongoing oversight and monitoring of the security controls in the IT system and to inform the authorizing official or designated representative when changes occur that may impact the security of the system. During this phase, the status of the IT system is monitored to ensure that residual risk is kept within an acceptable level, and any significant changes to the system configuration or to the operational/threat environment that might affect system security are identified. CBP must re-accredit their IT systems every 3 years or whenever a major change occurs, whichever occurs first.

TAF addresses the annual self-assessments.

3.10 IT Security Review and Assistance

The Federal Information Security Management Act of 2002 (FISMA) requires that a thorough review of the DHS Information Security Program be conducted on an annual basis. This review must include a report on the degree to which security requirements have been implemented, significant deficiencies discovered, remedial actions taken or in progress to correct deficiencies, and level of compliance with NIST standards. Attachment E provides detailed information on the required FISMA reporting, including use of the mandated TrustedAgent FISMA (TAF) automated COTS tool. (https://tafisma.dhs.gov/).

Policy ID	CBP Policy Statements	Relevant Controls
3.10.a	Submit CBP information security policies to the DHS CISO for review.	PL-1
3.10.b	Establish an Information Security Review and Assistance Program.	CA-7, PL-1
3.10.c	Conduct reviews in accordance with FIPS 200/NIST SP 800-53, for specification of security controls. NIST SP 800-53A must be used for the assessment of security control effectiveness and for quarterly and annual FISMA reporting.	CA-7, PL-1
3.10.d	The DHS CISO shall conduct information security review and assistance visits throughout the Department in order to monitor the CBPs' security program compliance with DHS policies and procedures.	CA-2

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000118

Information security review and assistance responsibilities are provided below.

IT Security Review and Assistance Responsibilities
DHS CIO • Designates a full-time CISO. • Prepares the annual Congressional information security compliance report as required by FISMA. **DHS CISO** • Coordinates and prepares for the annual DHS Inspector General review of the Information Security Program. • Reviews and approves all DHS information security policies. • Establishes and implements an Information Security Review and Assistance Program. • Prepares and distributes a review and assistance handbook based on applicable NIST guidance. **DHS Compliance and Oversight Program Director** • Develops and implements a compliance review and assistance program. **CISO** • Implement an Information Security Review and Assistance Program at the CBP level. • Schedule information security review and assistance visits and ensure these visits are completed. • Provide trained personnel to participate in review and assistance visits. • Coordinate with ISSOs and provide guidance and oversight in identifying and documenting deficiencies and prioritizing them based on missions, risk, and funding. • Review and monitor Plans of Actions and Milestones (POA&Ms). • Ensure POA&M updates to the TrustedAgent FISMA database are timely (i.e., by March 10, June 10, September 15, and December 10 annually) • Coordinate issues with the Compliance and Oversight Program Director. • Generate candidate information security policies, as the need arises, for CISO review and approval. • Review NIST and other directives for applicability to the DHS Information Security Program. **ISSOs** • Prepare security self-assessment documentation as directed by the CISO. • Identify personnel qualified to participate in review and assistance visits. **System Owners** • Ensure that ISSOs have access to resources adequate for conducting self-assessments and review and assistance visits. • Implement corrective actions for deficiencies found during self-assessments. **Site Managers** • Ensure that adequate personnel resources are available to participate in site assistance visits.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000119

3.10.1 Review and Assistance Management and Oversight

The scope and complexity of the requirements necessary for the implementation and management of a successful IT security program requires active participation and oversight by a senior CBP official with a staff of qualified security professionals. In CBP, the senior security manager is the CISO. This individual is appointed in writing by the Commissioner, reviews and approves policy for the IT security program, oversees the CBP Information security assistance program, and prepares the annual assessment report.

3.10.2 Information Security Assistance

To the maximum extent practicable, CBP shall provide on-site assistance to DHS organizations in accordance with the Information Security Review and Assistance Program implemented by the DHS CISO. The CISO shall coordinate with ISSOs and provide guidance and oversight in identifying deficiencies and prioritizing them based on missions, risk, and funding. The size and the geographic dispersion of DHS offices and organizations require close coordination and planning between the DHS CISO, CISO, and ISSOs. Active support by site personnel and automated system development teams is imperative for the success of the assistance program.

3.10.3 IT Security Reviews

NIST Special Publication 800-53*, Recommended Security Controls for Federal Information Systems*, has served as the basis for reviewing and evaluating the DHS Information Security Program and has helped satisfy the FISMA program review requirements. For FY 2008 and beyond, FIPS 200/NIST SP 800-53 will be used for the specification of security controls, and NIST SP 800-53A will be used for the assessment of security control effectiveness and for the annual FISMA reporting. System and site ISSOs have primary responsibility for completing the annual review and reporting results to senior management in accordance with the procedures established by the CISO. The CISO monitors ISSO performance, provides updates to the TrustedAgent FISMA database, and interacts with the DHS Compliance and Oversight Program Director.

3.11 Security Working Groups and Forums

Working groups and other forums representing various functional areas convene on a regular basis. Once the DHS information security organization has been formalized and staffed, various working groups and forums such as those listed below will be established:

- DHS CISO Board
- DHS Information Security Training Working Group.

DHS senior security management officials such as the DHS CISO and CISO will utilize the experience offered by the organizations coming together to form the new Department to decide the composition and missions of security working groups, forums, and committees. At that time charters detailing the roles and responsibilities of these new groups will be prepared and specific requirements will be included in this handbook.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000120

3.11.1 DHS Chief Information Security Officer (CISO) Council

The DHS Chief Information Security Officer (CISO) Council is chaired by the DHS CISO. Its membership consists of Component CISOs and Component Information System Security Managers (ISSMs). The CISO Council will consider a broad range of IT security matters of importance to the DHS IT Security Program and is a decision-making body.

Policy ID	CBP Policy Statements	Relevant Controls
3.11.1.a	The CBP CISO shall actively participate in the DHS CISO Board.	PL-1
3.11.1.b	The CBP CISO shall ensure that the DHS CISO is kept apprised of all pertinent matters involving the security of IT systems.	PL-1
3.11.1.c	The CBP CISO shall ensure that security-related decisions and information, including updates to the 4300 series of security publications, are distributed to the ISSOs and other appropriate persons.	PL-1

3.11.2 DHS Information Security Training Working Group

The DHS Information Security Training Working Group is established to promote collaboration on information security training efforts throughout the Department and to share information on CBP-developed training activities, methods, and tools, thereby saving costs and avoiding duplication. The Information Security Training Working Group is chaired by the DHS Program Director for Information Security Training.

Policy ID	CBP Policy Statements	Relevant Controls
3.11.2.a	A representative shall be appointed to the DHS Information Security Training Working Group.	---
3.11.2.b	CBP members shall actively participate in the DHS Information Security Training Working Group.	---
3.11.2.c	Each representative shall be responsible for managing the CBP information security training program.	---

3.12 CBP Information Technology Security Policy Review Board

The CBP ITSPRB is chaired by a member of the Security and Technology Policy Team. Its membership consists of individuals from the CBP security area and program offices. Its purpose is to provide a mechanism to receive IT security policy issues, conduct analysis, interpret policy and propose revisions to this handbook.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000121

Policy ID	CBP Policy Statement	Relevant Controls
3.12.	OIT elements shall designate representatives to the Information Technology Security Policy Review Board.	---

3.13 CBP Information Systems Security Officer Working Group

The CBP Information System Security Officer (ISSO) Working Group is chaired by a member of the Security and Technology Policy Team. Membership of this working group includes CISO, the Regional ISSO Lead and ISSOs from all regions within CBP. The purpose of this working group is to work directly with end users and field and station organizational units to negotiate CBP policy compliance.

Policy ID	CBP Policy Statement	Relevant Controls
3.13.	ISSOs are tasked verifying compliance and oversight of DHS and CBP policies.	---

3.14 Information Security Policy Violation and Disciplinary Action

Individual accountability is a cornerstone of an effective security policy. CBP heads are responsible for taking corrective actions when security incidents and violations occur and for holding personnel accountable for intentional transgressions. CBP must determine how to best address each individual case.

An information security violation may result in disclosure of sensitive information to unauthorized individuals or in unauthorized modification or destruction of system data, loss of computer system processing capability, or loss or theft of any computer system resources. Information security violations also include a failure to adhere to DHS or CBP policy with respect to inappropriate use of CBP computer resources. The SOC is normally responsible for initiating any disciplinary action following investigation of a security event by notifying appropriate law enforcement authorities, who pursue the investigation and recommend disciplinary action, if required.

Policy ID	CBP Policy Statements	Relevant Controls
3.14.a	Information security-related violations are addressed in the CBP Security Policy and the *Standards of Ethical Conduct for Employees of the Executive Branch*, and CBP employees may be subject to disciplinary action for failure to comply, whether or not the failure results in criminal prosecution.	PS-8
3.14.b	Non-DHS Federal employees or contractors who fail to comply with DHS and CBP security policies are subject to having their access to CBP IT systems and facilities terminated, whether or not the failure results in criminal prosecution.	PS-8
3.14.c	Any person who improperly discloses sensitive information is subject to	PS-8

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000122

Policy ID	CBP Policy Statements	Relevant Controls
	criminal and civil penalties and sanctions.	

Information security policy violation and disciplinary action responsibilities are provided below.

Information Security Policy Violation and Disciplinary Action Responsibilities
Users • Be aware of information security policies described in this handbook and in other references provided by DHS or CBP security officials. • Be aware of and understand the disciplinary actions associated with violations of information security policy.

3.15 Required Reporting

The Federal Information Security Management Act (FISMA) requires that the status of the DHS Information Security Program be reported to the Office of Management and Budget on a recurring basis. Quarterly reports and an annual summary report are submitted by the DHS Office of the CISO, Office of Information Security (OIS) to OMB. Using the TrustedAgent FISMA automated tool, CBP shall update status information on a continual basis. This data is collected by OIS and compiled for the FISMA report and for other status reports. See Attachment E for information on FISMA Reporting and Attachment H for the POA&M Process Guide.

Policy ID	CBP Policy Statements	Relevant Controls
3.15.a	Collect and submit quarterly and annual information security program status data as required by FISMA.	CA-4
3.15.b	Utilize the automated tool approved for use by the DHS CISO.	CA-4

Note: CBP shall utilize the TrustedAgent FISMA (TAF) product when reporting Information Security Program status information to the OIS.

FISMA reporting responsibilities are provided below.

FISMA Reporting Responsibilities
CISO/ISSO • Ensure that the TAF automated tool is utilized for required reporting. • Ensure that C&A artifacts (e.g., Privacy Impact Assessment, System Security Plan, Security Test & Evaluation Report, Contingency Plan Test Results, Risk Assessment, ATO letter) are uploaded into TAF.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000123

3.16 Privacy and Data Security

The DHS Privacy Office is responsible for privacy compliance across the Department including assuring that technologies used by the Department sustain and do not erode privacy protections relating to the use of personal and Department information. The DHS Chief Privacy Officer has exclusive jurisdiction over the development of policy relating to personally identifiable information (PII). The CBP Privacy Office is responsible for privacy compliance across CBP, including assuring that technologies used sustain and do not erode privacy protections relating to the use of personal and CBP information.

Various regulations place restrictions on the Government's collection, use, maintenance, and release of information about individuals. Regulations also place requirements on agencies to protect personally identifiable information, which is defined as information in a system or online collection that directly or indirectly identifies an individual regardless of whether or not the the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to CBP. An example of PII is information that can be used to distinguish or trace an individual's identity, such as their name, Social Security number, date and place of birth, mother's maiden name, biometric records). Also considered PII is information about an individual's education, financial transactions, medical history, and criminal or employment history are examples of PII.

A privacy threshold analysis (PTA) provides a high level description of an information system including the information it contains and how it is used. The PTA is used to determine and document whether or not a PIA and/or System of Record Notices (SORN) are required. A PIA is a publicly released assessment of the privacy impact of an information system and includes an analysis of the PII that is collected, stored, and shared. A SORN describes the categories of records within a system of records and describes the routine uses of the data and how individuals can gain access to records and correct errors.

3.16.1 Personally Identifiable Information

OMB M-06-16, Protection of Sensitive Agency Information, requires that agencies protect personally identifiable information (PII) that is physically removed from the Department location or that is accessed remotely. Physical removal includes both removable media as well as media within mobile devices (i.e., laptop hard drive).

PII is defined as any information that permits the identity of an individual to be directly or indirectly inferred, including any other information that is linked or linkable to that individual regardless of whether the individual is a United States citizen, legal permanent resident, or a visitor to the U.S., or employee or contactor to CBP.

Sensitive PII is PII which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Examples of Sensitive PII include Social Security numbers, alien number (A-number), criminal history information, and medical information. Sensitive PII requires stricter handling guidelines due to the sensitivity of the information. For more information on handling Sensitive PII see: *Handbook for Safeguarding Sensitive Personally Identifiable Information at the Department of Homeland Security.*

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000124

General policies relating to personally identifiable information are provided below. Additional PII-related policies are included in the following sections:

1. Section 3.9: Certification and Accreditation, Remediation, and Reporting. For systems involving personally identifiable information, the confidentiality security objective shall be assigned an impact level of at least moderate.

2. Section 4.8.3: Laptop Computers and Other Mobile Computing Devices. All information stored on any laptop computer or other mobile computing device is to be encrypted using encryption that is FIPS 197 compliant and has received FIPS 140-2 validation.

3. Section 5.2.2: Automatic Session Lockout. Sessions on workstations and on laptop computers and other mobile computing devices are to be terminated after 20 minutes of inactivity.

4. Section 5.3: Auditing. DHS defines computer-readable data extracts as data removed from any C&A'd system where the process is not covered by the SSP and computer-readable data extracts are stored on hard drives, including desk top and laptop computers, floppy disks, compact discs (CDs), digital video disks (DVDs), USB drives, memory cards, and any other media that may be read or copied electronically.

5. Section 5.4.1: Remote Access and Dial-in. Remote access of personally identifiable information must be approved by the AO. Strong authentication via virtual private network (VPN) or equivalent encryption (e.g., https) and two-factor authentication is required. Remote access should only be allowed with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access. Restrictions are placed on the downloading and remote storage of personally identifiable information accessed remotely, as noted below in the CBP Policy.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000125

Policy ID	CBP Policy Statements	Relevant Controls
3.16.1.a	PII shall not be physically removed from a CBP facility without written authorization from the system AO or person designated in writing by the AO or in accordance approved SOPs for handling of computer-readable data extracts.	PL-5
3.16.1.b	PII removed from a CBP facility on removable media shall be encrypted, unless the information is being sent to the individual as part of a Privacy Act or Freedom of Information Act (FOIA) request.	PL-5
3.16.1.c	If PII can be physically removed from an IT system (printouts, CDs, etc), the System Security Plan shall document the specific procedures, training, and accountability measures in place to ensure remote use of the data does not bypass the protections provided by the encryption.	PL-5
3.16.1.d	Systems that as part of routine business remove PII from one IT system should address in the system security plan the risks associated with this removal as part of the system security plan and attach standard operating procedures to mitigate the risk. Computer-readable data extracts not included within the boundaries of a system accreditation must be logged and deleted after 90 days unless the extract is required beyond the 90 days.	PL-5

DHS Privacy Office has published official DHS guidance regarding the requirements and content for PTAs, PIAs, and SORNs. Privacy Compliance Guidance can be found on the DHS Privacy Office website at www.dhs.gov/privacy.

3.16.2 Privacy Threshold Analyses

The PTA provides a high-level description of the system, including the information it contains and how it is used. PTAs are required whenever a new IT system is being developed or an existing system is significantly modified. PTAs are the responsibility of the System Owner and the IT Program Manager as part of the system lifecycle process. The Component Privacy Officer or PPOC reviews the PTA and forwards it to the DHS Privacy Office, who determines whether a PIA and/or SORN are required. PTA artifacts expire after three (3) years. DHS MD 0470.2 defines the requirements for the PTA.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000126

Policy ID	CBP Policy Statements	Relevant Controls
3.16.2.a	A PTA shall be conducted as part of new IT system development or whenever an existing system is significantly modified.	PL-5
3.16.2.b	A PTA shall be conducted when an IT system undergoes C&A.	---
3.16.2.c	The CBP and DHS Chief Privacy Officer shall evaluate the PTA and determine if it is a Privacy Sensitive System and if the system requires a PIA and SORN.	PL-5
3.16.2.d	Information system shall not be designated operational until the CBP and DHS Privacy Office approves the PTA.	PL-5
3.16.2.e	For systems containing PII, the **confidentiality** security objective shall be assigned an impact level of moderate or higher.	RA-2

PTA responsibilities are provided below.

Privacy Threshold Analyses Responsibilities
DHS Chief Privacy Officer • Review and approve the PTA. • Determine whether a system is a Privacy Sensitive System. • Determine whether a PIA and/or SORN are required. • Upload validated PTAs to TAF. **System Owner** • Submit the PTA to the CBP Privacy Officer and provide any additional information required by the DHS Chief Privacy Officer to assist in the PTA process. **Privacy Officer** • Review and submit the PTA for approval and provide any additional information required by the DHS Chief Privacy Officer to assist in the PTA process. PTAs are to be emailed to PIA@dhs.gov for validation by the DHS Privacy Office.

3.16.3 Privacy Impact Assessments

A PIA is a publicly released assessment of the privacy impact of an information system and includes an analysis of the PII that is collected, stored, and shared. PIAs are required (as determined by the PTA) whenever a new IT system is being developed or an existing system is significantly modified. PIAs are the responsibility of the System Owner and the IT Program Manager as part of the system lifecycle process. OMB Memorandum M-03-22, DHS MD 0470.1, and the *Official DHS Privacy Impact Assessment Guidance* discuss the requirements for conducting PIAs at DHS.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000127

Policy ID	CBP Policy Statements	Relevant Controls
3.16.3.a	PIA (as determined by the PTA) as part of new IT system development or whenever an existing system is significantly modified.	PL-5
3.16.3.b	Information systems that the CBP and/or DHS Privacy Office has determined require a PIA (as determined by the PTA) shall not be designated operational until the CBP and DHS Privacy Office approves the PIA for that system.	PL-5

PIA responsibilities are provided below.

Privacy Impact Assessment Responsibilities
DHS Chief Privacy Officer • Review IT systems for privacy concerns. Identify mitigation strategies for privacy risks and document risks and mitigations in the approved PIA. • Approve all PIAs. • Upload validated PIAs to TAF. **System Owner** • Draft accurate and complete PIA using the DHS approved template. • As part of the PIA identify privacy risks and mitigation strategies. • Submit the draft PIA to the Privacy Officer for review and comment. **Privacy Officer** • Review draft PIAs for possible privacy risks and mitigation strategies and work with system owners to address any privacy considerations associated with the system. • Submit the complete and accurate PIA for DHS Chief Privacy Officer review and approval. • Include CBP counsel in review of PIAs to ensure legal compliance.

3.16.4 Systems of Records Notices

The Privacy Act of 1974 requires a system of records notice (SORN) when PII is maintained by a Federal agency in a "system of records" and the PII is retrieved by a personal identifier. IT Systems that are considered a "system of record" may not be designated operational until a SORN has been published in the *Federal Register* for thirty days. The Office of Management and Budget, specifically *Privacy Act Implementation, Guidelines and Responsibilities*, July 9, 1975, and *Circular A-130* including *Appendix I*, DHS MD 0470.2, and *Official DHS Guidance on System of Records and System of Records Notices* are the benchmark references when developing SORNs.

A "system of records" means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. The term "system of records" is not synonymous with an IT system, so it is possible to have one IT system with multiple "system of records" or multiple IT systems covered by one "system of records".

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000128

OMB requires each SORN to be reviewed every two (2) years to ensure that it accurately describes the system of records. CBP shall review and republish SORNs every two (2) years (this process is called the Biennial SORN Review Process) as required by OMB A-130. DHS Privacy Office works with CBP to ensure that SORN reviews are conducted every two (2) years following publication in the Federal Register.

Policy ID	CBP Policy Statements	Relevant Controls
3.16.4.a	A SORN is required when PII is maintained by a Federal agency in a system of records where information about an individual is retrieved by a unique personal identifier.	---
3.16.4.b	Information systems containing PII shall not be designated operational until a SORN has been published in the Federal Register for thirty (30) days.	CA-6
3.16.4.c	A SORN must be reviewed every two years to ensure that it accurately describes the system of records.	---

3.16.5 Protecting Privacy Sensitive Systems

OMB M-06-16, *Protection of Sensitive Agency Information* requires that agencies protect PII that is physically removed from Department locations or that is accessed remotely. Physical removal includes both removable media as well as media within mobile devices (i.e., laptop hard drive).

Please refer to the following documents for additional information and policies on protecting PII and Sensitive PII at DHS:

- *Handbook for Safeguarding Sensitive Personally Identifiable Information at the Department of Homeland Security*;
- 4300 A, Attachment S, *Compliance Framework for Privacy Sensitive Systems*; and
- *DHS Policy and Procedures for Managing Computer-Readable Extracts Containing Sensitive PII*.

Policy ID	CBP Policy Statements	Relevant Controls
3.16.5.a	Sensitive PII contained within a non-routine or ad hoc Computer-readable extract (CRE) [e.g. CREs not included within the boundaries of a source system's written system security plan (SSP)] shall not be removed, physically or otherwise, from a DHS facility without written authorization from the Data Owner and in accordance with the *DHS Guide to Managing Computer-readable Extracts Containing Sensitive PII*. 1. Ad hoc CREs must be approved by the Data Owner. 2. Ad hoc CREs must be documented, tracked, and validated every ninety	---

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000129

Policy ID	CBP Policy Statements	Relevant Controls
	(90) days after their creation to ensure either continued authorized use or that they have been appropriately destroyed or erased in accordance with the *DHS Guide to Managing Computer-Readable Extracts Containing Sensitive PII*.	
3.16.5.b	PII and Sensitive PII removed from a DHS facility on removable media, such as CDs, DVDs, laptops, PDAs, shall be encrypted, unless the information is being sent to the individual as part of a Privacy Act or Freedom of Information Act (FOIA) request.	---
3.16.5.c	If PII and Sensitive PII can be physically removed from an IT system (e.g., printouts, CDs, etc), the SSP shall document the specific procedures, training, and accountability measures in place to ensure remote use of the data does not bypass the protections provided by the encryption.	---
3.16.5.d	Systems that, as part of routine business, remove Sensitive PII in the form of a computer-readable extract, e.g., routine system-to-system transmissions of data (routine CREs) should address in the SSP the risks associated with this removal as part of the SSP. 1. Data Owners[2] shall ensure that routine CREs are carried out with appropriate oversight, security, and diligence to ensure that Sensitive PII is protected and that CREs are used and destroyed in accordance with the *DHS Guide to Managing Computer-Readable Extracts Containing Sensitive PII* and other established policies and procedures. 2. Routine CREs must be appropriately secured during storage and transmission in accordance with the *Handbook for Safeguarding Sensitive Personally Identifiable Information at the Department of Homeland Security*.	---
3.16.5.e	CREs shall be erased within 90 days unless the information included in the extracts is required beyond the 90 days. Permanent erasure of the extracts or the need for continued use of the data shall be documented by the System Owner and audited periodically by the Component Privacy Officer or PPOC.	---

3.16.6 Privacy Incident Reporting

Reporting of privacy incidents and incidents that may involve PII are a special case, subject to strict reporting standards and timelines based on requirements outlined in OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*.. These types of incidents are reported using the Privacy Event Notification (PEN).

[2] *For the purposes of this section and subsequent sections referencing computer-readable extracts, the Data Owner refers to the agency, program or office that has responsibility for and the authority to determine the allowable uses of the data sought as part of a routine or ad hoc CRE. With some systems the Data Owner may also be the Program Manager, Business Owner or System Owner.*

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000130

Policy ID	CBP Policy Statements	Relevant Controls
3.16.6.a	All suspected or confirmed privacy incidents must coordinated with the Privacy Office and the CISO to evaluate and subsequently report the incident to the DHS EOC. The DHS EOC will then transmit the report to the US-CERT within one (1) hour.	---
3.16.6.b	The Privacy Officer, in cooperation with the CISO, shall jointly evaluate the incident, but the CISO is responsible for reporting the incident to the CSIRC/SOC.	---
3.16.6.c	CBP personnel must also report suspected or confirmed privacy incidents or incidents involving PII to their Program Manager immediately upon discovery/detection, regardless of the manner in which it might have occurred.	---
3.16.6.d	CBP shall follow the *DHS Privacy Incident Handling Guide*.	---

Privacy Incident Reporting responsibilities are provided below.

Privacy Incident Reporting Responsibilities
CBP Personnel • Provides notification of incident to Program Manager
Program Manager • Prepares preliminary privacy incident report and passes report to the CISO or CSIRC/SOC
CISO/CSIRC/SOC • Evaluates Privacy Incident; Prepares and Submits Incident Report in SOC Online Incident Handling System
DHS SOC • Notifies Chief Privacy Officer, CISO, CIO and Dep. CIO; Processes and Transmits Privacy Incident Report to US-CERT.

3.16.7 E-Authentication

To ensure that online Government services are secure and protect privacy, some type of identity verification or authentication ("e-authentication") is needed. Each IT system must be evaluated as to whether e-authentication requirements apply. Only federated identity providers approved through the Federal CIO Council's Identity, Credentialing, and Access Management's (ICAM) Trust Framework Provider Adoption Process (TFPAP) should be used. Components should see www.IDmanagement.gov for details regarding the Federal Identity, Credentialing, and Access Management (FICAM) initiative.

E-authentication guidance is provided in the following:

- OMB M-04-04: E-Authentication Guidance for Federal Agencies, December 16, 2003
- NIST SP 800-63: Electronic Authentication Guideline, April 2006.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000131

See Section 3.9.3 (E-Authentication) for additional information.

Policy ID	CBP Policy Statements	Relevant Controls
3.16.7.a	Determine whether or not Government e-authentication security requirements apply to the systems allowing online transactions.	IA-2
3.16.7.b	Determine the appropriate assurance level for e-authentication by following the steps described in OMB M-04-04, *E-Authentication Guidance for Federal Agencies*.	IA-2
3.16.7.c	Implement the technical requirements described in NIST SP 800-63, *Electronic Authentication Guideline*, at the appropriate assurance level for those systems for which e-authentication requirements apply.	IA-2
3.16.7.d	System Owners shall ensure that each SSP reflects the e-authentication status of the respective system.	IA-2, PL-2
3.16.7.e	Programs considering the use of e-authentication are required to conduct a PTA to initiate the review of privacy risks and how they will be mitigated.	PL-5

3.17 DHS Chief Financial Officer – Designated Financial Systems

DHS CFO designated financial systems are systems that require additional management accountability and effective internal control over financial reporting. This section provides additional requirements for these systems based on OMB Circular A-123, *Management's Responsibility for Internal Control (A-123)* Appendix A. These requirements are in addition to the other security requirements established in this document and other CFO developed financial system Line of Business requirements. *Wherever there is a conflict between this and other sections of this policy regarding requirements for CFO designated financial systems, this section takes precedence.*

These additional requirements provide a strengthened assessment process and management assurance on the internal control over financial reporting. The strengthened process requires management to document the design and test the effectiveness of controls over financial reporting. The system owner is responsible for ensuring that all requirements, including security requirements, are implemented on CBP financial systems. The CISO must coordinate with the CFO's organization to ensure that these requirements are implemented.

Policy ID	CBP Policy Statements	Relevant Controls
3.17.a	System owners are responsible for ensuring that security assessments of key security controls (i.e., ST&E & SAR) for CFO Designated Systems are completed annually in TAF. This includes updating the ST&E & SAR annually.	CA-2, CA-7

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000132

Policy ID	CBP Policy Statements	Relevant Controls
3.17.b	The DHS CFO shall designate the financial systems that must comply with additional internal controls and the DHS Office of the CFO will review and publish this list during the fourth quarter of every fiscal year.	---
3.17.c	The CISO shall ensure that semi-annual vulnerability assessments and verification of critical patch installations are conducted on all CFO designated financial systems. Vulnerability assessment shall be performed during the second quarter of each fiscal year.	RA-5
3.17.d	All CFO designated financial systems shall be assigned a minimum impact level of "**moderate**" for confidentiality, integrity, and availability. If warranted by a risk based assessment, the integrity objective shall be elevated to "high."	RA-2
3.17.e	All security accreditations for CFO designated financial systems shall be approved and signed by the AO *and* by the CFO.	---
3.17.f	System owners are responsible for ensuring that Disaster Recovery (DR) plans are created for *all* CFO designated financial systems requiring high availability and that each plan is tested annually, no later than the third quarter of each fiscal year.	CP-2, CP-4
3.17.g	The CISO shall ensure that weekly incident response tracking is performed for all CFO designated financial systems.	IR-5
3.17.h	The CISO shall ensure that incidents related to CFO designated financial systems are reported to the CBP CFO.	IR-4, IR-6
3.17.i	System owners are responsible for ensuring that risk assessments for all CFO designated financial systems are updated at least annually.	RA-4
3.17.j	Financial application mission owners shall update CFO designated financial systems' System Security Plans (SSP) at least annually. Key controls that address the relevant assertions for a material activity shall be identified in the SSP.	PL-2
3.17.k	The CISO must request a waiver from the DHS CISO if a key control weakness is identified for a CFO designated financial system and not remediated within 12 months.	CA-5, CA-7
3.17.l	CFO shall ensure that a full-time dedicated ISSO is assigned to each CFO designated financial system. ISSOs should not be assigned collateral duties outside information security responsibilities. Designated financial system ISSOs may be assigned to more than one CFO designated financial system.	---
3.17.m	CFO designated financial system ATOs shall be rescinded if CBP fail to	CA-1, CA-6

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000133

Policy ID	CBP Policy Statements	Relevant Controls
	comply with testing and reporting requirements established within this policy.	
3.17.n	CBP CFO shall work with the CISO to approve any major system change to CFO designated financial system identified in the DHS inventory.	CA-1, CM-8

OMB A-123, Appendix A defines two types of system controls: Information Technology General Controls (ITGC) and Application Controls. This policy accounts for ITGCs which address structure, policies, and procedures that apply 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 the Line of Business processes.

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. Application controls, as defined by OMB A-123, which provide controls over input, processing, and output of data associated with individual applications are not addressed in this policy.

Key controls are defined as a control, or a set of controls, which address the relevant assertions for a material activity or significant risk. Key controls are required to be identified in system security plan and tested as part of an annual ST&E. System owners may perform rolling compliance tests that test other (non-key) controls annually and controls that were not tested in the previous years. Documentation and testing artifacts (see Table 3.18) for CFO designated financial systems will be tracked and captured through the DHS mandated RMS and TAF compliance systems. These requirements must be met within the specified timeframes. Failure to do so will result in the suspension of the systems' ATO.

Table 3.18: Documentation and Testing Artifacts

Artifact	Required Action	Frequency	Completion Deadline	Reporting Requirements
Risk Assessment (RA)	A complete RA shall be conducted	Annual	As determined by the CISO	Report no later than (NLT) Sep 30 of each year
System Security Plan (SSP)	The SSP shall be evaluated and updated	Annual	During first quarter of each FY	Report NLT Sep 30 of each year
Key Security Controls Security Assessment Results	Key security controls shall be evaluated and updated	Annual	During first quarter of each FY	Report completion NLT Dec 31 of each year
Disaster Recovery (DR) Plan Results	The DR plan shall be exercised	Annual	First quarter of each FY	Report completion NLT Dec 31 of each year
Vulnerability Assessment (VA)	A complete VA shall be conducted	Semi-Annual	One assessment completed during the first quarter	Report completion of one assessment

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000134

Artifact	Required Action	Frequency	Completion Deadline	Reporting Requirements
			of each FY; Second assessment completed during the third quarter.	NLT Dec 31; report completion of second assessment NLT Jun 30
Critical Patch Installation	Installation of critical patches shall be verified	Semi-Annual	As determined by the CISO	Report NLT Sep 30 of each year

3.18 Social Media

Social Media hosts are public, commercial, content sharing Web sites that allow individual users to upload, view and share content such as video clips, press releases, opinions and other information. The CBP and DHS Office of Public Affairs (OPA) will publish Terms of Service (TOS) and guidelines for posting to these sites. In some cases, CBP and/or DHS will develop its own and in other case will endorse those of other Federal agencies, such as GSA or OPM.

Policy ID	CBP Policy Statements	Relevant Controls
3.18.a	Only CBP OPA designated content managers may post content, and only those individuals designated by OPA for this purpose will be granted access on a continuing basis.	---
3.18.b	Posted content shall be in keeping with the CBP and DHS's Terms of Service (TOS) and guidelines for a given social media host (e.g., YouTube, Twitter, etc). This condition is also met if CBP and DHS endorses another appropriate Federal agency's guidance or TOS (e.g., GSA, OPM)	---
3.18.c	Content shall not be posted to any social media site with which the CBP and DHS has not approved and published final posting guidelines *and* TOS.	---
3.18.d	CBP Content managers shall review and understand the appropriate DHS-level Terms of Service (TOS) for the appropriate social media host.	---
3.18.e	CBP Content managers shall make a risk decision prior to posting any information and shall recognize that social medial hosts are not CBP or DHS information systems and therefore subject only to the CBP and/or DHS TOS and not to CBP and DHS policy. Information, once released is no longer under CBP control.	---

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000135

3.19 Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act of 1996 (HIPPA) addresses the privacy of individuals' health information by establishing a Federal privacy standard for health information and how it can be used and disclosed.

HIPAA prohibits the use or disclosure of protected health information (PHI) for any purpose other than treatment, payment, or health care operations without the authorization of the individual or as part of an exception within HIPAA.

CBP may collect PHI as part of its larger mission requirement. (e.g. law enforcement, targeting, etc.). This sub-section applies to all CBP systems and personnel who collect, process, or store PIH.

Policy ID	DHS Policy Statements	Relevant Controls
3.19.a	Any CBP system that collects, processes, or stores Protected Health Information (PHI) shall ensure that the stored information is appropriately protected and that access or disclosure is limited to the minimum required.	---
3.19.b	CBP shall work with the CBP Privacy Office and the DHS Privacy Office to ensure that privacy and disclosure policies comply with HIPPA requirements.	---
3.19.c	CBP shall ensure that employees with access to CBP systems that collect, process, or store PHI are trained on HIPPA requirements.	---
3.19.d	CBP shall establish administrative processes that can respond to complaints, requests for corrections of health information, and track disclosures of PIH.	---
3.19.e	When collecting PIH, CBP shall issue a privacy notice to individuals concerning the use and disclosure of their PIH.	---

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000136

4.0 OPERATIONAL CONTROLS

Operational Controls address security methods executed by users of information systems, which may include a business process owner, administrator, and users of information systems. These controls are put into place to improve the security of a group, particular system, or a group of systems by requiring a practice or standard of care. This section describes operational controls required in CBP.

4.1 Personnel

CBP systems face threats caused by the actions, either intended or accidental, of employees or vendor personnel. Individuals can harm or disrupt CBP systems or the facilities that host them. This may result in destruction or modification of data being processed, denial of service to the end users, or unauthorized disclosure of data. It is highly important that stringent safeguards be taken to reduce the risk associated with these types of threats.

4.1.1 Citizenship, Personnel Screening, and Position Categorization

CBP policy requires that only Government and contractor personnel who are U.S. citizens shall be granted access to CBP systems processing sensitive information. However, at times there is a need to grant access to non-U.S. citizens. The Commissioner or designee may grant access to CBP systems for non-CBP Government employees and/or non-U.S. citizens only when (1) the individual is a legal permanent resident of the United States or a citizen of Ireland, Israel, the Republic of the Philippines, or any nation on the Allied Nations List maintained by the Department of State, (2) all required security forms specified by the Government and any necessary background check have been satisfactorily completed, (3) a compelling reason exists for using this individual instead of a U.S. citizen, (4) the exception to the U.S. citizenship requirement is in the best interest of the U.S. Government, and (5) the DHS Chief Security Officer and the Chief Information Officer or their designees concur in approving access for the individual. CBP Attachment J provides an electronic form for requesting an exception to the U.S. citizenship requirement.

All personnel accessing CBP systems are required to have an appropriate security clearance and a valid need to know in order to access these systems. All CBP employees must have favorably adjudicated background investigations commensurate with the defined sensitivity level of the positions they hold. Determining the appropriate position sensitivity level is based on such factors as the type and degree of harm (e.g., disclosure of sensitive information, interruption of critical processing, computer fraud) the individual can cause through misuse of the computer system.

Another prudent safeguard is to ensure that individuals who support CBP systems are highly qualified technically and are adequately trained for the position they occupy. This can reduce the risk of unintentional actions. A major threat to an IT system can be the loss of key technical personnel. While unintentional acts and accidents cannot be eliminated, effective training can help to mitigate the possibility or frequency of unintentional user errors.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000137

Position sensitivity levels for all Government positions involving the use, development, operation, or maintenance of IT systems shall be designated, and risk levels for each contractor position shall be determined.

Table 4.1.1 provides the investigative requirements for CBP employees and contractors. Additional information on investigative requirements can be found on the Personnel Security Website at http://cbpnet.cbp.dhs.gov/xp/cbpnet/ia/bi/

Table 4.1.1: CBP Investigative Requirements

Type of Position	Initial Investigation	Required Forms*	Periodic Reinvestigation	Required Forms*
Critical Sensitive Positions (e.g., BPA, CBO, IA, Intel, Air and Marine)	SSBI BI (AG Specialist, Import Specialist	• SF-86 (3) • SF-87 (2) • CBP-258 (2) • FCRA (2)	**Conducted every 5 years: SSBI-PR – includes Subjects with Top Secret clearances PRI – includes AG Specialist and Subjects with Secret clearances	• SF-86 (3) • CBP-258 (2) • FCRA (1)
High Risk for Public Trust positions (e.g., HR Specialist, Budget Analyst, IT Specialist	BI	• SF-85P (3) • SF-85PS (3) • SF-87 (2) • CBP-257 (2) • FCRA (2)	**MBI conducted every 10 years: Periodic Reinvestigation for High Risk positions for Public Trust	• SF-85P (3) • SF-85PS (3) • CBP-258 (2) • CBP-257 (2) • FCRA (1)
Contractors	BI	• SF-85P (3) • SF-85PS (3) • CBP 258 (3) • CBP-257 (2) • FCRA (2) • Criminal History Request (D.C. employment only (2) • ADP Sheet (2) • Non-Disclosure Statements	**MBI Conducted every 10 years: Periodic Reinvestigation for Contractors	• SF-85P (3) • SF-85PS (3) • CBP-258 (2) • CBP-257 (2) • FCRA (1)
Similar Positions (NTEU) (e.g., Auditor/0511, Gen. Attorney/0905, Paralegal/0950)	BI	• SF-85P (3) • SF-85PS (3) • SF-87 (2) • FCRA (2)	**MBI conducted every 10 years: Periodic Reinvestigation for High Risk positions w/ restrictions	• SF-85P (3) • SF-85PS (3) • SF-87 (2) • FCRA (1)

* Number in parentheses for Required Forms includes the original and required copies, e.g., (3) = 1 original and 2 copies. **All copies must have the original signature.**

** A reinvestigation may be initiated outside the normal time frame should the Personnel Security Division receive information that raises a question concerning an employee's or contractor's continued suitability for employment.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000138

Policy ID	CBP Policy Statements	Relevant Controls
4.1.1.a	CBP shall designate the position sensitivity level for all Government and contractor positions that use, develop, operate, or maintain IT systems and shall determine risk levels for each contractor position. Position sensitivity levels shall be reviewed annually and revised as appropriate.	PS-2, PS-3, PS-7
4.1.1.b	CBP shall ensure incumbents in positions that use, develop, operate, or maintain IT systems shall have favorably adjudicated background investigations commensurate with the defined position sensitivity levels.	PS-2, PS-3, PS-7
4.1.1.c	All Federal employees shall have favorably adjudicated Background Investigation (BI) on file prior to being given full access to CBP systems. Background Investigations are defined in DHS MD 11050.2, *Personnel Security and Suitability Program* and CBP HB 1400-07, *Personnel Security Handbook.*	PS-3
4.1.1.d	No contractor personnel shall be granted access to CBP systems without having a favorably adjudicated Background Investigation (BI) as defined in DHS MD11055, *Suitability Screening Requirements for Contractor Employees.*	PS-3
4.1.1.e	Only U.S. Citizens shall be granted access to CBP systems processing sensitive information. Exceptions to the U.S. Citizenship requirement may be granted by the AO or designee with the concurrence of the Office of Security and the DHS CIO, in accordance with Section 1.10.4, U.S. Citizen Exception Requests.	PS-3
4.1.1.f	Personnel, who have favorably completed initial checks are permitted access to Local Area Networks (LANs), printers, electronic messaging, CBP Intranet and the Internet. However, the individual will not have full computer access until the investigation has been conducted and adjudicated. Access will be allowed to any For Official Use Only (FOUO) data, but not Law Enforcement Sensitive documents or data.	PS-3
4.1.1.g	With the consent of the business owner, access to certain administrative systems and shared drives is available to personnel who have successfully completed the initial BI checks as part of the BI process and who also possess written approval of their direct supervisor.	PS-3 AC-2
4.1.1.h	Non-CBP personnel who access CBP information systems and data (e.g., members of the trade community, local law enforcement, or emergency response personnel) must be identified. Access will be authorized through procedures that comply with CBP system access policies.	PS-3 AC-2
4.1.1.i	Non-CBP technical support personnel who are required to perform maintenance on CBP information systems within CBP-controlled facilities must be escorted at all times, unless they have been approved for unescorted access after having completed a BI.	MA-5

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000139

Policy ID	CBP Policy Statements	Relevant Controls
4.1.1 j	CBP personnel, including vendor personnel, shall receive periodic security awareness training (at least annually) in security practices and Rules of Behavior.	AT-3 PL-4

Responsibilities related to personnel issues are provided below.

Citizenship, Position Categorization, and Personnel Screening Responsibilities
Commissioner • Requests exceptions to the DHS requirement for U.S. citizenship for non-U.S. citizens who require access to CBP systems processing sensitive information. **System Owners** • Designate the position sensitivity level for all in-house or contractor positions that use, develop, or operate IT systems. **Security Managers** • Ensure all personnel who use, develop, or operate CBP IT systems have a favorably adjudicated background investigation commensurate with the defined sensitivity level associated with their position.

4.1.1.1 Background Investigations for Government Employees

CBP employees shall undergo the appropriate security investigations to obtain the needed clearances for their positions. The types of security investigations can be found in CBP HB 1400-07 Personnel Security Handbook. CBP's Office of Internal Affairs, Personnel Security Division (PSD) will initiate and adjudicate pre-employment and reinvestigations for CBP applicants, employees, and contractors. Position sensitivity designations within CBP are designated High Risk, Public Trust or Critical Sensitive National Security. Based on the position designation PSD will conduct either a Single Scope Background Investigation or a Background Investigation.

For more detailed information on Security Clearances and Background Investigations go to the Personnel Security Website at http://cbpnet.cbp.dhs.gov/xp/cbpnet/ia/bi/.

4.1.1.2 Background Investigations for Contractor Personnel

The level of BI required for contractor personnel accessing CBP IT systems is dependent on the level of risk associated with each contractor position: high, moderate, or low. The Table 4.1.1 depicts the investigative requirements for type of position. All CBP contractors must undergo a BI to determine suitability for employment.

4.1.2 Rules of Behavior

Rules of Behavior define the acceptable use of CBP-owned information systems and networks, and apply to all personnel and contractors using CBP information systems. Rules of behavior

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000140

that are understood and followed help ensure the security of systems and confidentiality, integrity, and availability of sensitive information. Rules of behavior inform users of their responsibilities and let them know they shall be held accountable for their actions while they are accessing CBP systems and using CBP IT resources that are capable of accessing, storing, receiving, or transmitting sensitive information. By its very nature, the CBP Information Security Policies and Procedures Handbook establish standards of use within the CBP computing environment, and as such, constitute a set of Rules of Behavior.

Policy ID	CBP Policy Statements	Relevant Controls
4.1.2.a	CBP shall define rules of behavior for all IT systems and ensure that users are trained regarding these rules and are aware of the disciplinary actions that may result from violating these rules.	PL-4
4.1.2.b	Users shall sign the rules of behavior prior to being granted IT accounts or access to any CBP IT systems or data.	AT-1, AT-2, PL-4

Rules of behavior responsibilities are provided below:

Rules of Behavior Responsibilities
System Owners • Develop and enforce rules of behavior for IT systems under their authority. **ISSOs** • Advise system owners concerning the establishment and implementation of a set of rules of behavior for CBP IT systems. • Ensure that rules of behavior for CBP general support systems and major applications are included or referenced in the System Security Plan. • Ensure users read and sign general rules of behavior regarding use of CBP systems and IT resources and rules of behavior specific to the CBP systems to which they will be given access. **Users** • Adhere to the general rules of behavior regarding the use of CBP systems and IT resources and to the system-specific rules of behavior for the IT system to which they have been granted access.

Rules of behavior must be developed for each automated information system and general support system. These rules must clearly delineate responsibilities and the expected behavior of all individuals with access to the system. As such, they form the basis for security awareness and training. The rules must state the consequences of inconsistent behavior or noncompliance. Rules of behavior must be in writing and must be made available for each user to read and sign before that user is granted access to the system.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000141

Rules of behavior for individual systems may be inherited from organizational rules or site rules of behavior (e.g. an individual LAN GSS rules of behavior may be automatically included as part of an organization-wide GSS rules of behavior to which all employees and staff are held accountable). The CBP general Rules of Behavior are detailed in Attachment G.

Annual security awareness training reinforces the understanding of CBP standards of use and the requirement to comply with policy. Enforcement actions of CBP Standards of Conduct are detailed in the Table of Offenses and Penalties, which includes security offenses and their associated disciplinary actions. Any person who is in noncompliance with the rules of behavior is subject to penalties and sanctions, including verbal or written warning, removal of system access for a specific period of time, reassignment to other duties, criminal or civil prosecution, or termination, depending on the severity of the violation. More information about these standards and the penalties associated with noncompliance or specific violations can be found on CBPnet using the following link:

http://www.cbp.gov/xp/cgov/careers/neo_kit/additional_info/standards_of_conduct/

For groups of individuals who may require elevated privileges within the CBP computing environment, additional Rules of Behavior may apply, as determined by system managers/owners and require additional approval/signature forms.

4.1.3 Access to Sensitive Information

Sensitive information is information that if lost, misused, or accessed or modified without authorization could adversely affect the national interest, the conduct of Federal programs, or the privacy to which individuals are entitled under the Privacy Act could be adversely affected.

To protect sensitive information and limit the damage that can result from accident, error, or unauthorized use, the principle of least privilege must be applied. The principle of least privilege requires that users be granted the most restrictive set of privileges (or lowest clearance) needed for performance of authorized tasks—i.e., users should be able to access only the system resources needed to fulfill their job responsibilities.

Principle of Least Privilege: Requires that a user be granted the most restrictive set of privileges (or lowest clearance) needed for performance of authorized tasks.

Application of this principle ensures that access to sensitive information is granted only to those users with a valid need to know.

Policy ID	CBP Policy Statement	Relevant Controls
4.1.3.a	System owners shall ensure that users of the IT systems supporting their programs have a valid requirement to access these systems.	AC-2

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000142

Access to sensitive information responsibilities are provided below.

Access to Sensitive Information Responsibilities
System Owners • Ensure users have a valid need to know prior to granting access to information contained in CBP IT systems. • Ensure users have the appropriate level of clearance prior to being granted access to sensitive IT resources. **ISSOs/System Administrators** • Ensure users have a valid requirement prior to being granted access to CBP IT systems. • Ensure users have the appropriate level of clearance prior to being granted access to sensitive IT resources.

Section 5.2, Access Control, provides implementation guidelines regarding access to sensitive information.

4.1.4 Separation of Duties

Separation of duties divides the steps in a critical function among different individuals. OMB Circular A-123, "Management Accountability and Control," requires that key duties and responsibilities in authorizing, processing, recording, and reviewing official agency transactions be separated among individuals. Managers should ensure that individuals do not exceed or abuse their assigned authority. No single individual should possess total control of the system's security mechanisms. In cases where strict separation of duties cannot be fully implemented, the ISSO should ensure compensating controls are in place.

Separation of duties is intended to prevent a single individual from being able to disrupt or corrupt a critical security process.

Policy ID	CBP Policy Statement	Relevant Controls
4.1.4.a	CBP shall divide and separate duties and responsibilities of critical IT system functions among different individuals to minimize the possibility that any one individual would have the necessary authority or systems access to be able to engage in fraudulent or criminal activity.	AC-2
4.1.4.b	All individuals requiring administrator privileges shall be reviewed and approved by the appropriate AO. The AO may delegate this duty to the appropriate system owner or Program Manager.	AC-2
4.1.4.c	Individuals requiring administrator privileges shall be assigned administrator accounts separate from their normal user accounts.	AC-6

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000143

Policy ID	CBP Policy Statement	Relevant Controls
4.1.4.d	Administrator accounts shall be used only for performing required administrator duties. All other functions not directly tied to administrator duties (checking email, accessing the Internet, etc) shall be performed through individuals' regular user accounts.	AC-6

Responsibilities related to separation of duties are provided below.

Separation of Duties Responsibilities
System Owners • Ensure personnel work assignments comply with CBP policy regarding separation of duties for sensitive IT systems. **ISSOs** • Ensure controls are in place that enforce compliance with CBP policy in regards to separation of duties. • Ensure compensating controls are in place for situations in which strict separation of duties cannot be fully implemented.

Assignment and segregation of system responsibilities must be clearly defined and documented for all CBP IT systems. Segregation of responsibilities, in addition to appropriate access controls, is intended to ensure that no individual has all necessary authority or information access to be able to engage in fraudulent activity without collusion. For this reason, it is essential that thorough and specific job descriptions be documented for every individual working with CBP IT systems and sensitive information.

An example of separation of duties is the separation of security duties on a network system. One individual would be responsible for backing up the system, another responsible for the physical access controls, and another responsible for the access privileges.

Whenever practical, the positions of security administrator and system administrator need to be filled by separate individuals. The same principle should also be applied to ISSO and system administrator positions. When having separate system and security administrators is not possible, the system administrator will be responsible for maintaining the system security configuration of systems, but will be subject to periodic audit/configuration review by the ISSO.

Note: If CBP does not have sufficient manpower resources necessary to meet strict separation of duties requirements, the AO may authorize exceptions provided that a shortage of personnel is formally identified as a residual risk and compensating controls have been put in place.

4.1.5 Information Security Awareness, Training, and Education

A key objective of an effective information security program ensures that each employee understands his or her role and responsibilities and is adequately trained to perform them. CBP cannot protect the confidentiality, integrity, and availability of its IT systems and the information

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000144

they contain without the knowledge and active participation of its employees in the implementation of sound security principles. Two components of this policy that assist CBP users are initial and annual refresher security awareness training. IT security-related roles also receive annual training commensurate with their responsibilities.

5 CFR part 930, subpart C, as revised, requires that all users (Federal employees as well as contractors) of Federal information systems must be exposed to security awareness materials at least annually. Additional to the annual training requirement, training will occur when employees are hired (they must receive the training before they are allowed access to systems), when system security changes occur, when an employee's work responsibilities change."

OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources, requires that persons be trained in their responsibilities and in the "rules of behavior" for using general support systems (e.g., LANs) and for using major applications before being given access to those systems or applications. Computer security training must be addressed in the security plan for each IT system. In addition, the CISO shall prepare and submit to the DHS IT Security Training Program Director a training plan outlining their plan for IT security awareness, training, and education for the year. The plan shall follow the guidance in the CBP Information Technology (IT) Security Awareness, Training and Education Plan template, issued by the DHS IT Security Training Office.

In 5 CFR Part 930, the Office of Personnel Management (OPM) requires Federal agencies to identify employees responsible for the management or use of computer systems that process sensitive information and to provide training to the following groups: executives; program and functional managers; information resources management (IRM), security, and audit personnel; automated data processing (ADP) management and operations personnel; and end users. It requires that employees in these groups receive their required training within 60 days of their appointment. It also requires that additional training be provided whenever there is a significant change in the Department's information security environment or procedures, or when an employee enters a new position involving the handling of sensitive information. It also requires that computer security refresher training be given as frequently as determined necessary by the Department based on the sensitivity of the information that the employee uses or processes.

The Federal Information Security Management Act of 2002 (FISMA) tasks the Chief Information Officer (or comparable official) of each agency with training and overseeing personnel with significant responsibilities for information security. Additionally, FISMA requires that each agency include security awareness training within an agency-wide information security program. Security awareness training must inform personnel, including contactors and other users of IT systems that support the operations and assets of the agency, of (1) information security risks associated with their activities and (2) their responsibilities in complying with agency policies and procedures so that such risks will be reduced. FISMA also requires each agency to include as part of its performance plan a description of the resources—including budget, staffing, and training—that are necessary to implement the program.

NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, provides Federal agencies with detailed guidelines for developing a robust training program for staff within 26 security-related roles. This document will be used to the extent that it is practical in developing and implementing awareness and training materials and courses for CBP employees and support contractors.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000145

Policy ID	CBP Policy Statements	Relevant Controls
4.1.5.a	CBP shall establish an appropriate Information Security Training Program for users of CBP systems.	AT-1
4.1.5.b	CBP personnel and contractors accessing CBP IT systems shall receive initial training and annual refresher training in security awareness and accepted security practices. Personnel shall complete security awareness within 24 hours of being granted a user account. If the user fails to comply, user access will be suspended.	AT-1, AT-4
4.1.5.c	CBP personnel and contractors with significant security responsibilities (e.g., ISSOs, system administrators) shall receive initial specialized training, and annual refresher training thereafter, specific to their security responsibilities.	AT-3
4.1.5.d	CBP shall maintain training records, to include name and position, type of training received, and costs of training. IT awareness training must be completed before IT accounts are authorized.	AT-4
4.1.5.e	Unless a waiver is granted by the CISO, user accounts and access privileges, including access to email, shall be disabled for those CBP employees who have not received annual refresher training.	AT-1
4.1.5.f	CBP shall prepare and submit an annual training plan, outlining their plans for Information Security Awareness, Training and Education. This plan shall follow the guidance in the CBP Information Technology (IT) Security Awareness, Training and Education Plan template, issued by the DHS Information Security Training Office.	AT-1
4.1.5.g	a. CBP shall prepare and submit Information security awareness, training, and education statistics to the DHS Information Security Training Program Director on a quarterly basis. These statistics shall include: • Total number of personnel and number of personnel that have received awareness training. • Total number of personnel with significant security responsibility and the number that have received role-based training. • The cost of any Department-provided information security training or materials for the year. CBP shall account for Contingency Plan Training, and Incident Response Training conducted for Moderate and High IT Systems. CBP must also provide: • Brief descriptions of the awareness and training provided to personnel. Information concerning how they have explained policies relating to Peer-to-Peer (P2P) file sharing to all system users.	AT-1

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000146

Policy ID	CBP Policy Statements	Relevant Controls
4.1.5.h	CBP shall provide evidence of training by submitting copies of training schedules, training rosters, training reports, etc., upon request of the DHS IT Security Training Office, or during onsite validation visits performed on a periodic basis.	AT-4
4.1.5.i	Training plans shall include awareness of internal threats and basic IT security practices.	AT-2

Information security awareness, training, and education responsibilities are provided below.

IT Security Awareness, Training, and Education Responsibilities

CISO

- Establish overall policy for information security awareness, training, and education.
- Provide guidance on preparing and attending security awareness and training sessions.
- Submit to the DHS Information Security Training Program Director a training plan outlining their plan for Information Security Awareness, Training, and Education for the year.
- Analyze, on a quarterly basis, security awareness and training statistics submitted by the ISSOs and COTRs and submit a summary of these statistics to the DHS IT Security Training Program Director.

ISSOs

- Ensure that all new employees, including contractors, complete an initial Government- or contractor-sponsored security awareness course as part of their orientation.
- Unless a CISO waiver is issued, disable all accounts and access privileges, including access to email, of those CBP users who failed to complete the annual security refresher course.
- Ensure that all users, including all contractors, read and sign rules of behavior for the use of systems and applications prior to their being given access to those systems and applications.
- Implement annual awareness refreshers for employees and support contractors involved in the management, use, or operation of IT systems that process sensitive information.
- Maintain a record of security awareness and training that includes the name and position of the person trained, the type of training, the date of the training, and the cost of the training.
- Submit to the CISO, on a quarterly basis, statistics on initial and refresher security awareness and training.
- Implement continued training for personnel when there is a significant change in the system security environment or in procedures, or when an employee enters a new position involving the handling of sensitive information.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000147

IT Security Awareness, Training, and Education Responsibilities
COTRs • Ensure that contractors have their personnel complete an initial security awareness course as part of their orientation. • Ensure that contractors have their personnel complete a refresher awareness course each year. • Ensure that contractors have their personnel sign rules of behavior for the use of systems and applications prior to their being given access to those systems and applications. • Ensure that contractors provide additional security awareness training to their personnel whenever there is a significant change in the system security environment or in procedures, or when contractor personnel enter a new position. • Ensure that contractors maintain a record of their personnel who have completed initial and refresher security awareness training, with the record to include the name of the person trained, the type and date of the training, and training cost. • Ensure that contractor security awareness and training statistics are provided to the CISO on a quarterly basis.

4.1.5.1 Initial Awareness

CBP must give newly hired employees an initial information security awareness course and have them read and sign a rules of behavior acknowledgement statement before giving those employees being given access to CBP network resource or application. The awareness course and the rules of behavior should be a part of the orientation process. CBP must also provide an initial awareness course to newly hired contractor staff or ensure that the contractors provide an equivalent course for their staff. Participation in the awareness course is mandatory. Records of the training must be maintained and retained to verify compliance; records must include at a minimum the employee's name and position, the type of training received, and the date of training.

The Security and Technology Policy Branch will review the IT Security Awareness Training annually to ensure the training reflects the evolving and changing nature of computer security incidents.

Alternative media for providing this initial awareness include seminars, presentations, awareness videotapes, and computer-based products delivered via CD-ROM Intranet/Internet and/or LAN.

4.1.5.2 Refresher Awareness

Each organization within CBP must ensure that employees and contractors complete CBP security awareness refresher courses at least annually. Participation in the refresher course is mandatory. User accounts and access privileges, including access to email, will be disabled for those who have not received annual refresher training. The CISO may issue a waiver to this requirement. Records of the training must be maintained and retained to verify compliance; records must include at a minimum the employee's name and position, the type of training received, and the date of training.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000148

Alternative media for providing this refresher awareness training include seminars, presentations, awareness videotapes, and computer-based products delivered via CD-ROM or the Intranet/Internet.

Additional awareness sessions should be conducted whenever a significant change occurs in a specific security environment or when an employee enters a new position involving the handling of a new category of sensitive information.

CBP policies relating to Peer to Peer (P2P) file sharing to all system users is also included in the security awareness training.

4.1.5.3 Ongoing Awareness Activities

CBP reinforces the awareness message throughout the year through the use of posters, newsletters, electronic messages, trinkets (e.g., pens, lanyards, notepads) with a security message, and other appropriate communication media.

4.1.5.4 Role-Based Training

CBP personnel and contractors assigned significant information security responsibilities such as CAs, ISSOs, network administrators, system administrators, and the AO – must receive specialized training specific to their security responsibilities annually. CBP must ensure specialized security-related training also be provided to senior managers, system owners and IT project managers. The level of training shall be commensurate with the individual's duties and responsibilities. CBP must track, by name and position, the type of the training received, the dates of the training, and the costs of the training.

4.1.6 Separation from Duty

This section addresses the procedures to be followed when an employee or contractor terminates employment or transfers to another organization.

Policy ID	CBP Policy Statements	Relevant Controls
4.1.6.a	CBP shall implement procedures to ensure that system accesses are revoked for employees or contractors who leave the CBP or are reassigned to other duties. Accounts for personnel on extended absences shall be temporarily suspended.	AC-2
4.1.6.b	CBP shall establish procedures to ensure that sensitive information stored on any media is transferred to an authorized individual upon termination or reassignment of an employee or contractor.	PS-4
4.1.6.c	Accounts for personnel on extended absences shall be temporarily suspended.	AC-2
4.1.6.d	System Owners shall review information system accounts supporting their programs at least annually.	AC-2

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000149

Responsibilities related to separation from duty are provided below.

Separation from Duty Responsibilities
System Owners/Senior Site Managers • Implement procedures to ensure appropriate system access privileges are revoked for employees or contractors who either leave CBP or are reassigned to other duties.
Supervisors • Notify system administrators in writing when employees or contractors no longer require access to CBP IT systems. • Retrieve all sensitive data from departing employees and contractors.
Network/System Administrators • Disable or delete user accounts when notified that an individual's access to CBP IT systems is reassigned or terminated.
Site Security Officers • Change combinations to all locks and safes when an employee or contractor with access has been reassigned or terminated. • Collect all keys, badges, and other devices used to gain access to premises, information, or equipment from employees and contractors who have been terminated or reassigned.
Employees and Contractors • Turn in laptops, cell phones, PEDs, secure ID tokens, and other Government-owned devices to the local property administrator in accordance with local procedures when reassigned or terminated.

In most circumstances, the transfer or termination of an employee or contractor is amicable. Allowing an employee or contractor to complete his or her duties and obligations through the last day of employment is normally the most effective course of action.

When the employee or contractor demonstrates resentment because of termination of duties, it is often better to immediately eliminate the employee's contact with the organization, including system access. It is also recommended that the employee be escorted from the premises, and that personal items be mailed or delivered at a later date. The security office for each CBP site should assist in creating a prudent plan of action.

CBP must adhere to the following guidelines when dealing with employee separation or termination:

- **Revoke all authorizations.** All authorizations granted to a departing employee or contractor are to be revoked. When an employee leaves CBP, personnel paperwork for resignation or transfer to another Government agency is processed in the personnel and payroll system. LAN access and other client/server systems must be revoked. It is the responsibility of the supervisor or IT Project Manager to ensure that these steps have been followed and the necessary levels of access have been revoked. If the departing employee or contractor authorizations include the granting of authorization to others, this

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt1 000150

must be reviewed and changed accordingly. If a user is being transferred within the CBP, it is possible to transfer the employee's user ID. However, since users are given access on a need-to-know basis, the supervisor must request that the user's access privileges be deleted before transferring. The proper level of access will be granted once the employee is officially in the new position.

- **Retrieve hard and soft copy sensitive information.** The supervisor should collect all hard and soft copy sensitive information.
- **Retrieve all keys, badges, and other access devices.** The local ISSO in coordination with the site security officer should collect all keys, badges, and other devices used to gain access to premises, information, or equipment.
- **Change locks.** The security officer will assist in changing combinations of all locks and safes known to the departing employee or contractor immediately.
- **Turn in Government-owned equipment.** Employees and contractors must turn in laptops, cell phones, portable electronic devices (PED), secure ID tokens, and other Government-owned property to the local property administrator in accordance with local procedures, and provide evidence at their exit interview that this action has been accomplished.
- **Conduct exit interview.** All employees and contractors leaving their positions must participate in an exit interview. One purpose of an exit interview is to provide management with information as to why people are leaving. This information will permit management to make positive changes, if necessary. The employee should return all CBP sensitive materials, and receive information concerning restrictions on divulging certain CBP information. There should be a review of any special conditions to the departing employee or contractor employment, such as the denial of right to use certain information. The exit meetings should occur prior to an employee or contractor departure from CBP. Failure to complete this step may make subsequent legal recourse (if needed) more difficult or impossible. The cognizant personnel or security office should conduct the exit interview in accordance with local procedures.

4.2 IT Physical Security

CBP security personnel must address physical security as an integral element in the effective implementation of an information security program. Physical security represents the "first line of defense" against intruders and adversaries attempting to gain access to CBP facilities and IT systems. Like other aspects of information assurance, physical security technology is advancing rapidly.

Physical security must be addressed during each step of the risk management cycle. Physical security vulnerabilities are identified during the risk assessment. Cost-effective controls are then documented in the security plan. These controls are then evaluated during the Security Test and Evaluation (ST&E). Any residual risks must be documented in the C&A package and reviewed on an annual basis. IT systems must be physically and environmentally protected to prevent unauthorized disclosure, denial of service, destruction, or modification.

The office of Internal Affairs (IA) develops and publishes the (b)(7)(E) (b)(7)(E), which addresses physical security for all of CBP. However, the *CBP Information*

Systems Security Policies and Procedures Handbook only addresses the minimum physical security requirements imposed for information security assets.

Section 4.2.1, General Physical Access, provides general physical security guidance for sensitive systems. Section 4.2.2, Sensitive Facility, addresses specific security considerations for facilities housing IT systems that store or process classified data.

4.2.1 General Physical Access

General physical access controls restrict the entry and exit of personnel from an area, such as an office building, data center, or room containing IT equipment. These controls protect against threats associated with the physical environment. It is important to review the effectiveness of general physical access controls in each area during business hours and at other times. Effectiveness depends not only on the characteristics of the controls used but also on their implementation and operation.

Policy ID	CBP Policy Statements	Relevant Controls
4.2.1.a	Access to CBP buildings, rooms, work areas, spaces, and structures housing IT systems, equipment, and data shall be limited to authorized personnel.	PE-2
4.2.1.b	Controls for deterring, detecting, restricting, and regulating access to sensitive areas shall be in place and will be sufficient to safeguard against possible loss, theft, destruction, damage, hazardous conditions, fire, malicious actions, and natural disasters.	PE-3
4.2.1.c	Controls shall be based on the level of classification and risk, determined in accordance with Departmental security policy.	PE-1
4.2.1.d	Visitors must sign in upon entering CBP facilities, be escorted during their stay, and sign out upon leaving. Non-CBP contractors' access shall be limited to those work areas requiring their presence. Visitor logs shall be maintained and available for review for one year.	PE-7
4.2.1.e	These requirements will extend to CBP assets, located at non-CBP facilities or non-CBP assets and equipment hosting CBP data.	---
4.2.1.f	CBP information systems and data, when not operational or under the direct control of an authorized individual, must be protected by control systems and measures consistent with the policies, procedures and standards provided by IA.	PE-3 MP-4
4.2.1.g	Rooms containing information systems hardware and software, such as Local Area Network (LAN) rooms or telephone closets, must be secured and accessible by CBP authorized personnel only. NOTE: Authorized personnel is defined as the individual who has control of the local assets or space or has permission from that individual.	PE-2

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000152

General physical access responsibilities are provided below.

General Physical Access Responsibilities
Facility Managers • Ensure that physical controls are in place. • Ensure that environmental controls are in place. • Ensure that physical and environmental controls are in working order at all times. • Ensure that access control logs are maintained and reviewed for the facility and all computer rooms. **Site Security Officers/ISSOs** • Provide specific security briefings to CBP employees and contractors, as necessary. • Assess the adequacy of physical security controls as part of the risk management cycle. • Change combinations to locks on security containers housing sensitive information, funds, and other valuables that must be safeguarded. • Conduct periodic inspections of offices and areas under their jurisdiction, during or after working hours, to ensure sensitive and proprietary materials are being adequately safeguarded. • Ensure security violations are appropriately reported and investigated, in accordance with CBP requirements. • Provide oversight of the issuance and return of Service badges, credentials, and identification documents; ensure proper reporting of the loss or theft of Service badges, credentials and identification documents. • Apply the security disciplines to the contractor environment. • Ensure Government-owned and controlled property, funds, and valuables are properly safeguarded and accounted for. • Ensure the physical security of IT Systems within their jurisdiction. • Ensure that physical and environmental security controls are addressed in the Security Plan. • Address physical security as an integral part of the risk management process. • Ensure that physical security risks are reviewed and evaluated throughout the System Life Cycle (SLC). **Users** • Adhere to established security policies. • Display building passes or other ID when required. • Challenge individuals who are not in compliance with established requirements. • Ensure that un-cleared visitors are escorted at all times.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000153

4.2.1.1 Physical Controls

Physical security encompasses the full range of protective measures designed to safeguard personnel and prevent unauthorized access to, and the loss, theft, destruction, sabotage, or compromise of equipment, facilities, material, and information. Physical controls include barriers, badges, guard or security forces, supporting infrastructure, contingency and emergency support, lighting, facility intrusion detection systems, and surveillance systems. Physical security protects computer facilities as well as individual computer systems and personnel. Standards for physical security must be based on an analysis of mission criticality, severity of impact levels, local criminal and intelligence threats, and the value of the telecommunications and automated information systems equipment contained within the facility being protected as well as the value of the data being processed.

Security personnel must ensure that physical security controls are considered throughout the life of the system. At a minimum, they should be reviewed in conjunction with the annual self-assessments and during each C&A cycle. The following in-place and planned controls associated with the following physical security features should be included in the appropriate security plan:

- Controlled access to building (i.e., physical building access, guards)
- Controlled access to computer room(s)
- Locks
- Key control procedures
- Keypads and cipher locks
- ID badges (worn above the waist area)
- Visitor logs
- Biometric devices
- Access control logs (to the building)
- Access control logs (to the computer rooms and facility)
- Motion detectors
- Intrusion detection devices
- Property passes
- Additional controls

Normally, not all of the above security features will be necessary for every facility. ISSOs and site security officers must determine, based on the criticality of the systems and sensitivity of the data being processed, which security features are warranted.

4.2.1.2 Building Passes

Building passes must be issued and displayed by direct hire and contract employees at all facilities that store or process sensitive information.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000154

Building passes should be displayed above the waist and below the neck with the photo side facing out. Each visitor must be issued a temporary building pass, which must be turned in before the visitor exits the facility.

Any persons not displaying proper credentials should be challenged. If there is any doubt as to their authorization, they are to be escorted from the area and local security personnel are to be contacted. Security personnel and supervisors at all management levels must ensure that all CBP staff, including contractors, are made aware of this requirement through awareness sessions and other means. Supervisors are expected to periodically reinforce this requirement during staff meetings and through emails and other communication methods. Where practical, challenge procedures should be posted.

4.2.1.3 Property Removal

Removal of items from CBP facilities must be controlled and documented.

4.2.1.4 Loss or Theft of Property

Any missing property, whether lost or stolen, must be reported.

4.2.1.5 Environmental Controls

In addition to the physical security controls discussed above, facility managers and security administrators must also ensure that environmental controls are established, documented, and implemented to provide needed protection in the following areas:

- Fire protection, detection, and suppression
- Water damage risk reduction, detection, and corrective measures, and devices for water hazard prevention
- Electronic power supply protection, to include uninterruptible power supplies for multiuse systems and surge protectors for stand-alone systems
- Temperature and humidity recording, monitoring, and alert systems (e.g., humidograph)
- Housekeeping protection from dirt and dust
- Combustible cleaning supplies protection (not to be kept in computer areas)
- Appropriate personnel safety features (evacuation routes specified)
- Emergency exit provisions, such as equipping emergency and exit-only doors with hardware that permits immediate egress in the event of an emergency

4.2.1.6 Fire Protection

Fire protection systems should be serviced by professionals on a recurring basis to ensure the system stays in proper working order. The following should be taken into consideration when developing a fire protection strategy:

1. When a centralized fire suppression system is not available, fire extinguishers should be readily available:

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000155

a. Facilities should store Class C fire extinguishers (which are designed for use with electrical fire and other types of fire).

b. Fire extinguishers should be located in such a way that a user would not need to travel more than 50 feet to retrieve a fire extinguisher.

2. Fire drills must be conducted a minimum of once per year in order to ensure that all personnel are familiar with their responsibilities.

4.2.1.7 Electronic Power Supply Protection

Electrical power must be filtered through an uninterruptible power supply (UPS) system for all servers and critical workstations. A surge suppressing power strip is necessary for all other ADP equipment to protect it from sudden power surges. For larger and more critical systems it may be appropriate to have an electrical generator available for the most critical of operational requirements.

4.2.1.8 Temperature and Humidity Control

The condition of the air is important to prevent damage to IT equipment. The following should be considered when developing a strategy for temperature and humidity control:

1. Temperatures in computer storage areas should be held between 60 and 70 degrees Fahrenheit. Most systems will continue to function when temperatures go beyond this range, but the associated risk to data is increased.

2. Humidity should be at a level between 35 percent and 65 percent. Most systems will continue to function when humidity goes beyond this range, but the associated risk to data is increased.

3. Low humidity can result in static, and high temperature can melt sensitive components of computer systems.

Check the system documentation for the proper levels for your hardware. Security personnel should obtain a device that will sound an alarm and send out an automatic notification (via email or pager) when the operating environment exceeds recommended boundaries.

4.2.1.9 Housekeeping Considerations

Housekeeping is another important area to monitor.

1. Sub-floors (where installed) should be cleaned on an annual basis.

2. If the computer room has carpet it should be of the antistatic variety. This also applies to areas that house workstations.

3. Dusting of hardware and vacuuming of work areas should be performed weekly with trash removal performed daily. Dust accumulation inside of monitors and computers is a hazard that can damage computer hardware.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000156

4. Cleaning supplies should not be stored inside the computer room.

4.2.1.10 Personnel Safety Features

The facility manager should brief all personnel on emergency procedures including:

1. Evacuation procedures.
2. Location of emergency exits.
3. Location of emergency equipment such as fire extinguishers and first-aid kits.

4.2.1.11 Emergency Exits

Emergency exits should be clearly marked and all personnel should be familiar with established evacuation routes.

4.2.2 Sensitive Facility

Facilities supporting large-scale IT operations, such as enterprise servers and telecommunications facilities, require consideration of additional environmental and physical controls as determined by a risk analysis.

Section 4.2 provides procedural guidance for both general physical access and sensitive facilities. For facilities supporting large-scale IT operations, all of the physical security features outlined in Section 4.2 must be addressed. The risk assessment shall specifically document the rationale for any such physical security controls not incorporated. Additionally, (b)(7)(E) (b)(7)(E), has additional information addressing physical security issues.

Policy ID	CBP Policy Statements	Relevant Controls
4.2.2.a	Facilities processing, transmitting, or storing sensitive information shall incorporate physical protection measures based on the level of risk. The risk should be determined in accordance with DHS and CBP security policy.	PE-1
4.2.2.b	Any sensitive information or data not suitable for public dissemination shall be secured in one of the following: a locked office, room, desk, bookcase, file cabinet, or other storage prohibiting access by unauthorized persons.	PE-?
4.2.2.c	CBP information systems, while operational, must process, store, or transmit sensitive information in buildings, communications facilities, or other physical spaces that are under the exclusive control of CBP. Space used but not owned by CBP must be documented in a current and validated Memorandum of Understanding (MOU) or in contractual and bilateral agreements.	PE-3 SA-9

See section 4.2.1 for summary of responsibilities for sensitive facilities.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000157

4.3 Media Controls

Storage media that contain sensitive information must be controlled so that the information on the media is protected. This section addresses the protection, marking, sanitization, production input/output, and disposal of media containing sensitive information. Storage media include but are not limited to the following:

1. Magnetic storage media: including reel and cassette format magnetic tapes; magnetic disks, including hard disk drives, floppy disks and diskettes, and disk packs; magnetic cards; and magnetic memory devices, including core memory and magnetic bubble memory.

2. Optical storage media: including optical cartridges, laser disks, compact disks (CD), digital video disks (DVD), Magneto-Optical (MO) disks, holographic devices, and optical tapes.

3. Solid-state storage media: including Random Access Memory (RAM), Read Only Memory (ROM), Field Programmable Gate Array (FPGA) devices, Personal Computer Memory Card International Association (PCMCIA) cards, Flash cards, Smart Cards, and USB removable media drives (also called flash drives, jump drives, and thumb drives).

4. Hard-copy storage media: including paper and microforms (e.g., microfilm and microfiche).

All CBP data stored on removable or transportable media/devices must be encrypted using CBP or other approved encryption method prior to leaving CBP-controlled environments. Data owners are responsible for determining the security category, handling, and markings for their data. Where additional caveats are required, they may be added to the markings on the media. For example, media labeled For Official Use Only media may further specify "Favorably Adjudicated BI Required" to limit access to the data contained in such media.

4.3.1 Media Protection

Proper storage of media enhances protection against unauthorized disclosure. There are additional security risks associated with the portability of removable storage media. Loss, theft, or physical damage to disks and other removable media can compromise the confidentiality, integrity, or availability of the data contained in these media.

All media containing sensitive information must be labeled and kept in a secure location. Backup and archive media must be sent to an off-site location as identified in the appropriate business continuity and IT contingency plans.

Policy ID	CBP Policy Statements	Relevant Controls
4.3.1.a	All CBP employees and contractors shall ensure all that media containing sensitive information, including hard copy media, backup media, and	MP-2, MP-4,

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000158

Policy ID	CBP Policy Statements	Relevant Controls
	removable media such as USB drives, are stored in a secure location (e.g., a locked office, room, desk, bookcase, file cabinet, or other storage prohibiting access by unauthorized persons) when not in use.	PE-1
4.3.1.b	CBP shall ensure backup media are stored off site in accordance with their business continuity and IT Contingency plans.	CP-6
4.3.1.c	CBP personnel and contractors are prohibited from using any non government issued removable media (USB drives, in particular) or connecting them to CBP equipment or networks or to store CBP sensitive information.	MP-2
4.3.1.d	All CBP USB drives shall use encryption that is FIPS 197 (AES-256) compliant and has received FIPS 140-2 validation.	IA-7, SC-13
4.3.1.e	CBP-owned removable media shall not be connected to any non-CBP information system unless the ISSO has determined the acceptable level of risk based on compensating controls, published acceptable use guidance and the guidance has been approved by the CISO.	AC-20, MP-2
4.3.1.f	CBP-owned USB removable media shall not be connected to any non-CBP information system.	AC-20, MP-2
4.3.1.g	CBP shall follow established procedures to ensure that paper and electronic outputs from systems containing sensitive information are protected.	MP-1
4.3.1.h	Users must ensure proper protection of printed output. Printing of sensitive documents shall occur only when a trusted person is attending the printer.	SI-12
4.3.1.i	Transportation or mailing of CBP sensitive media shall follow the procedures established by DHS MD 11042.1, *Safeguarding Sensitive But Unclassified (For Official Use Only) Information*.	MP-5

Media protection responsibilities are provided below.

Media Protection Responsibilities
CISO • Establishes and enforces CBP policy relating to labeling, storage, media reuse, and disposal of CBP equipment. **System Owners** • Ensure any special storage requirements are communicated to the IT project manager and system administrators. **System/Network Administrators** • Ensure that sensitive information is stored in a locked container or in an area with adequate

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000159

Media Protection Responsibilities
access controls to prevent unauthorized access, disclosure, damage, modification, or destruction. • Ensure that recipients of sensitive information have a valid "need to know" and proper authorization. • Ensure that copies of backups are stored at secure offsite locations. **Facility Managers** • Ensure that sensitive information is stored in a locked container or in an area with adequate access controls to prevent unauthorized access, disclosure, damage, modification, or destruction. • Establish both onsite and offsite storage locations. • Establish and maintain an inventory accounting system for all media entering or leaving a media storage area. Inventory should be verified at least semiannually. • Ensure that backup storage facilities meet the minimum requirements enumerated in Section 4.11, Information and Data Backup. **ISSOs** • Ensure that media are stored in accordance with the requirements enumerated in this handbook. • Ensure that storage requirements are addressed in the Security Plan and rules of behavior.

4.3.2 Media Marking

CBP processes, stores, and transmits sensitive information, including investigative information, information that could be sold for profit, information that could result in physical risk to individuals, law enforcement information, and criminal information. Appropriately labeling the media containing such information ensures that all recipients of the material are aware that the information requires protection.

Note: It is important to remember that if information with different levels of sensitivity is combined, the total package must carry the sensitivity level of the information that has the greatest sensitivity.

The following definitions apply within this section:

1. **Hardcopy Material:** printed material, including reports, emails, briefings, manuals, guidance, letters, and memoranda.

2. **Label:** a piece of information that indicates the sensitivity level of an object and the information contained in or on the object. A label can be either internal or external as follows:

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000160

a. **Internal Label:** a marking that reflects the sensitivity of the information within the confines of the medium that contains the information.

b. **External Label:** has a visible marking on the outside of the medium, or a cover that reflects the sensitivity of the information contained in or on the media.

3. **Storage Media:** includes but is not limited to magnetic storage media such as hard disk drives and diskettes; optical storage media such as CDs and DVDs; solid-state storage media, including USB drives; and hardcopy materials, including reports, emails, briefings, manuals, guidance, letters, and memoranda.

It is recommended that a label be affixed to PCs, terminals, and laptop computers and other mobile computing devices not authorized to process classified information, especially in environments where both sensitive information and classified information are processed. Labels stating "this medium is unclassified" are available from GSA (standard form 710).

Policy ID	CBP Policy Statement	Relevant Controls
4.3.2.a	Media determined by the information owner to contain sensitive information shall be appropriately marked in accordance with DHS MD 11042.1: *Safeguarding Sensitive But Unclassified (For Official Use Only) Information*.	MP-3

Media marking responsibilities are provided below.

Media Marking Responsibilities
CISO • Establishes and enforces policy relating to labeling, storage, reuse, and disposal of media containing CBP sensitive information. **System Owners** • Ensure that mission security needs based on the sensitivity of the information being processed are communicated to project managers and system administrators. **IT Project Managers** • Implement electronic marking requirements and warning banners for automated systems. **System Administrators** • Implement electronic marking requirements and warning banners on their systems. **ISSOs** • Ensure that sensitive systems and information are appropriately identified and that Sensitivity and Criticality levels are established for each system. • Ensure marking requirements are addressed in the System Security Plan and that noncompliance areas are identified.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000161

Media Marking Responsibilities
• Ensure that automated system and site personnel understand and are adequately trained in the identification of sensitive information and marking instructions. • Ensure that marking procedures and warning banners are reviewed with CBP employees on a periodic basis, such as during annual Computer Security Awareness sessions. • Ensure that all users are aware of the value and sensitivity of CBP information. • Ensure that users understand their responsibilities for safeguarding CBP information and how to fulfill their responsibilities. • Ensure that procedures are in place to ensure that CBP employees follow guidelines and procedures regarding marking.

4.3.3 Media Sanitization and Disposal

To protect sensitive information from unauthorized disclosure, media containing sensitive information must be sanitized prior to reuse (either within or outside of the organization) or disposition (i.e., disposal or recycling; return of leased media to the owner; return of defective or inoperable media for repair or replacement).

Policy ID	CBP Policy Statements	Relevant Controls
4.3.3.a	CBP shall ensure that any information systems storage medium containing sensitive information is sanitized using approved sanitization methods before it is disposed of, reused, recycled, or returned to the owner or manufacturer. Any authorized CBP government or contractor personnel with the appropriate technical expertise, Background Investigation (BI), and access may execute the cleansing, sanitizing, and/or destruction procedures for media.	MP-6
4.3.3.b	CBP shall maintain records of the sanitization and disposition of information systems storage media.	MP-6
4.3.3.c	Electronic storage media shall be sanitized appropriately by overwriting or degaussing. Additionally, CBP shall periodically test degaussing equipment to verify that the equipment is functioning properly. Contact local IT security personnel for additional guidance	MP-6

Media sanitization responsibilities are provided below.

Media Sanitization Responsibilities
Site Managers • Allocate resources to meet media sanitization requirements. • Enforce media sanitization requirements. **CISO**

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000162

Media Sanitization Responsibilities

- Develop and implement media sanitization procedures for storage media to be disposed of or recycled, reused, returned to the owner, or returned for repair or replacement.

ISSOs

- Ensure that media sanitization requirements are addressed in the System Security Plan and Security Operating Procedures.
- Maintain records of the sanitization and disposition of sensitive storage media.

System/Network Administrators

- Ensure that storage media for disposal, recycling, or reuse are properly sanitized.
- Ensure that leased storage media are properly sanitized before they are returned to the owner.
- Ensure that defective or inoperable storage media are properly sanitized before they are returned to the vendor or manufacturer for repair or replacement. Ensure that defective or inoperable storage media that cannot be sanitized are physically destroyed and disposed of.
- Periodically test degausser equipment to ensure proper operation.

Users

- Ensure the safekeeping of sensitive storage media in their possession.
- Notify ISSO or Site Security Manager when media containing sensitive information are no longer required.

NIST SP 800-88, *Guidelines for Media Sanitization*, provides guidelines for the sanitization of numerous types of information storage media, including the following:

- Magnetic disks (floppies; hard drives; USB removable media such as pen drives, thumb drives, flash drives, and memory sticks with hard drives; zip disks; and SCSI drives)
- Magnetic tapes (reel and cassette format magnetic tapes)
- Magnetic cards
- Optical disks (CDs, DVDs)
- Memory
- Hard copy (paper and microforms)
- Networking devices such as routers
- Handheld devices such as cell phones and personal digital assistants (PDA)
- Equipment (copy machines, fax machines).

The NIST guidelines apply to media containing sensitive information. The DHS 4300B National Security Systems Handbook provides information on the sanitization requirements for media containing classified information.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000163

NIST SP 800-88 identifies sanitization options for various IT storage media. Sanitization options depend on the type of storage medium (e.g., hard drive, CD or DVD, hard copy), intended disposition of the medium (e.g., reuse, disposal), and FIPS 199 categorization for the confidentiality security objective (see Section 3.9.1, FIPS 199 Categorization and the NIST SP 800-53 Controls).

NIST SP 800-88 defines sanitization as the removal of data from storage media such that there is reasonable assurance the data cannot be easily retrieved and reconstructed. Sanitization methods include clearing, purging, and destruction:

1. Clearing: the removal of information stored on media in such a way that the information is irretrievable through means such as robust keyboard attacks or the use of data, disk, or file recovery techniques. For magnetic media such as hard drives and diskettes, simple deletion of files is not sufficient for clearing, as the deleted data can be retrieved by various recovery utilities. Overwriting the information with random data, however, will clear the media of information and will help ensure that the information is irretrievable except perhaps by advanced laboratory techniques. There are overwriting software or hardware products that are available. In many cases, multiple overwrite/erasure of the drive shall be sufficient to allow transfer.

   Overwriting cannot be used for magnetic media that are damaged or not writeable. In such cases, the media must be physically destroyed.

2. Purging: the removal of information stored on media in such a way that the information is irretrievable through any means, including advanced laboratory techniques. Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging. For example, magnetic media such as hard drives and diskettes can be purged by degaussing. Degaussers expose the medium to a strong magnetic field, which effectively erases the information (however, a degausser designed and approved for the type of medium being purged is required). Note that degaussing destroys hard drives, as the firmware that manages the drive is also purged during the degaussing process.

   Degaussing is effective only on magnetic media such as hard drives, diskettes, and magnetic tapes. It is not effective, for example, on optical media such as CDs and DVDs.

3. Destruction: Destruction of media is the ultimate form of sanitization. Physical destruction can be accomplished through disintegration, incineration, pulverizing, shredding, and melting. Destruction of media should be conducted only by trained and authorized personnel. Safety, hazmat, and special disposition needs should be identified and addressed prior to conducting any media destruction.

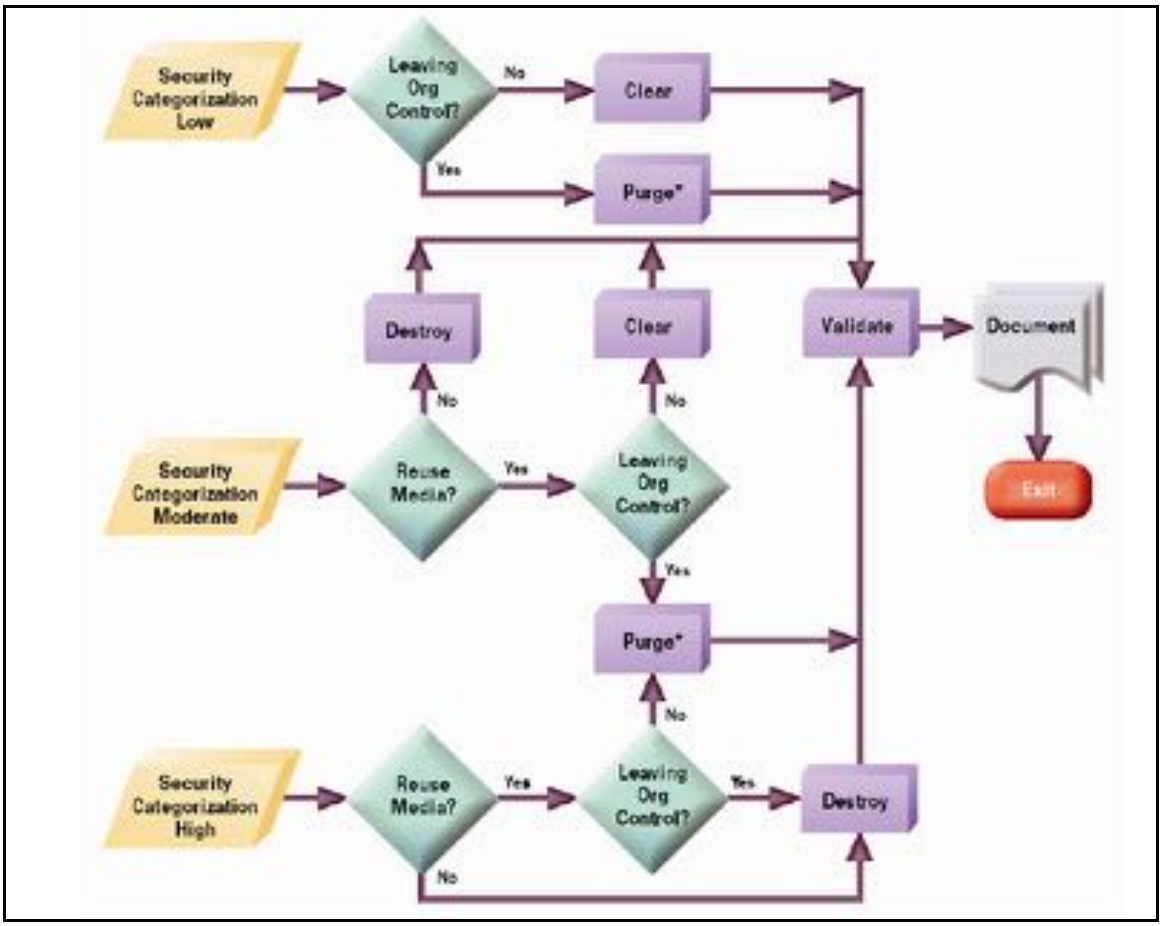
Sanitization also requires the removal of all labels, markings, and activity logs.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000164

Steps for sanitizing of media are the following:

- Determine the categorization (i.e., low, moderate, or high impact) for the confidentiality security objective.
- Determine whether the media will be disposed of or reused (either within or outside of the organization).
- Use Figure 4.3.3 to determine the appropriate method of sanitization.

Figure 4.3.3: Flowchart depicting the process for selecting media sanitization method by categorization of impact for the confidentiality security objective. (Adapted from NIST SP 800-88.)



- Refer to Attachment Y and Table A-1 in NIST SP 800-88 for sanitization options for the type of medium to be sanitized
- Validate and document the sanitization of the medium. Appendix F in NIST SP 800-88 provides a sample sanitization validation form
- Refer to Media Sanitization Procedures, Attachment Y of this handbook for additional procedures addressing Sensitive-But-Unclassified data. Refer to CBP National Security Systems Handbook for procedures relating to classified media.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000165

Sensitive media can be shipped to facilities for clearing, sanitization, or disposal following the guidelines in Section 4.3.4, Production, Input/Output Controls.

The National Security Agency (NSA) may accept sensitive media for destruction. For more information and for requirements, contact NSA Classified Material Conversion Customer Service at [redacted].

4.3.4 Production, Input/Output Controls

Regardless of method, transmission of sensitive information should be effected through means that limit the potential for unauthorized public disclosure. Unintended recipients may intercept information transmitted over unencrypted electronic links (e.g., telephone lines). Custodians of sensitive information should decide whether specific information warrants a higher level of protection accorded by a secure fax, phone, or other encrypted means of communication.

Policy ID	CBP Policy Statements	Relevant Controls
4.3.4.a	CBP shall follow established procedures to ensure that sensitive information cannot be accessed or stolen by unauthorized individuals.	SI-12
4.3.4.b	These procedures shall address not only the paper and electronic outputs from systems but also the transportation or mailing of sensitive media.	SI-12
4.3.4.c	All CBP generated and non-generated data must be protected according to its classification or designation level as documented in Table 4.3.4. If the CBP Sensitive Security Information (SSI) would be detrimental to transportation security refer to Section 4.3.4.1. Information not owned by CBP must be controlled in accordance with the owner's labeling.	SI-12
4.3.4.d	Hard Copy materials will be destroyed by shredding, burning, pulping, pulverizing, such as to assure destruction beyond recognition and reconstruction. After destruction, materials may be disposed of with normal waste.	MP-6
4.3.4.e	Paper product containing FOUO information will not be disposed of in regular trash or recycling receptacles unless the materials have first been destroyed as specified above.	MP-6
4.3.4.f	Removable media containing sensitive information (for example FOUO and PII) shall be transported via U.S. Postal Service or commercial carriers that provide tracking capabilities (per DHS MD 11042.1). Each item transported must be tracked. Media shall be encrypted following the standard defined in this handbook.	MP-5
4.3.4.g	All uploads or downloads from mainframes or servers of data files, databases or portions thereof must be part of an official related function and approved by the individual's supervisor before the activity is performed.	SI-12
4.3.4.h	Remove downloaded files from the workstation as soon as they are no longer needed.	SI-12

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000166

Responsibilities related to production, input/output controls are provided below.

Production, Input/Output Control Responsibilities
CISO • Develop and enforce policy relating to the input and output of CBP information. **Facility Managers** • Ensure that sensitive information is transported, transmitted and received in accordance with CBP policy. **ISSOs** • Ensure that the Security Plan addresses transmission of sensitive material. • Ensure that users have authority to access only information for which they have a valid "need to know." • Ensure that sensitive information is transmitted in a secure manner. • Ensure sensitive security information pertaining to transportation security is transported in accordance with the owner's labeling.

Table 4.3.4: Information Handling Policies by Classification Level

Category	Definition	Handling	Marking
Classified National Security Information	Information that has been determined, pursuant to E.O. 13526, as amended, to require protection against unauthorized disclosure: and marked to indicate its classified status	Data access requires both a proper security clearance and a need-to-know. Any media containing classified material must be properly stored in a GSA-approved safe when not in use and generated on accredited computer systems	Depending on level of damage to national security, Top Secret, Secret, Confidential, standard marking applies as defined in E.O. 13526, as amended, Section 1.6
For Official Use Only (FOUO)	The DHS caveat to identify unclassified information of sensitive nature, not otherwise categorized by statute or regulation, the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs or other programs or operations essential to the national	Information not releasable to the public shall be controlled, handled, and processed to ensure that only authorized users with a need-to-know can access the data (keep stored in bar lock or key lock cabinets, or in areas not accessible to unauthorized personnel) additional handling procedures as defined in the	"FOR OFFICIAL USE ONLY" Additional markings and or disclaimers may apply as needed. See Law Enforcement Sensitive Information below.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000167

Category	Definition	Handling	Marking
	interest	DHS MD 11042.	
Law Enforcement Sensitive (LES) **(Note- LES is a subcategory under FOUO)**	No DHS standard definition. Typically investigative information, records, TECS NCIC information etc.	The same handling procedures as FOUO.	Information containing specific types of FOUO may be further marked with the applicable caveat e.g. "FOR OFFICIAL USE ONLY" This document contains Law Enforcement Sensitive Information…
Procurement Sensitive **(Note- Procurement Sensitive is a subcategory under FOUO)**	No DHS standard definition. Sensitive procurement information that is restricted to individuals with a need to know.	The same handling procedures as FOUO.	Materials containing specific types of FOUO may be further marked with the applicable caveat e.g. "FOR OFFICIAL USE ONLY" This document contains Procurement Sensitive Information…
Sensitive Security Information (SSI)	Information that would be detrimental to transportation security if publicly disclosed and as defined in 49 CFR 1520.5 (b)	Generally the same handling procedures as FOUO. See MD 11056 for specific handling procedures.	Information designated, as SSI shall be marked in accordance with 49 CFR 1520.13 e.g. SSI and SSI marking disclaimer.

4.3.4.1 Sensitive Security Information

Sensitive information may be sent via the U.S. Postal Service, Army Post Office (APO), commercial messenger, or **unclassified** registered pouch, provided it is packaged in a way that does not disclose its contents or the fact that it is sensitive information (double-enveloped).

In data-center environments, procedures should be implemented to account for the receipt of input and output media to include paper and magnetic media. Authorization lists should be maintained identifying who is authorized to submit input for processing and receive output after processing. Logs should be maintained to document the transfer of sensitive data via a third party such as mail and courier services.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000168

Sensitive Security Information, as defined in 49 CFR 1520, is information that would be detrimental to **transportation security** if publicly disclosed. Sensitive Security Information is not classified information, however, there are clear procedures for recognizing, marking, protecting, sharing, and destroying Sensitive Security Information.

If a document belongs to one of the following 14 specific categories below (as defined in 49 CFR 5020.5, as it pertains to **transportation**), it is considered Sensitive Security Information and must be marked and protected accordingly.

- Security programs and contingency plans
- Security directives
- Information circulars
- Performance specifications
- Vulnerability assessments
- Threat information
- Security measures
- Security screening information
- Security training materials
- Identifying information of certain transportation security personnel
- Critical aviation or maritime infrastructure asset information
- Systems security information
- Confidential business information
- Research and development

The Transportation Security Administration (TSA) Administrator is the delegated authority within DHS for the implementation, management, and oversight of the Sensitive Security Information program. CBP is required to establish a viable Sensitive Security Information program. These responsibilities are defined in DHS Management Directive 11056, Sensitive Security Information.

4.4 Voice Communications Security

This section addresses vulnerabilities inherent in voice communications and the operational controls needed to mitigate the risks associated with these vulnerabilities. Voice communication security encompasses Private Branch Exchange (PBX) systems, telephone usage, and voice mail. **Note:** If encryption is used for voice communication, AES encryption per FIPS 140-2 must be used.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000169

4.4.1 Private Branch Exchange

A Private Branch Exchange (PBX) is a computer-based switch that acts as a small, in-house phone company for the organization that operates it. Failure to secure a PBX system can result in toll fraud as well as theft of proprietary, personal, and confidential information. Moreover, an attacker could also use the call tracking features of an unsecured PBX for traffic analysis to determine possible patterns of response to a planned incursion. Protecting the PBX is thus a high priority.

Private Branch Exchanges (PBXs) and other voice communications switches must be tested periodically for the existence of vulnerabilities that would permit unauthorized access to sensitive information or systems, theft of service (toll fraud), loss of revenue, or legal problems. Depending on the manufacturer of the PBX and the features available, other vulnerabilities may need to be evaluated. Annual PBX evaluations will be documented in the risk assessment for the overall system.

Policy ID	CBP Policy Statements	Relevant Controls
4.4.1.a	CBP shall provide adequate physical and IT security for all CBP-owned Private Branch Exchanges (PBX). (Refer to NIST SP 800-24, PBX Vulnerability Analysis, for guidance on detecting and fixing vulnerabilities in PBX systems.)	CM-2
4.4.1.b	CBP shall evaluate its PBXs annually for vulnerabilities associated with user features.	CM-2
4.4.1.c	CBP shall restrict physical and logical access to authorized personnel with a valid need-to-know.	AC-6
4.4.1.d	CBP communications via telephone, cell phone, facsimile, video teleconference, or voice mail shall not contain information that is considered classified national security information.	PL-4
4.4.1.e	CBP shall have in place transmission protections that are commensurate with the highest level of sensitivity of the information to be transmitted. Where possible, encrypted channels or hard-wired telephones are preferred for transmission of Sensitive-But-Unclassified (SBU) voice communications.	CM-6
4.4.1.f	CBP shall not store any Sensitive information in voice mailboxes.	PL-4

PBX security responsibilities are provided below.

PBX Security Responsibilities
CISO • Provide guidance concerning appropriate PBX-related security training to include: – Types of information personnel should not release to callers. – Security requirements for new PBX systems (e.g., disable test accounts, passwords,

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000170

PBX Security Responsibilities

and shortcut keys) and for maintenance activities for distribution to vendors.

Site Managers

- Ensure that employees and others with access to the facilities have agreed to and signed a PBX policy statement.
- Ensure that the PBX contracts and maintenance agreements include information on disputes, how they are settled, and the appeals process. Obtain approval from legal team before implementing.
- Explicitly include the requirements for integrity, availability, and confidentiality protection in the PBX, and directly address liability in PBX contractual agreements.
- Develop specific guidelines on acceptable and unacceptable use of telecommunications within the organization, and specify how the PBX policy deals with actions not explicitly covered by the policy.

ISSOs

- Address PBX issues in annual awareness sessions provided to all employees.
- Identify the personnel or position(s) responsible for telephone usage in the PBX policy statement.
- Ensure that agreements with the local exchange carrier (LEC), the inter-exchange carrier (IXC), and the equipment vendors allow for only authorized personnel to request service level changes, and to report errors.
- Verify all toll calls billed against PBX traffic reports.
- Ensure that internal PBX audits include verifying that all records are in electronic form.
- Ensure that internal IT auditors complete an audit of each PBX system at least once a quarter.
- Ensure that all personnel with access to the PBX or connected equipment have signed employee agreements including PBX-related material.
- Test audit mechanisms at least quarterly.
- Test audit computers periodically.
- Ensure external auditors do blind external testing.

PBX Administrators

- Identify the personnel or position(s) responsible for telephone usage in the PBX policy statement.
- Ensure that agreements with the LEC, the IXC, and the equipment vendors allow for only authorized personnel to request service level changes, and to report errors.
- Verify all toll calls billed against PBX traffic reports.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000171

PBX Security Responsibilities

- Ensure that internal PBX audits include verifying that all records are in electronic form.
- Ensure that internal IT auditors complete an audit of each PBX system at least once a quarter.
- Ensure that all personnel with access to the PBX or connected equipment have signed employee agreements including PBX-related material.
- Test audit mechanisms at least quarterly.
- Test audit computers periodically.
- Ensure external auditors do blind external testing.

Site Telephone Technical Support

- Clearly mark circuit numbers on channel banks, CSUs, DSUs, and modems.
- Clearly label main distribution frames (MDFs) and intermediate distribution frames (IDFs).
- Fully document procedures for making PBX software and hardware changes and use signed checklists to record all changes as they occur.
- Identify third party calls on phone bills and flag them on automated analysis.
- Generate and keep full call audit records in paper and electronic forms.
- Follow procedures to ensure the periodic dump of all PBX parameters and automatic comparison to the previous dump; report differences to management.
- Follow procedures to determine the frequency of the periodic dump and comparison as a normal part of risk management.
- Store PBX backups off-site, verify the media by reading back in, and periodically test the media on backup equipment to assure that they work properly.
- Ensure a complete dump of internal parameters is reconciled with previous dumps after completion of remote maintenance.
- Record all transactions in an external computer system.
- Ensure systems cannot redirect incoming calls from outside lines to make outside calls.
- Record and print all call details.
- Store records on a write once read many (WORM) disk for additional assurance.

Potential threats to a PBX include:

- Theft of service
- Disclosure of information
- Data modification
- Unauthorized access

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000172

- Denial of service
- Traffic analysis.

PBXs are sophisticated computer systems that share many of the threats and vulnerabilities associated with general purpose operating systems. There are, however, two important ways in which PBX security differs from conventional operating system security:

1. **External access/control.** Like larger telephone switches, PBXs typically require remote maintenance by the vendor. Instead of relying on local administrators to make operating system updates and patches, organizations normally have updates installed remotely by the switch manufacturer. This requires remote maintenance ports and access to the switch by a potentially large pool of outside parties.

2. **Feature richness.** The wide variety of features available on PBXs, particularly administrative features and conference functions, allow for the possibility of unexpected attacks. A hacker may use a feature in a manner not intended by its designers to eavesdrop on sensitive conversations. Features may also interact in unpredictable ways, leading to system compromise even if each component of the system conforms to its security requirements and the system operation and administration are correct.

4.4.1.1 Maintenance Vulnerabilities

PBX manufacturers may include features useful when on-site maintenance personnel cannot resolve problems. For example, the manufacturer could instruct the maintenance personnel to configure and connect a modem to the maintenance port. Use of such remote connections must be controlled (only made available as needed in response to a particular problem), logged, and supervised. The manufacturer may then be able to dial in and use certain special features to resolve the problems without sending a representative to the customer's location. Use of such remote connections must be controlled (only made available as needed in response to a particular problem), logged, and supervised. These types of features must not be accessible via accounts held privately by the manufacturer. Proper password procedures must be enforced, with the exception that passwords should expire in a shorter period (e.g., 30 days) or be single use (e.g., a secure remote access device). All such access and changes to the PBX data and configuration must be logged.

Examples of these special features include:

1. **Database upload/download utility.** This utility allows the manufacturer to download the database from a system that is malfunctioning and examine it at their location to try to determine the cause of the malfunction.

2. **Database examine/modify utility.** This utility allows the manufacturer to remotely examine and modify a system's database to repair damage caused by incorrect configuration, design bugs, or tampering.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000173

3. **Software debugger/update utility.** This utility permits the manufacturer to remotely debug a malfunctioning system. It also allows the manufacturer to remotely update systems with bug fixes and software upgrades.

These features are subject to intrusion, and could provide dangerous access to the PBX, if known by the wrong persons. To mitigate the risks associated with these vulnerabilities, ISSOs and site managers must:

1. Ensure that remote maintenance access is not operational. Whenever possible, some involvement of local personnel in opening remote maintenance ports is required.

2. Install two-factor (i.e., two different mechanisms) strong authentication on remote maintenance ports. Smart card-based systems or one-time password tokens, in addition to conventional login/password functions, make it much more difficult for attackers to breach the system's security.

3. Keep maintenance terminals in a locked, restricted area.

4. Locate the PBX equipment in a locked, restricted location, which does not indicate what it contains (e.g., do not post a sign saying "PBX room").

5. Turn off maintenance features when not needed.

6. Verify that non-U.S. citizens do not perform maintenance.

4.4.1.2 Software Loading and Update Tampering

A PBX is particularly vulnerable to software tampering when software is initially loaded and when any software updates/patches are being loaded. An adversary could intercept a software update sent to a PBX administrator. To mitigate the risks associated with these vulnerabilities, ISSOs and site managers must:

1. Make passwords resistant to cracking by automated tools.

2. Understand that conventional error detection codes such as checksums or cyclic redundancy codes (CRC) are not sufficient to ensure tamper detection. Strong error detection based on cryptography provides better protection.

3. Ensure that PBX boot disks, utilities, logs and records receive more protection than that for typical office software. Strong physical security should be provided, and these items must be appropriately labeled (see Sections 4.3.2 and 4.11).

4. Shred printouts and sanitize media before discarding.

4.4.1.3 User Features

The many features that make PBXs easy to configure and use have led to an expansion of vulnerabilities. These features include:

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000174

- Attendant console/override/forwarding/conferencing
- Automatic call distribution (ACD)
- Override (intrude)
- Diagnostics
- Feature interaction
- External/Remote access (e.g., remote vendor maintenance)
- Undocumented maintenance features
- Voice mail features
- Access to administrative databases and terminals or consoles
- Wiring closets and PBX facility
- Dial-back modems
- Live microphones

To mitigate the risks associated with these vulnerabilities, ISSOs and site managers must:

1. Connect the attendant console to the PBX with a different physical connection than that of the telephone instruments.

2. Use a line configuration feature if the attendant console connects to the PBX in the same manner as the telephone instruments. Such a feature could require specific line configuration for use with an attendant console. This would prevent the replacement of a telephone instrument with an attendant console to gain access to administrative features.

3. Ensure that only essential features are activated.

4. Log any changes to the configuration (software, database or physical) of the device.

5. Activate and periodically check any logging facilities provided by the device.

6. Perform periodic reviews of security facilities, confirming proper configuration and proper correlation of manual logs, device logs and other records.

4.4.2 Telephone Communications

CBP unsecured telephones shall not be used to discuss classified security information. Moreover, care must be exercised in discussing sensitive information. Adequate protection of sensitive information requires cognizance of the various risks related to telephone equipment and conversations. CBP shall ensure that users are cognizant of social engineering techniques used to obtain information over the telephone, including passwords and access codes.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000175

Policy ID	CBP Policy Statement	Relevant Controls
4.4.2.a	CBP shall develop guidance for discussing sensitive information over the telephone. Guidance shall be approved by a senior CBP official and is subject to review and approval by the DHS CISO. Under no circumstances shall classified national security information be discussed on unsecured telephones.	PL-4

Telephone communications responsibilities are provided below.

Telephone Communications Responsibilities
CISO • Establishes and enforces security policy relating to telephone communications. **ISSOs** • Ensure that users are aware of the telephone communications security policy. **Users** • Adhere to the telephone communications security policy not to discuss classified information over the telephone and to exercise care when discussing sensitive information.

The following vulnerabilities of unsecured telephone systems can result in unintentional transmission of classified or sensitive information. Commonly accepted best practices dictate that users be made aware of these vulnerabilities and exercise extreme caution when discussing sensitive information on unsecured phones. Unsecured phones shall not be used to discuss classified information.

1. Telephones that are "on-hook" can intercept voice communications by design, modification or attachment of monitoring devices.
2. Cordless telephones generate signals that can be monitored.
3. Speakerphones can pick up nearby conversations containing sensitive material.
4. Telephone answering devices can be accessed to retrieve sensitive information.
5. Call forwarding options can be used to redirect sensitive messages.
6. Improperly configured or physically unsecured PBXs and computerized telephone systems (CTS) can allow interception of sensitive voice communications.

These risks justify the policy restriction on the use of telephones. The basic telephony concepts behind these vulnerabilities are beyond the scope of this document. Restricting the use of desktop equipment (e.g., cordless telephones, speakerphones, answering devices, call forwarding options, etc.) in areas where sensitive information will be discussed mitigates some of the risks associate with these vulnerabilities. Following the procedures and guidance in NIST SP 800-24,

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000176

PBX Vulnerability Analysis: Finding Holes in Your PBX before Someone Else Does, will mitigate others. Finally, where telephones must be used to discuss sensitive information, additional guidance can be obtained from the NSA and DOD regarding telephone models that reduce or eliminate the vulnerabilities listed in this section.

4.4.3 Voice Mail

Sensitive information is not to be stored on voice mail systems. Since secure email will be made available, voice mail should be authorized only by exception for personnel whose responsibilities require it.

Since it is possible to perform traffic analysis or denial of service attacks on telephone systems by abusing voice mail, any user of voice mail should enable password protection for voice mail access. Voice mail passwords should have no fewer than four characters, and no consecutively repeated characters. Passwords should be changed at least every 90 days.

For more information, refer to Section 4.4.1, Private Branch Exchange.

Policy ID	CBP Policy Statement	Relevant Controls
4.4.3.a	Sensitive information shall not be communicated over nor stored in voice mail.	PL-4

Voice mail responsibilities are provided below.

Voice Mail Responsibilities
ISSOs • Identify the personnel or position(s) responsible for telephone usage in the applicable voice communications policy statement. **PBX Administrators** • Identify the personnel or position(s) responsible for telephone usage in the applicable voice communications policy statement. • Ensure that telephone systems are configured to enable enforcement of minimum password requirements for voice mail. **Telephone Users** • Create secure passwords that adhere to at least the minimum voice mail password requirements.

4.5 Data Communications

This section addresses vulnerabilities inherent in data communications and the operational controls needed to mitigate the risks associated with these vulnerabilities. Data communications encompasses telecommunications, video teleconferencing, and voice over data network technology.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000177

4.5.1 Telecommunications Protection Techniques

Extreme caution should be exercised when telecommunications protection techniques are being considered as alternatives to the use of encryption. While such technologies may represent a lower-cost approach, their ability to protect information may not provide an adequate level of protection. During the procurement process, emphasis must be placed on the effectiveness of the tool or approach selected.

Policy ID	CBP Policy Statement	Relevant Controls
4.5.1.a	CBP shall carefully select the telecommunications protection techniques that meet the security needs, in the most cost-effective manner, consistent with Departmental and CBP IT policies. Approved guided media techniques or approved protected network services (PNS) may be used as cost-effective alternatives to the use of encryption for sensitive information requiring telecommunications protection.	CM-2

Telecommunications protection responsibilities are provided below.

Telecommunications Protection Responsibilities
CISO • Advise DHS project managers in the selection of telecommunications protection techniques that would serve as an alternative to encryption for data transmission protection techniques. **System Owners** • Select the telecommunications protection techniques that meet their security needs consistent with DHS security policies in the most cost-effective manner.

Although sensitive data may be contained entirely within a PNS, there still exists the possibility that a disgruntled, malicious, or subversive individual may be able to access this information through devices or software that capture data traveling across the network. This is often accomplished by "sniffing" software, which uses low-level driver commands to turn a Network Interface Card (NIC) into a "promiscuous" mode. Normally, NICs only accept information directed to them and ignore information that does not have their address. A promiscuous NIC collects all information from the network to which it is attached, regardless of the intended address.

There are tools that are capable of detecting NICs that have been placed in a "promiscuous mode." The scanning of systems referred to in Section 5.4.9, Testing and Vulnerability Management, can detect software programs on DHS systems that are capable of enabling this mode. Scanning tools can also detect software operating in the promiscuous mode when it is collecting data from a NIC.

A malicious individual can make information unavailable by rendering the network unusable. This is commonly known as a denial of service (DoS) attack. An individual can initiate a DoS

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000178

attack by broadcasting large amounts of data, by physically compromising network components, or by taking advantage of some of the inherent weaknesses of the TCP/IP handshaking process.

Intrusion detection system tools exist that can detect most types of DoS attacks (see Section 5.4.4, Firewalls). Proper configuration of server systems can also mitigate these attacks by altering the default TCP/IP software configuration settings.

An additional vulnerability exists with respect to the accuracy of the information transmitted. There is an entire class of attacks known as "man in the middle" attacks. In these types of attacks, an individual receives information, alters it, and transmits the altered information to its originally intended recipient in such a manner that the recipient believes that the information was sent directly from the original destination. These attacks can be mitigated through the use of message digests. Message digests calculate a fixed length value from any amount of text. This fixed length value is very difficult to reproduce. Also, encryption and digital signing make the task of altering data difficult or sufficiently time consuming that it is of little use.

NIST SP 800-13, *Telecommunications Security Guidelines for Telecommunications Management Network*, outlines these and other security considerations involving telecommunications. NIST contends that 65 percent of the compromises regarding availability, integrity and privacy/ confidentiality are committed by employees through "errors, omissions and malicious acts."

4.5.2 Facsimiles

Facsimile technology was developed for scanning and transmitting documents or pages. Although facsimile is traditionally a telephony-based application, the technology has evolved to address the transmission of text or image files. Standards are under development for Internet-based fax using store-and-forward protocols and real-time connectivity between IP-connected fax gateways.

Facsimile inherently is not a secure means of communication, and faxes can easily be intercepted and decoded. Fax protocols provide neither authentication nor non-repudiation services, which allows fax traffic to be sent to or received by improper recipients. The commonly used Group III fax protocol implements support for proprietary and undocumented data exchange using a feature called nonstandard facilities (NSF). Therefore, fax servers or fax modems attached to networks provide a potential means for network intrusion and penetration.

Several proactive steps must be taken to ensure adherence to CBP facsimile policy. This policy is designed to prevent unauthorized paths into the protected network, commonly referred to as "backdoors." For example, "fax polling" features must be disabled. Fax polling allows a remote fax machine to access a fax machine and retrieve any data in memory waiting to be delivered.

Policy ID	CBP Policy Statements	Relevant Controls
4.5.2.a	CBP shall implement and enforce technical controls for fax technology and systems (including fax machines, servers, gateways, software, and protocols) that transmit and receive sensitive information.	SC-1, SC-7, SC-8, SC-9

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000179

Policy ID	CBP Policy Statements	Relevant Controls
4.5.2.b	CBP shall configure fax servers to ensure that incoming lines cannot be used to access the network or any data on the fax server.	AC-4

Facsimile responsibilities are provided below.

Facsimile Responsibilities
CISO • Establishes and enforces policy relating to the use of CBP facsimile machines. **System/Network Administrators** • Ensure that facsimile machines connected to CBP IT resources are protected and configured to prevent mishandling of sensitive information. **Facility Managers** • Ensure that appropriate physical security requirements are implemented for facsimile machines. **ISSOs** • Ensure that applicable IT security requirements are applied as necessary to facsimile machines. • Ensure that the Security Plan addresses facsimile machines connected to CBP IT systems.

Any fax machine used to transmit sensitive information needs to be placed in a locked room that only trusted individuals may access. The fax machine should also be placed in such a fashion that any documents being sent or retrieved are not visible to un-trusted individuals.

Anyone sending sensitive information should verify the recipient's secure fax number immediately before sending. They should also ascertain that the intended recipient (or trusted subordinate) will be present to receive the fax as soon as it is sent. Sensitive information should never be sent to an unattended fax machine. Sensitive material should be sent from a machine that has the "memory" features turned off, so that the information cannot be accessed or retransmitted (possibly to an un-trusted recipient) at a later time. All documents that are being transmitted should be appropriately labeled (see Sections 4.3.2 and 4.11 of this handbook). The reverse procedure should be used if the individual is receiving. All documents transmitted or received should be immediately removed from the fax machine room and appropriately stored.

Extremely sensitive or classified faxes require more stringent controls, such as transmission over trusted links (as opposed to the Public Switched Telephone Network (PSTN)). If such a fax must be sent via the PSTN, encryption devices should be used.

Because a fax machine is operated in a similar manner to a copying machine, transmission of extremely sensitive or classified data should be followed by using the machine in copier mode to process several copies of a test pattern or some unclassified data to remove the image of the sensitive data from the fax machine's imaging apparatus.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000180

4.5.3 Video Teleconferencing

Video teleconferencing permits CBP personnel to engage in live exchanges of information without the lost time and high cost of traveling to attend a face-to-face meeting in a distant city. Video teleconferencing offers many beneficial applications, including training and distance learning, data collaboration, large and small meetings, and informational broadcasts.

Policy ID	CBP Policy Statements	Relevant Controls
4.5.3.a	CBP shall implement controls to ensure that only authorized individuals are able to participate in each videoconference.	AC-3, PE-3
4.5.3.b	CBP shall ensure appropriate transmission protections, commensurate with the highest sensitivity of information to be discussed, are in place throughout any video teleconference.	SC-8, SC-9
4.5.3.c	Video teleconferencing equipment and software shall be disabled when not in use.	AC-3, PE-3

Video teleconferencing responsibilities are provided below.

Video Teleconferencing Responsibilities
AO • Carefully weigh the risk associated with the use of video teleconferencing equipment connected to CBP IT systems prior to accreditation. **CISO** • Advise CBP personnel in the selection and secure use of video teleconferencing technologies. **Supervisors** • Establish procedures to ensure only authorized attendees participate in teleconferencing sessions. • Ensure procedures are in place to disable video teleconferencing equipment when not in use. • Ensure procedures are in place to label and store videotapes recorded during the teleconferencing. **ISSOs/Teleconferencing Operators** • Ensure video teleconferencing is addressed in the Security Plan if the equipment is connected to a CBP IT system. • Ensure video teleconferencing equipment is disabled and secure when not in use. • Ensure appropriate transmission protections are in place commensurate with the highest sensitivity of information to be discussed when conducting a video teleconferencing session.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000181

Video Teleconferencing Responsibilities
Users • Shall not discuss information during a teleconferencing session at a higher level of classification than that established for the conference.

Two basic mechanisms allow video teleconferencing to take place. The most basic uses professional quality video equipment, which displays remotely on television monitors or similar projection devices. The second uses inexpensive video devices, which are attached to computers and display on computer screens using protocols such as H.323 over IP networks. The transmission medium for both can be within a protected network, across the PSTN or across an internal or external (Internet) network connection.

The first approach allows the equipment to be controlled, operated, and secured by trusted individuals with specific responsibilities for the teleconferencing equipment. Operators can assure that any recording of information is labeled and secured according to its sensitivity (see Section 4.3.2), properly disposed of when no longer useful (see Section 4.3.3), and secured during transmission by use of proper encryption (see Section 5.7.1) or tunneling. They can also confirm that the broadcasted information is being sent to the proper location. It is recommended that, to the degree possible, such conferences occur in a point-to-point manner between two sites.

The second approach is not authorized. This technology introduces all of the vulnerabilities associated with sensitive data transmission across an IP network (see Section 4.5.1), as well as the vulnerabilities associated with other devices, which may unwittingly make sensitive data available to unauthorized parties (see Sections 4.4.2 and 4.6.3). The ability of an individual to easily eavesdrop on such communications or record them on media for improper dissemination is an unnecessary risk.

The design of the video teleconferencing capability and facility must be approved by the CISO before purchase and installation. CBP shall develop standard operating procedures for the operations and maintenance of this capability. These procedures must specify that:

1. All participants must have the appropriate clearance and need-to-know
2. The video conferencing must be disabled when not in use
3. Any videotapes created of the teleconference must be appropriately labeled with the highest classification of the information contained on the videotape and secured in accordance with established media controls

4.5.4 Voice over Data Networks

Voice over Internet Protocol (VoIP) and similar technologies move voice digital networks. These technologies use protocols originally designed for data networking. Such technologies include Voice over frame relay, Asynchronous Transfer Mode (ATM), and Digital Subscriber Line (DSL).

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000182

Policy ID	CBP Policy Statements	Relevant Controls
4.5.4.a	Prior to any implementation of voice over data networks, a rigorous security risk assessment, security test and a business justification that includes a detailed technical solution shall be conducted before approval to proceed is granted. Any IT system that employs this technology must be certified and accredited for this purpose with residual risks clearly identified in the Accreditation Package.	SC-19
4.5.4.b	Security of voice communications service within CBP must include sufficient redundancy in the event of catastrophic outages that impact network IP-based communications and electric power, and to ensure that network outages do not result in the loss of both voice and data communications.	SC-19
4.5.4.c	CBP shall ensure appropriate identification and authentication controls, audit logging, and integrity controls are implemented on every component of their voice over data networks. Ensure that auditing is enabled and audit logs are reviewed on a regular basis.	SC-19
4.5.4.d	CBP shall ensure that physical access to voice over data network components is restricted to authorized personnel.	SC-19
4.5.4.e	A detailed engineering design of a VoIP service must address bandwidth, security, and Quality of Service (QoS) features. This effort is necessary to ensure that both data and voice traffic on the network have adequate bandwidth for effective performance and security controls commensurate with the security categorization of the network. (See FIPS PUB-199.)	SC-19
4.5.4.f	VoIP networks must include e-911 service.	SC-19
4.5.4.g	Dynamically opened ports for voice communications must immediately and properly close upon session disconnect.	SC-19
4.5.4.h	VoIP services will be subject to the same level and type of security monitoring as data services on CBP networks. That is to say, there shall be no expectation of privacy for any information transmitted across the network.	SC-19
4.5.4.i	VoIP network solutions must support the key CBP security objectives of confidentiality, integrity, availability and non-repudiation.	SC-19
4.5.4.j	Identification and authentication controls shall be implemented at both device and network levels.	SC-19
4.5.4.k	VoIP shall use encryption mechanisms that provide a commensurate level of protection for voice traffic that is equivalent to that provided for data on the same network. These levels are based on the sensitivity of information handled by the system and the security categorization of the system.	SC-19
4.5.4.l	VoIP networks must implement stateful firewall inspection, which understands VoIP, specifically H.323, the ITU specification for audio and video communication across the packetized networks. (Such firewalls can read	SC-19

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000183

Policy ID	CBP Policy Statements	Relevant Controls
	H.323 messages and dynamically open the correct ports for each channel as the protocol moves through its call setup process.)	
4.5.4.m	Security of voice communications service within CBP must include alternate communications systems in the event of catastrophic outages that impact network IP-based	SC-19

Responsibilities related to voice over data networks are provided below.

Voice Over Data Networks Responsibilities

CISO

- Formally review technical documentation for any proposed VoIP system before granting approval to proceed with the SLC and implementation processes.
- Ensure that rigorous security testing of the VoIP is an integral part of the C&A process.
- Ensure that VoIP network solutions support the key CBP security objectives of confidentiality, integrity, availability and non-repudiation.

IT Project Managers

- Ensure the design of voice over data network implementations have sufficient redundancy to ensure network outages do not result in the loss of both voice and data communications.
- Ensure that a detailed engineering design of a VoIP service addresses bandwidth, security, and Quality of Service (QoS) features. VoIP networks must also include e-911 service.
- Ensure appropriate identification and authentication controls, audit logging, and integrity controls are implemented on every component of their voice over data networks.

ISSOs

- Prior to any implementation of voice over data networks, ensure any inherent risks are clearly identified in the Accreditation Package to include a business justification that includes a detailed technical solution.
- Ensure that VoIP services are subject to the same level and type of security monitoring as data services on CBP networks. That is to say, there shall be no expectation of privacy for any information transmitted across the network
- Ensure physical access to voice over data network components is restricted to authorized personnel.
- Ensure appropriate identification and authentication controls, audit logging, and integrity controls are implemented on every component of their voice over data networks.
- Ensure that auditing is enabled and audit logs are reviewed on a regular basis.
- Ensure IT systems that employ VoIP technology have been certified and accredited for this purpose with residual risks clearly identified and addressed in the Accreditation Package.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000184

Voice Over Data Networks Responsibilities
Network/System Administrators • Ensure appropriate identification and authentication controls, audit logging, and integrity controls are properly configured on every component of their voice over data networks. • Ensure VoIP networks implement stateful firewall inspection, which understands VoIP, specifically H.323. • Ensure that dynamically opened ports for voice communications must immediately and properly close upon session disconnect. • Ensure that VoIP implementations employ encryption mechanisms that provide a commensurate level of protection for voice traffic that is equivalent to that provided for data on the same network. **Facility Managers** • Ensure physical access to voice over data network components is restricted to authorized personnel.

Voice over data networks cannot yet be considered a mature technology. Although various standards are currently being promulgated, there is little assurance at this time that systems that incorporate these capabilities can be adequately protected. Moreover, there are hidden costs associated with their use that make their implementation suspect on technical grounds other than security considerations. These include interoperability issues.

The implementation of these technologies is thus discouraged. Prior to implementing voice over data network technology, CBP must conduct rigorous risk assessments and security testing and provide Department business justification for their use. Furthermore, any IT systems that employ this technology must be certified and accredited for this purpose with residual risks clearly identified in the Accreditation Package. Redundancy can be accomplished by establishing major (trunk) links in a load balancing fashion. This concept involves having multiple pathways, which appear to be a single pathway in terms of addressing or routing. If one of the alternate pathways fails, the share of traffic that it was handling is distributed to the other pathways. If there is only one other pathway, the situation is known as "fail over." Such a failure should show an indication on the network monitoring tools. Technicians could then be dispatched to repair the failed component and return the link to full operation.

Information integrity is a significant security concern is information integrity. Frame Relay, Asynchronous Transfer Mode (ATM) and Digital Subscriber Line (DSL) facilities are usually provided by commercial entities. The fact that these links are not directly controlled by CBP staff mandates encryption of any data (including voice) that traverses these links. The contractual arrangements with these suppliers must specify that only United States citizens shall be involved in the maintenance and operation of these links.

Authentication controls and audit logging can be provided by the same technologies that provide these capabilities for digital data traffic. VoIP standards also include (among others) a specification of a Media Gateway Control Protocol (MGCP), which also collects audit information.

Voice over IP (VoIP) is a relatively new technology. As with most new technologies, there are numerous vendor-specific protocols and numerous standards in development. Many of the security issues related to VoIP are dependent upon vendor selection and architecture design. Rigorous testing and clear business justification should be completed before the AO approves the use of this technology.

4.6 Wireless Communications

Wireless communications technologies include the following:

1. Wireless systems (e.g., wireless local area networks [WLAN], wireless wide area networks [WWAN], wireless personal area networks [WPAN], peer-to-peer wireless networks, IT systems that leverage commercial wireless services). Wireless systems include the transmission medium, stationary integrated devices, firmware, supporting services, and protocols.

2. Wireless portable electronic devices (PED) capable of storing, processing, or transmitting sensitive information (e.g., personal digital assistants [PDA], smart telephones, two-way pagers, handheld radios, cellular telephones, personal communications services [PCS] devices, multifunctional wireless devices, portable audio/video recording devices with wireless capability, scanning devices, and messaging devices).

3. Wireless tactical systems, including mission-critical communication systems and devices (e.g., include Land Mobile Radio [LMR] subscriber devices and infrastructure equipment, remote sensors, and technical investigative communications systems).

4. Radio Frequency Identification (RFID).

General policies pertaining to all wireless communications technologies are provided in this section. Policies more specific to wireless systems, wireless PEDs, wireless tactical systems, and RFID are provided in Sections 4.6.1, 4.6.2, 4.6.3, and 4.6.4, respectively.

The DHS Wireless Management Office (WMO) must be notified within 30 days of all wireless communications systems acquisitions. CBP shall follow the procedures outlined in Section 1.10, Waivers and Exceptions when requesting waivers or exceptions.

CBP must implement and enforce a key management plan consistent with DHS PKI Policy Authority when employing encryption on wireless technologies. The key management plan shall clearly define the practices, procedures, and techniques used to enforce the key management policy and functional requirements. Representative guidance may be drawn from the draft NIST SP 800-57, *Recommendation for Key Management – Part 2: Best Practices for Key Management Organization (2002).*

For wireless technologies classified as general support systems or major applications, the key management plan must be addressed in the System Security Plan (SSP).

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000186

Policy ID	CBP Policy Statements	Relevant Controls
4.6.a	Wireless communications technologies are generally prohibited from use within CBP unless the appropriate AO specifically approves a technology and application.	AC-18
4.6.b	When using PKI-based encryption on wireless systems, wireless PEDs, and wireless tactical systems shall implement and maintain a key management plan approved by the DHS PKI Policy Authority.	IA-5, SC-12

Wireless communications responsibilities are provided below.

Wireless Communications Responsibilities

PKI Policy Authority

- Establishes and enforces the security requirements detailed in the key management plan.

AO

- Specifically approve or prohibit the use of wireless communications technologies within CBP.
- Approve the implementation and use of the key management plan at acceptable risk levels.
- Ensure appropriate and effective security measures are included in the key management plan.
- Approve migration plans for transitioning legacy wireless systems.
- Notify the WMO and the DHS Enterprise Architecture Center of Excellence (EACOE) of any approval action.

DHS CISO

- Review waivers and exceptions to wireless systems policy.
- Vet wireless security-related issues to the WMO.

CISO

- Advise system owners and IT project managers concerning the implementation of key management plans.
- Enforce CBP key management policy and procedures.

ISSOs

- Ensure key management security controls and functional requirements are implemented.
- Ensure security assessments are conducted to evaluate the effectiveness of security objectives and controls supported by the key management plan.

System/Network Administrators

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000187

Wireless Communications Responsibilities
• Implement and enforce technical security mechanisms specified in key management plan.
Managers, Supervisors, and Employees
• Adhere to CBP policy concerning the use of wireless communications technologies.
• Adhere to CBP policy concerning key management policy and procedures.

4.6.1 Wireless Systems

Wireless systems include wireless local area networks (WLAN), wireless wide area networks (WWAN), wireless personal area networks (WPAN), peer-to-peer wireless networks (i.e., ad hoc wireless networks), and IT systems that leverage commercial wireless services.

Wireless systems allow mobile devices, wired devices, and other devices to process, store, or transmit sensitive information using radio frequency (RF) or infrared (IR) capabilities. Wireless systems are vulnerable to a number of traditional attacks and attacks specific to wireless technologies. These attacks fall into the following categories: unauthorized access, denial-of-service/jamming/interference, signal detection/eavesdropping, spoofing/masquerading, and message modification. The use of appropriate countermeasures will help ensure that wireless systems to be deployed will comply with CBP information security policy.

Attachment Q1, Wireless Systems, provide guidance for CBP to use in developing and implementing security for wireless systems.

Policy ID	CBP Policy Statements	Relevant Controls
4.6.1.a	Annual security assessments shall be conducted on all approved wireless systems. Wireless security assessments shall enumerate vulnerabilities, risk statements, risk levels, and corrective actions.	CA-2
4.6.1.b	Risk mitigation plans shall be developed to address wireless security vulnerabilities. These plans shall prioritize corrective actions and implementation milestones in accordance with defined risk levels.	CA-5
4.6.1.c	Cost-effective countermeasures to denial-of-service attacks shall be identified and established prior to a wireless system being approved for use.	AC-19, SC-5
4.6.1.d	System Security Plans shall adopt a defense-in-depth strategy that integrates firewalls, screening routers, wireless intrusion detection systems, antivirus software, encryption, strong authentication, and cryptographic key management to ensure security solutions and secure connections to external interfaces are consistently enforced.	SI-3
4.6.1.e	Legacy wireless systems that are not compliant with DHS information security policy shall implement a migration plan to outline the provisions, procedures, and restrictions for transitioning these systems to DHS-compliant security	CA-5

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000188

Policy ID	CBP Policy Statements	Relevant Controls
	architectures. Operation of these noncompliant systems requires an approved waiver or exception to policy from the DHS CISO, as appropriate.	
4.6.1.f	Wireless technology implementations will be evaluated by the Security and Technology Policy (STP) Branch on a project-by-project basis and require approval by the CISO prior to final approval by the CBP AO.	AC-18
4.6.1.g	At a minimum, all wireless designs must undergo C&A in accordance with federal, DHS and CBP policy. Compliance with wireless system configuration and hardening guidelines (e.g., NIST SP 800-48) is mandatory and shall be detailed in the C&A documentation.	AC-18
4.6.1.h	CBP data must not be transmitted, unprotected over a wireless network.	AC-18
4.6.1.i	All elements of CBP must seek appropriate assistance from the STP Branch prior to placing any CBP operational data onto a wireless device.	AC-19
4.6.1.j	Control measures such as end-to-end encryption and strong (two-factor) authentication are required when there is a need to transmit CBP production data via a wireless network.	AC-18
4.6.1.k	Encryption of CBP unclassified data for transmission to and from wireless devices is required. At a minimum, data encryption must be implemented end-to-end over an assured channel and use only cryptographic modules that are FIPS 197 (AES-256) compliant and have received FIPS 140-2 validation.	AC-18
4.6.1.l	As part of the C&A process, wireless devices must undergo rigorous security testing prior to being granted Approval-To-Operate in the production environment.	AC-19
4.6.1.m	Due to the inherent risks involved with wireless technologies, frequent risk assessment and security testing and evaluation of system controls must be conducted for deployed wireless technologies.	AC-18
4.6.1.n	Strong authentication, identification, and non-repudiation are required for wireless access to a CBP information system in accordance with published CBP and DHS policy and procedures.	AC-18
4.6.1.o	Wireless messaging devices must be configured to lock out logon attempts after ten unsuccessful logon attempts.	AC-19
4.6.1.p	Wireless devices shall not be used for storing, processing, or transmitting classified information.	AC-19
4.6.1.q	Countermeasures shall be taken to mitigate denial of service attacks. These measures shall address external threats and potential interference from friendly sources.	AC-18
4.6.1.r	Wireless technologies/devices used to store, process, and/or transmit information shall not be operated in areas where classified information is electronically stored, processed, or transmitted.	AC-19

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000189

Policy ID	CBP Policy Statements	Relevant Controls
4.6.1.s	The Wireless Personal Area Network (WPAN) capability must be removed or physically disabled from a device unless cryptographic modules are FIPS 197 (AES-256) compliant and have received FIPS PUB 140-2-validation. Exceptions may be granted on a case-by-case basis only as determined by the AO.	AC-18
4.6.1.t	On wireless messaging devices pin-to-pin messaging potentially permits unencrypted messaging between wireless devices and must be disabled.	AC-19
4.6.1.u	The CBP STP Branch shall actively screen for wireless devices. Active electromagnetic sensing at CBP or contractor premises to detect/prevent unauthorized access of CBP information systems shall be performed by the STP Branch. Periodic scanning ensures compliance with the CBP C&A process and wireless configuration requirements.	AC-18
4.6.1.v	CBP wireless devices and network configurations shall limit access to the CBP network to authorized devices and authorized users only by enabling Media Access Control (MAC) filtering.	AC-18
4.6.1.w	The Service Set Identifier (SSID) broadcast feature shall be disabled to reduce availability of the access point identifier to the general public.	AC-18
4.6.1.x	CBP-owned wireless devices shall be configured to enable wireless connections to CBP network access points only.	AC-19
4.6.1.y	Strategic placement of CBP wireless access points and antenna attenuation shall be designed to minimize risks of eavesdropping or access by unauthorized users. Building construction and location can impact control of wireless technology and must be considered and tested comprehensively for any wireless implementation.	AC-18
4.6.1.z	CBP system administrators shall maintain accurate labeling and inventories of fielded wireless and handheld devices.	AC-19
4.6.1.aa	All wireless equipment and software must be under Configuration Management (CM)/change control to ensure that software releases for security enhancements and patches for vulnerabilities are properly managed across the enterprise. Patch updates must follow the guideline set forth in section 4.9.5 Vulnerability Management.	AC-18 PL-2 SI-2
4.6.1.bb	Wireless devices must be managed at the device level to enforce security configuration, use of strong passwords, and to enable remote shut down of devices in case of theft/loss and deletion of sensitive data on device memory.	AC-19
4.6.1.cc	STP Branch shall monitor wireless industry for new products and changes to standards that enhance security features and evaluate them for inclusion in the CBP Security Architecture Solutions Catalog and the Technical Reference Model (TRM).	AC-18
4.6.1.dd	Should an IT resource (e.g., laptop, wireless device, smartcard) be lost or stolen, immediately report the loss or theft to the Information System Security Officer (ISSO), supervisor/manager and the CSIRC. After the CSIRC has	AC-19

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000190

Policy ID	CBP Policy Statements	Relevant Controls
	been contacted, the CSIRC staff will ensure that the investigation, analysis, documentation, and resolution of the reported incident are conducted.	

Questions regarding introduction of wireless technologies into standard uses as a standalone or as part of a network project shall be addressed to the CISO at SecurityPolicy@dhs.gov .

Wireless system responsibilities are provided below.

Wireless System Responsibilities

AO

- Approve the use of standards-based wireless system technologies.
- Approve the implementation and use of wireless systems at a specified risk level during the C&A process.
- Ensure appropriate and effective security measures are included in the System Security Plan.

CISO

- Advise System Owners and IT project managers concerning the implementation of wireless technologies.
- Enforce CBP policy concerning wireless systems.
- Enforce CBP policy concerning the reporting requirements for wireless security vulnerability assessments.

System Owners/IT Project Managers

- Develop risk mitigation plans for prioritizing corrective actions and implementation milestones.
- Develop migration plans that outline provisions, procedures, and restrictions for transitioning legacy wireless systems to DHS-compliant security architectures.

ISSOs

- Ensure wireless systems security controls are properly implemented and configured and are addressed in the System Security Plan.
- Ensure routine security assessments are accomplished on wireless systems to identify unauthorized wireless devices, backdoors, and other system vulnerabilities, and to enumerate vulnerabilities, risk statements, risk levels, and corrective actions.
- Implement risk mitigation plans for prioritizing corrective actions and achieving implementation milestones.
- Implement migration plans that outline provisions, procedures, and restrictions for transitioning legacy wireless systems to DHS-compliant security architectures.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000191

Wireless System Responsibilities
System/Network Administrators • Ensure wireless system security controls are properly implemented and configured in accordance with the System Security Plan. • Ensure routine security assessments are accomplished on wireless systems to identify rogue access points, backdoors, and other system vulnerabilities, and to enumerate vulnerabilities, risk statements, risk levels, and corrective actions. **Managers, Supervisors, and Employees** • Adhere to CBP policy concerning the use of wireless systems to process, store, or transmit sensitive information. • Adhere to CBP policy concerning the use of wireless systems in areas where sensitive information is being discussed.

4.6.2 Wireless Portable Electronic Devices

Wireless PEDs include personal digital assistants (PDA), smart telephones, two-way pagers, handheld radios, cellular telephones, personal communications services (PCS) devices, multifunctional wireless devices, portable audio/video recording devices with wireless capability, scanning devices, messaging devices, and any other wireless clients capable of storing, processing, or transmitting sensitive information.

NOTE: There is currently no DHS-approved encryption software for PEDs, although CBP may be using products that provide adequate protection. As DHS or National Security Agency (NSA) standards are established, they will be discussed in this section of the handbook.

Personally owned PEDs are not authorized to process, transmit, or store sensitive or classified information. Personally owned PEDs may not be connected to sensitive or classified systems or networks.

Government-owned PEDs can be used in conjunction with CBP networks or systems (to include any downloading of data from a user's workstation to these devices) only if the current C&A documentation specifically addresses the inherent risks associated with their use and the AO evaluates and accepts any residual risk. Re-certification and accreditation are required if these issues are not currently addressed in the most current C&A documentation.

System owners and IT project managers must identify and implement as many countermeasures as appropriate to strengthen the security of wireless PEDs. These countermeasures include the use of passwords, personal firewalls, and antivirus software; the monitoring of malicious activities; the use of modification detection software and of software that will allow the device to dynamically identify and adapt to each wireless mode of operation; the tracking of data and assets; and management protocols. Countermeasures should allow the system administrator to maintain a user and community profile through unit identification and validation, which would in turn allow administrators to remove data, update software, and log and track unauthorized removal where appropriate.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000192

Because of their portability and mobility, PEDs are also extremely susceptible to theft, physical damage, and loss—all of which could lead to compromise of information.

CBP shall develop and maintain a property inventory list of all PEDs authorized for use. This list is to include serial numbers and/or seat numbers, user names, use, and location of all PEDs for accountability purposes. Each CBP-owned PED is to have an asset tag, whose number is included in the inventory list. Rules of behavior for PEDs must be published and enforced.

CBP Attachment Q2 *(Wireless Portable Electronic Devices)* provides guidance for CBP to use in developing and implementing wireless PED security.

Policy ID	CBP Policy Statements	Relevant Controls
4.6.2.a	The use of wireless PEDs and accessory devices in areas where sensitive or classified information is discussed is prohibited unless specifically authorized by the CBP AO in writing.	AC-19, PL-4
4.6.2.b	Wireless PEDs shall not be connected physically or wirelessly to the CBP-wired core network without written consent from the AO.	AC-18, AC-19
4.6.2.c	Wireless PEDs shall not be used to store, process, or transmit combinations, personal identification numbers (PIN), or sensitive information in unencrypted formats.	AC-19, IA-5, IA-7
4.6.2.d	Wireless PEDs such as BlackBerry devices and smartphones shall implement strong identification, authentication, data encryption, and transmission encryption technologies. Portable electronic devices such as BlackBerry devices and smartphones shall be password-protected, with a security timeout period established. For BlackBerry devices, the security timeout shall be set to 10 minutes.	AC-19, IA-7, SC-8, SC-9, SC-13
4.6.2.e	System Security Plans shall promulgate the provisions, procedures, and restrictions for using wireless PEDs to download mobile code in an approved manner.	---
4.6.2.f	Wireless PEDs shall be operated only when current CBP Technical Reference Model (TRM)-approved versions of antivirus software and software patches are installed.	---
4.6.2.g	Cost-effective countermeasures to denial-of-service attacks shall be identified and established prior to a wireless PED being approved for use.	---
4.6.2.h	A current inventory of all approved wireless PEDs in operation shall be maintained.	---
4.6.2.i	Wireless PEDs shall be cleared of all information before being reused by another individual, office, or before they are surplused; wireless PEDs that are being disposed of, recycled, or returned to the owner or manufacturer shall first be sanitized using approved procedures.	---
4.6.2.j	Legacy wireless PEDs that are not compliant with CBP information security policy shall implement a migration plan that outlines the provisions,	---

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000193

Policy ID	CBP Policy Statements	Relevant Controls
	procedures, and restrictions for transitioning these wireless PEDs to DHS-compliant security architectures. Operation of these noncompliant systems requires an approved waiver or exception from the DHS CISO, as appropriate.	
4.6.2.k	Personally owned PEDs shall not be used to process, store, or transmit sensitive CBP information.	AC-19, PE-18
4.6.2.l	The AO shall approve the use of Government-owned PEDs to process, store, or transmit sensitive information.	---
4.6.2.m	The use of add-on devices such as cameras and recorders is not authorized unless approved by the AO. Functions that can record or transmit sensitive information via video, IR, or RF shall be disabled in areas where sensitive information is discussed.	AC-19, CM-7, PE-18, SC-7
4.6.2.n	For data at rest, all wireless Portable Electronic Devices (PEDs), including Personal Digital Assistants (PDAs) and laptops, shall use file encryption that are FIPS 197 (AES-256) compliant and have received FIPS 140-2 validation requirements.	AC-19

Wireless portable electronic device responsibilities are provided below.

Wireless Portable Electronic Device Responsibilities

AO

- Approve the use of Government-owned, DHS-approved wireless PEDs and accessory devices to connect, process, store, or transmit sensitive information.
- Ensure appropriate and effective security measures are included in the System Security Plan.
- Authorize the use of Government-owned wireless PEDS and accessory devices in areas where sensitive information is discussed.
- Evaluate the risk associated with authorizing wireless PEDs to connect, process, store, transmit, or access sensitive information and systems during the C&A process.
- Approve/disapprove the use of mobile code (e.g., ActiveX).

System Owners/IT Project Managers

- Develop risk mitigation plans for prioritizing corrective actions and implementation milestones.
- Develop migration plans that outline provisions, procedures, and restrictions for transitioning legacy wireless PEDs to CBP-compliant security architectures.
- Maintain an inventory of all approved wireless PEDs in operation.

CISO

- Enforce CBP policy on the use of wireless PEDs and accessory devices in areas where

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000194

Wireless Portable Electronic Device Responsibilities

sensitive information is discussed.

- Enforce CBP policy concerning the use of wireless PEDs and accessory devices to connect, store, process, or transmit combinations, PINs, or sensitive information.
- Develop procedures for implementation of strong identification, authentication, data encryption, and transmission encryption for wireless PEDs to protect sensitive information from compromise.
- Enforce CBP policy concerning the use of mobile code and antivirus software on wireless PEDs.
- Identify and establish cost-effective countermeasures to denial-of-service attacks for wireless PEDs.

ISSOs

- Ensure wireless PEDs are not permitted in areas where sensitive information is discussed unless authorized in writing by the AO.
- Enforce CBP policy concerning the use of wireless PEDs to process, store, or transmit sensitive information.
- Enforce CBP policy concerning the use of mobile code and antivirus software on wireless PEDs.
- Implement cost-effective countermeasures to denial-of-service attacks for wireless PEDs.
- Ensure that all information is cleared from wireless PEDs that are to be reused or surplused; ensure that all information is sanitized from wireless PEDs that are being disposed of, recycled, or returned to the owner or manufacturer (see Section 4.3.3, Media Sanitization and Disposal, for approved procedures).
- Implement migration plans that outline provisions, procedures, and restrictions for transitioning legacy wireless PEDs to CBP-compliant security architectures.
- Enforce prohibition of add-on devices such as cameras and recorders.
- System/Network Administrators
- Ensure wireless PED security controls are properly implemented and configured in accordance with the Systems Security Plan.
- Ensure routine security assessments are accomplished on wireless PEDs.

Managers, Supervisors, and Employees

- Adhere to CBP policy concerning the use of wireless PEDs in areas where sensitive information is being discussed.
- Adhere to CBP policy concerning the use of wireless PEDs to process, store, transmit, or access combinations, PINs, or sensitive information.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000195

The differences among wireless PEDs are becoming less clear-cut as voice communications, email, calendars, text messaging, Internet capabilities, and other services converge on integrated PED platforms. These product innovations—while they improve mobility, flexibility, portability, and economies of scale—are subject to all the threats, vulnerabilities, and security risks inherent in evolving wireless technologies.

4.6.2.1 Cellular Phones

Cellular phones used in areas where sensitive information is discussed have the same inherent vulnerabilities as cordless telephones and speakerphones as discussed in Section 4.4.2. They potentially allow a discussion of sensitive information being held in the same area to be overheard by a third party who would not normally have access to such information.

As is the case with traditional telephones, cellular communications can be intercepted. However, the interception of conversations over telephones requires the insertion of a monitoring device; the interception of cellular communications does not, and information transmitted by cellular phones can be intercepted at reasonably great distances. An individual could be in a neighboring building or in the street outside the building and monitor conversations that are within the reach of the microphone in the cellular phone. In fact, cellular phone credentials can be cloned to other phones, allowing the "cloned" phone to masquerade as the original phone and allow covert monitoring of conversations near the original caller.

Policy ID	CBP Policy Statement	Relevant Controls
4.6.2.1.a	CBP shall develop guidance for discussing sensitive information on cellular phones. Guidance shall be approved by a senior CBP official and is subject to review by the DHS CISO and the DHS Wireless Management Office. Under no circumstances shall classified information be discussed on cellular phones.	PL-4

Cellular phone responsibilities are provided below.

Cellular Phone Responsibilities
Managers • Ensure employees are aware of CBP policy prohibiting the discussion of sensitive CBP information while using a wireless telephone. **Users** • Ensure sensitive CBP information is not discussed while using a wireless telephone.

4.6.2.2 Pagers

Text pagers can send text messages up to 110 or 160 characters long, depending on the carrier. Text messages also can be sent from a cellular service provider's Web page, or from Web sites that allow users to send text messages for free. Pagers have the same inherent vulnerabilities as cellular phones with respect to exposure of sensitive information to unauthorized recipients (see Section 4.6.2.1).

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000196

Text messages rely on the service provider's network and are not encrypted. There is thus no assurance of the security of these services. Moreover, text-message devices can be spammed with text messages until the user's mailbox is full and the user can no longer receive new text messages until previously stored messages are deleted.

Pagers shall not be used to transmit information that is explicitly labeled as sensitive or classified. In addition, pagers should not be used to transmit information on computer or network problems or status. This information could be intercepted and used to identify the configuration and possibly the location of IT assets, which could be then be targeted for attack by an outsider or untrustworthy insider.

A preferred alternative to transmitting text messages is to page an individual with a phone number and require the individual to call that number using a traditional (i.e., non-cellular or non-mobile) telephone in a location where the conversation could not be monitored by others in the immediate area and where sensitive information can safely be discussed.

Policy ID	CBP Policy Statement	Relevant Controls
4.6.2.2.a	Pagers shall not be used to transmit sensitive information.	PL-4

Pager responsibilities are provided below.

Pager Responsibilities
Managers • Ensure employees are aware of CBP policy prohibiting the transmission of sensitive CBP information to pagers. **Users** • Ensure sensitive CBP information is not transmitted to pagers.

4.6.2.3 Multifunctional Wireless Devices

Wireless devices have evolved to be multifunctional (cell phones, pagers, and radios can surf the Internet, retrieve email, take and transmit pictures, etc), and most of these functions have no security.

Where there is a strong business justification for their use, CBP-owned wireless devices can be equipped to allow synchronization with approved CBP owned computers. Data is encrypted or decrypted, as needed, for synchronization with computer based personal information managers (PIMs) and other programs.

The risk assessment for multifunctional wireless devices is to include an assessment of the risks associated with all the functions, including infrared (IR), radio frequency (RF), and video. The AO must approve the associated risks identified by the risk assessment. Based on the sensitivity and classification of the data and the associated risk from the risk assessment, the AO may allow the use of multifunctional wireless devices.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000197

Use of peripheral devices must be tightly controlled. Audio and video recording capabilities should be prohibited unless specifically required for an individual's duties. Unauthorized recordings of sensitive conversations or images of sensitive equipment could be used to compromise the security of the CBP.

Policy ID	CBP Policy Statements	Relevant Controls
4.6.2.3.a	Functions that cannot be encrypted using approved cryptographic modules shall not be used to process, store, or transmit sensitive information.	AC-19, SC-8, SC-9, SC-12
4.6.2.3.b	Functions that transmit or receive video, infrared (IR), or radio frequency (RF) signals shall be disabled in areas where sensitive information is discussed.	AC-19, PE-18
4.6.2.3.c	Short Message Service (SMS) and Multimedia Messaging Service (MMS) shall not be used to process, store, or transmit sensitive information, and shall be disabled whenever possible.	---

Multifunctional wireless device responsibilities are provided below.

Multifunctional Wireless Device Responsibilities
AO • Approve the implementation of multifunctional wireless devices at an acceptable level of risk. • Ensure that the System Security Plan adequately addresses the protection of sensitive material accessed and stored on multifunctional wireless devices prior to accreditation. **IT Project Managers/System Owners** • Ensure security requirements for multifunctional wireless devices are communicated to the IT project manager and system administrators. **System/ Network Administrators** • Ensure that multifunctional wireless devices are configured properly with encryption enabled to prevent unauthorized access, disclosure, damage, modification, or destruction of data. • Ensure multifunctional wireless devices are periodically scanned for rogue access points and other vulnerabilities. **ISSOs** • Ensure that the System Security Plan addresses the protection of sensitive material accessed and stored on wireless devices. • Ensure that security requirements for multifunctional wireless devices are addressed in the

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000198

Multifunctional Wireless Device Responsibilities
System Security Plan and rules of behavior. • Ensure routine security assessments are accomplished on multifunctional wireless devices to identify rogue access points, backdoors, and other system vulnerabilities, and to enumerate vulnerabilities, risk statements, risk levels, and corrective actions.

4.6.3 Wireless Tactical Systems

Wireless tactical systems include Land Mobile Radio (LMR) subscriber devices, infrastructure equipment, remote sensors, and technical investigative communications systems. Because they are often deployed under circumstances in which officer safety and mission success are at stake, wireless tactical systems require even greater security measures. To ensure secure tactical communications, CBP must implement strong identification, authentication, and encryption protocols designed specifically for each wireless tactical system.

Wireless tactical communications systems are also subject to issues such as technology advances, standards, and functional convergence. As their use of wireless tactical communications systems evolves, develop and implement plans for migration to the new technologies. The AO must ensure that these migration plans are consistent with CBP policy and that appropriate waivers or exceptions have been obtained.

LMR systems are the primary means of wireless communications. Security and risk management principles must be included in every phase of the LMR system development lifecycle. LMR network communications traffic should include encryption and security controls such as those specified by NIST Federal Information Processing Standard (FIPS) 140-2, *Security Requirements for Cryptographic Modules* (May 2001), and FIPS 197, *Advanced Encryption Standard (AES)* (November 2001). LMR subscriber units can periodically update and rekey encryption protocols manually by using a handheld key variable loader (KVL) or automatically via OTAR techniques. With OTAR technology, radios can be rekeyed within seconds over the air from a remote location—allowing for easier and more regular rekeying, and resulting in improved security. In addition, the OTAR channel can be used for digital voice transmissions in the encrypted mode for emergency interoperability.

LMR security and policy guidelines and standards defined by Project 25 (P25) should be implemented where appropriate. The primary objectives of the P25 standards are to promote interoperability among digital or analog LMR equipment used by various levels of Government, support backward compatibility with legacy LMRs, enhance spectrum efficiency, and maximize economies of scale. Therefore, all CBP LMRs shall be built on P25-compliant platforms or shall be capable of interfacing with P25-compliant platforms to ensure homeland security requirements can be satisfied in a timely manner. Waivers or exceptions to this requirement must be approved in writing by the DHS CISO. (See Section 1.10)

Wireless tactical system policy and procedures are described more completely in Attachment Q3 (*Wireless Tactical Systems*) to the DHS 4300A *Sensitive Systems Handbook*.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000199

Policy ID	CBP Policy Statements	Relevant Controls
4.6.3.a	AOs shall be immediately notified when any security features are disabled in response to time-sensitive, mission-critical incidents.	CM-3
4.6.3.b	Wireless tactical systems shall implement strong identification, authentication, and encryption.	IA-2, IA-7, SC-8, SC-9
4.6.3.c	Cost-effective countermeasures to denial-of-service attacks shall be identified and established prior to a wireless tactical system being approved for use.	SC-5
4.6.3.d	A current inventory of all approved wireless tactical systems in operation shall be maintained.	---
4.6.3.e	Legacy tactical wireless systems that are not compliant with CBP IT security policy shall implement a migration plan to outline the provisions, procedures, and restrictions for transitioning these systems to CBP-compliant security architectures. Operation of these noncompliant systems requires an approved waiver or exception from the DHS and/or CISO. (See Section 1.10)	---
4.6.3.f	The security configuration of Land Mobile Radio (LMR) subscriber units shall be validated via over-the-air-rekeying (OTAR) or hard rekey using a crypto-period no longer than 180 days.	SC-12
4.6.3.g	All LMR systems shall comply with Project 25 (P25, EIA/TIA-102) security standards where applicable.	CM-2

Wireless tactical system responsibilities are provided below.

Wireless Tactical System Responsibilities

AO

- Approve the use of wireless tactical systems technologies.
- Approve the implementation and use of wireless tactical systems to process, store, or transmit sensitive information at acceptable risk levels during the C&A process.
- Ensure security measures are included in the System Security Plan.
- Evaluate and submit waivers and exceptions to the CISO for wireless tactical systems when compliance with CBP information security policy could potentially compromise tactical investigations, endanger personnel safety, or put the public at risk. (See Section 1.10)

System Owners/IT Project Managers

- Implement cost-effective security measures specified in the System Security Plan including strong identification, authentication, and encryption.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000200

Wireless Tactical System Responsibilities

- Ensure the AO is immediately notified when any security features are disabled in response to time-sensitive, mission-critical incidents.
- Ensure allocation of resources to support security requirements and enforcement controls specified in the System Security Plan.
- Ensure tactical wireless communication security requirements are communicated to ISSOs and system administrators.
- Develop and implement migration plans that outline provisions, procedures, and restrictions for transitioning legacy wireless tactical systems to CBP-compliant security architectures.
- Maintain an inventory of all wireless tactical systems used to process, store, and transmit sensitive information.
- Ensure all LMR systems comply with Project 25 (P25, EIA/TIA-102) security standards where applicable.

CISO

- Enforce CBP policy concerning the use of tactical communication systems to process, store, transmit, or access sensitive information.
- Develop and enforce CBP policy concerning mitigation measures for denial-of-service (DoS) attacks.
- Enforce LMR system compliance with Project 25 (P25, EIA/TIA-102) security standards.

ISSOs

- Ensure the AO is immediately notified when any security features are disabled in response to time-sensitive, mission-critical incidents.
- Implement DHS policy concerning the use of tactical communication devices to process, store, transmit, or access sensitive information.
- Ensure that any tactical communication devices used to process sensitive information are not permitted in conference rooms or secure facilities where sensitive information is discussed without written authorization from the AO.
- Perform security assessments and validate the security posture of land mobile radio (LMR) subscriber units via over-the-air rekeying (OTAR) or hard rekeying using a crypto-period no longer than 180 days.
- Ensure that all information is cleared from wireless tactical systems that are to be reused or surplused; ensure that all information is sanitized from wireless tactical systems that are being disposed of, recycled, or returned to the owner or manufacturer (see Section 4.3.3, Media Sanitization and Disposal, for approved procedures).

Managers / Supervisors

- Ensure the AO is immediately notified when any security features are disabled in response to time-sensitive, mission-critical incidents.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000201

Wireless Tactical System Responsibilities
• Ensure employees are aware of CBP policy and procedure for discussing sensitive information while using tactical communication devices.
Employees
• Adhere to CBP policy and procedures concerning the use of tactical communication devices that access, process, store, or transmit sensitive information and systems.

4.6.4 Radio Frequency Identification

Radio Frequency Identification (RFID) enables objects to be identified wirelessly over significant distances. Because of the computing limitations of RFID tags, it often is not feasible to implement many of the security mechanisms, such as cryptography and strong authentication that are commonly supported on personal workstations, servers, and network infrastructure devices. RFID security controls can support Departmental and CBP privacy objectives, mitigate risks to business processes, and prevent the disclosure of sensitive data.

CBP Attachment Q4, *Sensitive RFID Systems*, provides guidance for CBP to use in developing and implementing RFID security.

Policy ID	CBP Policy Statements	Relevant Controls
4.6.4.a	When implementing RFID systems assess the hazards of electromagnetic radiation to fuel, ordinance, and personnel before deployment of the RFID technology.	PE-18
4.6.4.b	Limit data stored on RFID tags to the greatest extent possible, recording information beyond an identifier only when required for the application mission. When data beyond an identifier is stored on a tag, the tag's memory shall be protected by access control. If Personally Identifiable Information (PII) is in any way persisted on the RFID tag or chip, the Authorizing Official (AO) will certify that this is an operational necessity which cannot be satisfied in any other way.	AC-6, PL-5
4.6.4.c	Program offices shall develop a contingency plan, such as the use of a fallback identification technology, to implement in case of an RFID security breach or system failure.	—
4.6.4.d	Program offices shall identify and implement appropriate operational and technical controls to limit unauthorized tracking or targeting of RFID-tagged items when these items are expected to travel outside CBP's physical perimeter.	AC-14
4.6.4.e	When the RFID system is connected to a DHS data network, CBP shall implement network security controls to appropriately segregate RFID network components such as RFID readers, middleware, and databases from other non-RFID network hosts.	CM-6

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000202

Policy ID	CBP Policy Statements	Relevant Controls
4.6.4.f	When implementing RFID technology, Program Offices shall determine whether or not tag cloning is a significant business risk. If such a significant risk exists, then tag transactions shall be cryptographically authenticated.	IA-7, RA-3
4.6.4.g	Compliance with RFID system configuration and hardening guidelines (e.g., NIST SP 800-98) is mandatory and shall be detailed in the C&A documentation.	AC-18

4.7 Overseas Communications

Overseas communications have different security requirements than domestic communications. The Department of State has published a series of Foreign Affairs Manuals relevant to this requirement.

Policy ID	CBP Policy Statement	Relevant Controls
4.7.a	Where required or appropriate, all overseas communications shall be in accordance with the Department of State Foreign Affairs Manual (FAM), 12 FAM 600, *Information Security Technology*.	---

Overseas communications responsibilities are provided below.

Overseas Communications Responsibilities
DHS CISO • Establishes and enforces policy relating to overseas communications. **CISO** • Ensure CBP IT systems under their purview comply with Department of State 12 FAM 600, *Information Security Technology*, for systems that communicate with overseas locations. **IT Project Managers/System Owners** • Ensure IT systems under their control or under development that will communicate with overseas locations comply with the requirements of Department of State 12 FAM 600, *Information Security Technology*. **System/Network Administrators** • Ensure that IT systems under their control that will communicate with overseas locations are properly configured and maintained to comply with the requirements of Department of State 12 FAM 600, *Information Security Technology*. **ISSOs** • Ensure IT systems under their control that communicate with overseas locations comply

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000203

Overseas Communications Responsibilities
with Department of State 12 FAM 600, *Information Security Technology*.

Wireless communications are highly vulnerable to interception and monitoring. CBP employees overseas must be informed of the risks and the appropriate precautions they should follow when using wireless devices overseas. Use of secure wireless devices overseas must be approved by the CISO.

The following 600 Series Foreign Affairs Manuals are provided for reference along with their current Internet links:

12 FAM 610 Organization and Purpose of Computer Security (COMPUSEC)
http://www.foia.state.gov/masterdocs/12fam/12m0610.pdf

12 FAM 620 Unclassified Automated Information Systems
http://www.foia.state.gov/masterdocs/12fam/12m0620.pdf

12 FAM 630 Classified Automated Information Systems
http://www.foia.state.gov/masterdocs/12fam/12m0630.pdf

12 FAM 640 Domestic and Overseas Automated Information Systems Connectivity
http://www.foia.state.gov/masterdocs/12fam/12m0640.pdf

12 FAM 650 Acquisition Security Requirements for Operating Systems and Subsystem Components
http://www.foia.state.gov/masterdocs/12fam/12m0650.pdf

12 FAM 660 Communications Security (this subchapter has been designated Sensitive—NOFORN and is not available via the Internet; contact the Department of State for a paper version)

4.8 Equipment

This section addresses the use and maintenance of computer equipment. It stresses the importance of individual accountability in protecting these resources. Equipment security encompasses workstations, laptops, other mobile computing devices, personally owned equipment, and the maintenance of these items.

The emergence of new technology always seems to outpace policy developed to regulate its use in the CBP environment. Therefore, any new technology must first be assessed for inclusion in the CBP Enterprise Architecture (EA) managed by the Technology Architecture and Engineering Branch and, for consistency, with the Enterprise Security Services (ESS) Architecture. Devices approved for use in CBP will become part of the Enterprise Architecture (EA) and listed in the Technical Reference Model (TRM). The EA Repository enables reuse by documenting the existence and characteristics of reusable artifacts and provides users with a reference mechanism. The TRM and the EA form the foundation for CBP information technology insertion standards.

As part of the technology assessment process, each proposed product should be investigated to determine the extent to which it:

- Has been independently security tested (e.g., by NSA or NIST)

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000204

- Meets the relevant security requirements including its potential adverse impact on the ability of interconnected products to meet their security requirements
- Is consistent with the security mandates in this handbook
- Provides reasonable and appropriate security within the defined context.

The following sub-sections address the acceptable use and maintenance of computer technology and the importance of individual accountability in protecting these resources.

4.8.1 Servers

A server is a computer specifically configured to communicate through a network and provide a service to one or more individuals. Server management involves controlling user access, setting/maintaining security measures in place, and monitoring server configuration and performance.

The owner of a server is responsible for the management, operation and security of the server. At a minimum, the owner shall assure the server is physically secured, electronic access to the server is properly controlled, and server configuration is maintained within specified security parameters. The owner of a server may have to place additional requirements beyond the scope of this policy to achieve mandated regulatory compliance and to protect any designated private, confidential, sensitive, or otherwise protected information maintained or archived in the server.

Policy ID	CBP Policy Statements	Relevant Controls
4.8.1.a	All servers will have the standard CBP tools installed for proper monitoring and management of the hardware, operating system, and significant applications and processes. In certain cases, where the standard CBP tools are not sufficient or are implausible to implement (especially in the case of specific applications), a custom tool based on the application architecture may be used in lieu of standard CBP tools.	TBD
4.8.1.b	The following minimum requirements will be followed for Server Monitoring: (1) System state (up/down); (2) CPU utilization; and (3) available drive space.	TBD
4.8.1.c	The following monitoring checks are recommended be followed: • Hardware checks (redundant power failures, RAID disk failures, and other hardware related issues which can be managed through Lights-Out-Management-type interfaces); • Relative/threshold-based CPU utilization, disk availability, and memory (physical and virtual) utilization; • Network connection state (up/down) • Significant application process state (e.g. database, web server, email server up/down); and Functional application checks (e.g. website content check, application login check, and email relay check)	TBD
4.8.1.d	All servers shall be configured to allow adequate communications to support any	TBD

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000205

Policy ID	CBP Policy Statements	Relevant Controls
	CBP approved monitoring and management systems that are not installed and do not use an agent on a server.	
4.8.1.e	Appropriate identification and authorization, audit logging, and integrity controls are required to be implemented on every server in production.	TBD
4.8.1.f	All server audit and security log data shall be made accessible to the CBP Security Operations Center (SOC) via automatic forwarding to SOC log systems for any necessary security analysis and for security log retention.	TBD
4.8.1.g	All servers shall have adequate backups to ensure the recovery of electronic information in the event of a failure. The server backup policy minimum requires all production systems be performed daily incremental/differential and weekly full backups. Multiple generations of backups shall be maintained.	TBD
4.8.1.h	Server Management Policy shall comply with all Federal or DHS/CBP regulations pertaining to long-term retention of various types of information (e.g. financial records retention, etc) as determined by the Business Owner of the information and in accordance with the Record Management Program.	TBD
4.8.1.i	All server equipment shall be removed and replaced by the end of its life expectancy as dictated by the Chief Technology Officer (CTO). Any technology refreshes must adhere to DHS/CBP target architecture and follow the approved processes and meet the necessary standards. Any replacement server must be identified within the CBP Technical Reference Model (TRM).	TBD
4.8.1.j	All new servers shall be built with the latest approved security baseline configurations which are built, tested, and maintained within the Enterprise System Engineering Group.	TBD
4.8.1.k	Server Managers and Administrators shall abide by existing CBP Password Policy; specifically they shall NOT share passwords for special purpose accounts such as "root" and "administrator".	TBD
4.8.1.l	"Root" and "administrator" passwords shall be recorded for emergency access and stored in a locked, monitored location (e.g. safe in the OIT datacenter, etc). Any passwords stored electronically shall abide by existing CBP password policy and be encrypted using FIPS 140-2 compliant encryption and never stored in plain text.	TBD
4.8.1.m	Vulnerability scans of the servers shall be performed at least once a quarter. Any identified vulnerability shall be remedied within 30 days. The vulnerability scan records shall be stored and accessible via the DHS EOCOnline Portal.	TBD
4.8.1.n	Server system shall run an appropriately licensed version of an operating system that supports appropriate Internet communications protocol.	TBD
4.8.1.o	All additional software and services must be licensed as appropriate to the technology and may not violate licensing restrictions.	TBD
4.8.1.p	Servers shall run only necessary services. After it has been determined what services are needed, all unnecessary services shall be disabled and documented.	TBD
4.8.1.q	Server shall have all default account passwords changed and after determining	TBD

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000206

Policy ID	CBP Policy Statements	Relevant Controls
	what default accounts are required, have all other default accounts disabled.	
4.8.1.r	Servers shall have the latest system and application security updates applied regularly, normally within thirty days. All ISVM's that are put forth through the DHS SOC shall be patched and remedied within the specified timeframe. System owners may apply service packs, OS updates, update rollups, hot-fixes, and feature packs as necessary. The responsibility of testing non-security-related updates remains the responsibility of the system owner/administrator.	TBD
4.8.1.s	Servers shall authenticate all users to ensure only authorized users can access the resource. Supplementary authentication mechanisms shall be considered for systems that process or store mission critical or sensitive information.	TBD
4.8.1.t	Electronic communications may, at times, use unencrypted channels; for example, between servers within the same security zone/context. However, in all cases, all authentications must be conducted over an encrypted channel using a FIPS-approved encryption algorithm regardless of security zone/context. This is applicable for both client-to-server and server-to-server communications.	TBD
4.8.1.u	Servers shall enforce password policy including requiring periodic password changes for all users within 180 days (max) and denying login after a specified number of failed login attempts.	TBD
4.8.1.v	Servers shall have all old user accounts terminated promptly (normally within five working days). A clear deadline shall be established for account termination of persons no longer affiliated with the CBP.	TBD
4.8.1.w	Servers shall have virus protection software installed and maintained current with antivirus definitions not more than seven days from the current date. Where possible, anti-virus shall be centrally managed and updated by internal CBP anti-virus management systems, for compliance, reporting and management purposes.	TBD
4.8.1.x	Servers shall capture and archive critical user, network, system and security event logs to enable review of system data for forensic and recovery purposes.	TBD
4.8.1.y	Servers may not function as a relay for SMTP or other means of relaying non-CBP related email, unless otherwise approved by the Chief Information Security Officer (CISO) and documented.	TBD
4.8.1.z	Servers are prohibited from being used as a workstation (i.e. web browsing, checking emails, etc)	TBD
4.8.1.aa	Adequate audit logging must be in place on the system and must log both successes and failures of events such as account logon, security policy changes, account management, system changes. This is applicable to all layers including the operating system, databases and applications.	TBD

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000207

Server Management Responsibilities
Server Owner(s) • Shall work jointly with the team in charge of monitoring and management in order to ensure that the server is monitored and managed as required. Server Manager(s) • Ensures anyone assigned to manage a server is qualified to perform technical duties, has adequate data backup in place, and receives resources necessary, including appropriate training or instruction, to comply with the requirements of this and all other applicable DHS and CBP policies. Server Administrators • Administrators shall control and configure servers in compliance with the requirements of the owner and ensure all applicable DHS and CBP policies are enforced.

4.8.1.1 Special Servers

In addition to above server requirements, the following requirements apply to special servers that process or store mission critical or sensitive information.

Policy ID	CBP Policy Statements	Relevant Controls
4.8.1.1.a	Servers designated as Special Servers are prohibited from being used for inappropriate functions such as testing applications or research and development.	N/A
4.8.1.1.b	Servers designated as Special Servers shall maintain a password history to prevent the reuse of recent passwords, and shall be capable of testing user passwords for easy guessing (dictionary words, common acronyms, etc.).	N/A
4.8.1.1.c	Servers designated as Special Servers shall be physically secured and have an approved firewall or third party firewall software installed or hardware firewall device to safeguard against inappropriate access from/to the Internet and prevent unauthorized access, theft, and destruction.	N/A
4.8.1.1.d	Servers designated as Special Servers shall have a limited number of user accounts with administration privileges. All elevated accounts shall be documented and reviewed every six months to determine if access is still required.	N/A
4.8.1.1.e	Servers designated as Special Servers prohibit use a dial-in/dial-out modem for remote access unless specifically approved by the server Chief Information Security Officer (CISO).	N/A
4.8.1.1.f	Servers designated as Special Servers shall have file backup tools and devices installed and used to periodically archive user and system data.	N/A
4.8.1.1.g	Servers designated as Special Servers shall encrypt remote administration traffic and shall accept remote administration commands only from an authenticated administrator and only approved hosts.	N/A

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000208

4.8.2 Workstations

All users must be instructed to log off or lock their workstation any time the workstation is left unattended. As an added precaution, users should also use a password-protected screensaver. The screensaver should activate after no more than 900 seconds (fifteen minutes) of inactivity as dictated by OMB Federal Desktop Core Compliancy.

The 900 second (15 minute) screensaver timeout policy may adversely impact some CBP job functions. These include those in situation rooms and front lane workstations. Extending the screensaver timeout to 30 minutes, 60 minutes, or no timeout at all will be considered by the ISSO and CISO to alleviate these issues. Mitigating controls must be in place around these workstations to minimize their risk to the CBP enterprise. Requests that include the workstation name must be made through the appropriate Information System Security Officer (ISSO) and CISO to the AO in writing through an screensaver policy exception request.

Policy ID	CBP Policy Statements	Relevant Controls
4.8.2.a	Workstations shall be configured to either log off or activate a password-protected lock, or password protected screensaver, within 900 seconds (fifteen minutes) of user inactivity as dictated by OMB Federal Desktop Core Compliancy.	AC-11, CM-6
4.8.2.b	Workstations shall be protected from theft.	---
4.8.2.c	Users shall either log off or lock their workstations when unattended.	---
4.8.2.d	Screensaver policy exception requests shall be submitted through the ISSO and CISO to the AO for approval for any workstations considered to be adversely impacted by the 900 second (15 minute) screensaver timeout policy. The exception request shall include mission justification, workstation(s) name(s), and mitigating security controls in place to minimize their risk to the CBP enterprise.	---

Workstation responsibilities are provided below.

Workstation Responsibilities
Authorizing Official (AO) • Consider for approval any screensaver timeout policy exception request memorandum based on the recommendation of the CISO. **CISO** • Consider for approval any screensaver timeout policy exception request memorandum based on the recommendation of the ISSO. **Facility Managers** • Ensure physical security measures are adequate to protect computers (PCs, laptops, and

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000209

Workstation Responsibilities
servers) from theft. **Site Security Staff/ISSOs/Supervisors** • Enforce CBP policy to secure workstations when unattended by users. **Information System Security Officer (ISSO)** • Consider screensaver policy exception requests based on the potential adverse impact to certain mission positions. • If determined justified with sufficient mitigating security controls present, submit screensaver policy exception request to the CISO that includes the workstations name. **System/Network Administrators** • Ensure workstations are configured for automatic log-off, or with automatic screensaver activation after 900 seconds (15 minutes) of inactivity where possible. **Users** • Adhere to CBP policy by securing workstations when unattended.

System administrators and ISSOs must ensure that all users are educated in the proper procedures for logging off and for configuring screen savers. Specific procedures for logging off, locking workstations, and enabling password-protected screensavers are found in Attachment X.

The following guidelines apply to the protection of workstations used to process or store sensitive information:

1. Workstations must be adequately protected from theft.

2. Only licensed and approved operating systems and applications can be used on CBP workstations.

3. All default vendor or factory set administrator accounts and passwords shall be changed before installation or use.

4. All equipment shall be marked with the highest level of classification of information that has ever been processed or stored on the device, if there are any devices authorized for processing National Security information in the vicinity.

5. Equipment must be housed in facilities authorized to process sensitive information.

6. Computers must be used in a secure Type II facility (b)(7)(E) (b)(7)(E) and, if necessary, must be physically secured to the work area with a locking device.

7. No unauthorized software may be installed or downloaded onto production workstations or laptops. Users must request installation of approved software from

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000210

the Technology Support Center or the appropriate system administrator. Installation of software applications not currently approved for use in the CBP network environment is strictly prohibited (e.g., games, utilities, and "demo" software).

4.8.3 Laptop Computers and Other Mobile Computing Devices

CBP relies heavily on laptop computers and other mobile computing devices for conducting its business. The mobility of these devices has increased the productivity of the workforce, but at the same time has increased the risk of theft, unauthorized data disclosure, and virus infection. It is thus important to employ additional safeguard measures to protect these resources. This includes the laptops and other mobile computing devices themselves as well as the data processed and stored on these devices.

Many employees use a laptop or notebook computer while traveling both in and out of the United States. Traveling with a laptop computer automatically places employees and contractors in a high-risk situation. Tampering has occurred with laptops taken overseas. To minimize such risks, compliance with the following practices is required:

Policy ID	CBP Policy Statements	Relevant Controls
4.8.3.a	All CBP laptops or other mobile computing devices shall use encryption that is FIPS 197 (AES-256) compliant and has received FIPS 140-2 validation for data residing on it. Passwords and smart cards shall not be stored on or with the laptop or other mobile computing device. This standard software protects CBP information should the laptop fall into the hands of non-CBP individuals.	AC-19, IA-2, SC-12
4.8.3.b	Laptop computers shall be powered down when not in use (due to volatile memory vulnerabilities).	AC-19, PL-4
4.8.3.c	Laptop computers and other mobile computing devices in offices shall be secured when unattended via a locking cable, locked office, or locked cabinet or desk. Never leave a laptop unattended. Keep the laptop under your physical control.	AC-19, PE-3, PL-4
4.8.3.d	Employees shall obtain the written approval from the office director before taking a laptop computer or other mobile computing devices outside the United States.	AC-19, PL-4
4.8.3.e	Do not dispose of any diskettes while traveling. Return them for disposal in government offices.	MP-6
4.8.3.f	If a laptop needs to be repaired while on travel, do not go to a local facility to have it repaired. Contact the LAN administrator, U.S. Embassy or attaché's office for assistance.	AC-19
4.8.3.g	Be aware of your surroundings when using a laptop in public areas, including airports and commercial aircraft.	PL-4
4.8.3.h	Do not transport laptops in luggage that will be handled by airport personnel or allow laptops to be placed in the luggage compartment of the plane. Always	PL-4

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000211

Policy ID	CBP Policy Statements	Relevant Controls
	carry the laptop on the plane with you.	
4.8.3.i	When going through a security checkpoint, ask the security officer to prevent the laptop from passing through the scanner until you are physically on the other side to retrieve it.	PL-4
4.8.3.j	If there are two or more people traveling together, one individual should enter through security first in order to retrieve the laptop(s) or other government property as it comes through the scanning device.	PL-4
4.8.3.k	Transport smartcards and card readers separately from the laptop or mobile computing device. (Smartcards are small enough to store in a pocket or wallet.)	PL-4
4.8.3.l	Ensure that any other card devices such as modem cards, printers, etc., are also secured separately from the laptop. Do not store login names and passwords on the laptop.	PL-4
4.8.3.m	Always use a CBP-approved operating system that has been installed and configured in accordance with appropriate security guidelines. Do not alter issued CBP configurations.	CM-6
4.8.3.n	At least monthly, ensure that each laptop is updated with the latest antivirus software and security patches by connecting to the CBP network or contacting your LAN administrator.	SI-3
4.8.3.o	Immediately report loss or theft of any laptop to your manager, the helpdesk, CSIRC, your SA, or ISSO.	PL-4
4.8.3.p	When you no longer need your laptop, it should be treated like any other CBP storage media equipment through your Local Property Officer. In order to protect sensitive information that is stored on the laptop, you must follow the process for cleansing/sanitizing the media and then re-assigning or releasing the equipment using CBP Form 7610. (See Attachment Y.)	MP-6

Responsibilities related to laptop computers and other mobile computing devices are provided below.

Laptop Computer and Other Mobile Computing Device Responsibilities

DHS CISO

- Establishes DHS policy regarding the use of laptop computers and other mobile computing devices.

CISO

- Enforce CBP policy regarding the use of laptop computers and other mobile computing devices.
- Provide technical expertise and evaluate the effectiveness of encryption methods for laptop computers and other mobile computing devices.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000212

Laptop Computer and Other Mobile Computing Device Responsibilities

System/Network Administrators

- Provide technical expertise and evaluate the effectiveness of encryption methods for laptop computers and other mobile computing devices.
- Ensure that encryption technology is installed and properly configured on laptop computers and other mobile computing devices.
- Assist ISSOs in implementing technical requirements for laptop computers and other mobile computing devices.

ISSOs

- Ensure that security of laptop computers and other mobile computing devices is adequately addressed in the Security Plan.
- Ensure users are aware of their responsibilities to adhere to the rules of behavior for laptop computers and other mobile computing devices.
- Ensure users are trained in the use of encryption for laptop computers and other mobile computing devices.
- Ensure physical security controls are in place for laptop computers and other mobile computing devices.
- Ensure the unique requirements of connection of laptop computers and other mobile computing devices to the network are addressed in the System Security Plan.
- Ensure that encryption methods employed on laptop computers and other mobile computing devices provide the protection required in the Security Plan.

Users

- Obtain written approval of the office director before taking a laptop computer or other mobile computing device overseas.
- Comply with the rules of behavior for laptop computers and other mobile computing devices.
- Utilize encryption technology provided for laptop computers and other mobile computing devices.
- Physically secure laptop computers and other mobile computing devices when not in use.
- Read and adhere to the laptop computer and other mobile computing device policies and procedures in this section and Attachment X.
- Make supervisors and managers aware of any problems encountered in implementing laptop computer and other mobile computing device guidance and procedures.

The increased risk of theft of laptop computers and other mobile computing devices is both a security and a cost issue. There are significant costs associated with replacing the physical hardware as well as the costs of restoring the information residing on the device itself. The risk

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000213

of data disclosure is also a major security concern. Thus, care must be taken to guard against theft at all times. Moreover, fundamental security principles must be followed when using laptop computers and other mobile computing devices. For example, a user's password should never be written down and stored with the device.

Laptop computers and other mobile computing devices cannot be connected to CBP networks or systems unless the network or system is certified and accredited for that functionality. The Security Plan must identify the devices that can be used to access the network or system, the purposes for the access, and the security controls to be employed for the connection. In addition, any laptop computers or other mobile computing devices that process sensitive data (whether or not they are connected to a CBP network) must employ virus protection. All diskettes must be scanned prior to use to ensure they are virus-free.

Rules of behavior for laptop computers and other mobile computing devices must be published and enforced. Attachment G provides guidance on rules of behavior, including rules for laptop computers and other mobile computing devices, and provides sample rules of behavior.

Finally, laptop computers and other mobile computing devices that process sensitive data must employ encryption technology. Encryption policies and procedures are addressed in Section 5.7.1, Encryption.

4.8.4 Government Furnished Portable Electronic Devices

Use of Portable Electronic Devices (PEDs) presents security risks, particularly in an SBU environment. Therefore, careful consideration will be given to any decision to permit them in CBP. Prior to usage of any of these technologies in CBP, such devices may be subject to security analysis and testing, with results and recommendations provided to the CISO before approval for use is granted.

Policy ID	CBP Policy Statements	Relevant Controls
4.8.4.a	USB-based storage devices must employ encryption of stored data. FIPS 140-2 approved encryption is required.	MP-2
4.8.4.b	Approval to use these devices must be granted by the CISO. Denial/approval for use may be based on the particular CBP environment in which the device is proposed for use, as well as the nature of the data to be stored on the device.	MP-2
4.8.4.c	Government-approved and government-furnished PEDs may never be connected to non-CBP devices or used for classified data.	AC-19
4.8.4.d	CBP-owned cellular telephones and PDAs can only be used in conjunction with CBP networks or systems (to include any downloading of data from a computer workstation to these devices) if the current C&A documentation specifically addresses the inherent risks associated with their use. Use of such devices must be specifically authorized by the AO, who evaluates and makes the decision to accept the residual risk of use in the CBP environment.	AC-19
4.8.4.e	Government-owned PEDs may be used for SBU CBP information. Government-owned PEDs may be connected to a CBP computer system that	AC-19

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000214

Policy ID	CBP Policy Statements	Relevant Controls
	processes sensitive information, but not classified information, to perform file sharing, or for the updating of calendars.	
4.8.4.f	All PEDs must have timeout mechanisms activated that automatically prompt the user to enter a password after a period of inactivity.	AC-19
4.8.4.g	PEDs that have audio, video recording, and/or transmission capabilities are prohibited without the approval of the Authorizing Official (AO).	AC-19
4.8.4.h	PEDs that are connected directly to a CBP-wired network (e.g., via a hot synch connection to a workstation) shall not be permitted to operate wirelessly while directly connected.	AC-19
4.8.4.i	Anti-virus software shall be used on wireless-capable PEDs and workstations that are used to synchronize/transmit data. The network infrastructure shall update anti-virus software for all applicable PEDs and their supporting desktops.	AC-19
4.8.4.j	Government-owned PEDs must be treated as any other computer system or technology and be either accredited or included in the Technical Reference Model as part of the technology insertion process in accordance with DHS and CBP security policy. Any CBP computer or computer network that will have a PED connected to it must be approved through the accreditation process.	AC-19
4.8.4.k	Government PEDs will conform to a CBP-approved set of configuration parameters and settings.	AC-19
4.8.4.l	The information stored on individual PEDs will be evaluated during the accreditation process to determine the sensitivity of the information to be stored. If the AO considers the information to be highly sensitive, the information must be encrypted utilizing commercially available FIPS 197 (AES-256) compliance and receive FIPS 140-2 validation.	AC-19
4.8.4.m	Government-owned PEDs will have all files properly sanitized before being reused by another individual or office within CBP or before their disposal. Refer to Attachment Y for media sanitation procedures.	AC-19

4.8.5 Government Furnished Removable Media

CBP approved removable media (e.g. thumb drives, external hard drives, SD cards, etc) are permitted for use within the agency. Users must only use the CBP approved removable media is located in the CBP TRM, unless a waiver has been granted by the CISO. If a waiver has been granted, the waiver is valid for six months only.

Policy ID	CBP Policy Statements	Relevant Controls
4.8.5.a	Approved removable media (e.g. thumb drives external hard drives, SD cards, etc.) shall use encryption that is FIPS 197 (AES-256) compliant and has received FIPS 140-2 validation.	MP-2

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000215

Policy ID	CBP Policy Statements	Relevant Controls
4.8.5.b	All CBP approved removable media (e.g. thumb drives, external hard drives, SD cards, etc) should be stored securely. In addition, all content on thumb drives must be encrypted.	MP-2
4.8.5.c	Computer storage media, i.e., tapes, disks, removable drives, etc containing FOUO information will be marked "For Official Use Only" – per DHS MD 11042.1.	MP-2
4.8.5.d	Any system which movable media is connected to must have the AutoRun and AutoPlay functions disabled for these devices.	CM-6
4.8.5.e	All CBP thumb drives must be centrally tracked and must be assigned to an individual, and not a group of users. For groups requiring the use of thumb drives approval of the CISO is required.	MP-2

4.8.6 Personally Owned Equipment and Software (Not owned by or contracted for by the Government)

Users shall not use personally owned equipment (e.g., laptop computers, PDAs) or software to process, access, or store sensitive information. Such equipment also includes plug-in and wireless (e.g., BlackBerry) peripherals that may employ removable media (e.g., CDs, DVDs). Also included are USB flash (thumb) drives, external drives, and diskettes. Additional policy and guidance pertaining to the protection and disposal of personally owned equipment and software is addressed in Section 4.3, Media Controls. CBP shall ensure that this policy is reflected in appropriate rules of behavior documents and reinforced during periodic security awareness sessions.

Policy ID	DHS Policy Statements	Relevant Controls
4.8.6.a	Personally owned equipment and software shall not be used to process, access, or store sensitive information without the written prior approval of the Authorizing Official (AO). Any approved personally owned USB-based storage devices used shall use encryption that is FIPS 197 (AES-256) compliant and has received FIPS 140-2 validation.	SA-6
4.8.6.b	Equipment that is not owned or leased by the Federal Government, or operated by a contractor on behalf of the Federal Government, shall not be connected to CBP equipment or networks without the written prior approval of the CISO.	SA-9
4.8.6.c	CBP personnel shall not introduce any IT asset into the CBP computing environment and/or IT infrastructure, nor shall they process any CBP data on any IT asset or resource device that has been obtained by DHS, CBP or any other DHS component, or any other governmental or non-governmental entity through the means of civil or criminal asset forfeiture.	AC-20

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000216

Responsibilities related to personally owned equipment and software are provided below.

Personally Owned Equipment and Software Responsibilities
AO • Carefully evaluate the risk associated with authorizing the use of personally owned equipment or software. **CISO** • Enforce CBP policy prohibiting the use of personally owned equipment to connect, process, store, or access sensitive information and systems. **ISSOs** • Enforce CBP policy prohibiting the use of personally owned equipment to connect, process, store, or access sensitive information and systems. • Conduct reviews, at least semiannually, of all equipment and software in their respective offices to ensure that only Government-licensed software and equipment are being used. • Ensure that rules of behavior address policy regarding the use of personally owned equipment and software. • Ensure that security awareness sessions address policy regarding the use of personally owned equipment and software. **Users** • Adhere to CBP policies prohibiting the use of personally owned equipment and software.

No personally owned equipment is to be connected to CBP equipment. Exceptions require written approval from the AO. Exceptions shall be made only when the AO deems that the use or connection of personally owned equipment is essential to the mission. The AO shall accept any risk associated with personally owned equipment and this residual risk must be documented as part of the C&A process.

CBP shall conduct reviews, at least semiannually, of all equipment and software in their respective offices to ensure that only Government-licensed software and equipment are being used, or that appropriate exceptions have been documented.

4.8.7 Personally Owned Portable Electronic Devices

A Portable Electronic Device (PED) refers generically to the broad array of small, mobile computing devices, which include personal digital assistants (PDAs), cell phones, text messaging systems, and any device that records, stores, or transmits data or images electronically. A significant risk of using these devices is the limited availability of encryption technology needed to protect the data processed by mobile computing devices.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000217

Policy ID	CBP Policy Statements	Relevant Controls
4.8.7.a	Personally owned Portable Electronic Devices (PEDs) shall not be used to process, store, or transmit sensitive CBP information.	AC-19
4.8.7.b	Personally owned Portable Electronic Devices (PEDs) shall not be connected to a CBP computer system that processes sensitive information to perform file sharing or for the update of calendars. This specifically includes use of the Universal Serial Bus (USB) port to upload or download data to/from a CBP-owned device	AC-19
4.8.7.c	Use of these devices may be approved on a case-by-case basis by the AO. Any personally owned PEDs used shall have encryption that is FIPS 197 (AES-256) compliant and receive FIPS 140-2 validation. However, approved personal PEDs used with sensitive CBP systems must have all files sanitized as part of the personnel exit procedure when leaving CBP employment. Sensitive files will also be sanitized when an employee changes position to another duty position that does not require the sensitive data stored on the PED. Refer to Attachment Y for media sanitation procedures.	AC-19
4.8.7.d	PEDs that have audio, video recording, and/or transmission capabilities are prohibited without the approval of the AO.	AC-19
4.8.7.e	AO shall approve the use of other add on devices, such as cameras and recorders. Functions that can record or transmit sensitive information via video, infrared (IR), or radio frequency (RF) shall be disabled in areas where sensitive information is discussed.	AC-19

4.8.8 Hardware and Software

CBP must be cognizant of the threats and vulnerabilities associated with hardware and software installation and maintenance on IT systems.

DHS has published secure baseline configuration guides for several operating systems, the Oracle 9i database management system, and CISCO routers (see DHS 4300A, Enclosure 1), and will provide additional configuration guides as required. These hardening guides provide system and database administrators with a clear, concise set of procedures that will ensure a minimum baseline of security in the installation and configuration of the hardware and software. These baselines represent the minimum configuration requirements; CBP is authorized to implement more onerous configuration guides. These baselines were developed using a variety of security guidelines from the National Security Agency (NSA), the Defense Information Systems Agency (DISA), NIST (NIST SP 800-70: "Security Configuration Checklists Program for IT Products – Guidance for Checklists Users and Developers"), and other Federal agencies and from vendor recommendations.

Waivers to the requirements contained in the hardening guides should be requested using the Waivers and Exceptions Request Form (Attachment B).

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000218

Policy ID	CBP Policy Statements	Relevant Controls
4.8.8.a	CBP shall ensure that the installation of hardware and software products meets the requirements specified in applicable DHS secure baseline configuration guides.	CM-2, CM-6
4.8.8.b	CBP shall limit access to system software and hardware to authorized personnel.	AC-3, CM-5
4.8.8.c	CBP shall test, authorize, and approve all new and revised software and hardware prior to implementation in accordance with their Configuration Management Plan.	CM-2, CM-3
4.8.8.d	CBP shall manage systems to reduce vulnerabilities through vulnerability testing, promptly installing patches, and eliminating or disabling unnecessary services, if possible.	CM-3, RA-5
4.8.8.e	Maintenance ports shall be disabled and shall only be enabled during maintenance.	MA-1
4.8.8.f	System libraries shall be managed and maintained to protect privileged programs and to prevent or minimize the introduction of unauthorized code.	SI-7
4.8.8.g	Components shall develop maintenance policy and procedures.	MA-1
4.8.8.h	If cleared maintenance personnel are not available, a trusted DHS employee with sufficient technical knowledge to detect and prevent unauthorized modification to the information system or its network shall monitor and escort the maintenance personnel during maintenance activities. This situation shall only occur in exceptional cases. CBP shall take all possible steps to ensure that trusted maintenance personnel are available.	MA-5
4.8.8.i	Maintenance using a different user's identity may be performed only when the user is present. The *user* must log in and observe the maintenance actions at all times. *Users shall not share their authentication information with maintenance personnel.*	MA-5
4.8.8.j	Employees shall not use personally owned equipment or software to process, access, or store sensitive information without the prior written approval of the AO. This includes laptops, PDAs, portable data storage devices, and software.	AC-20
4.8.8.k	A property pass must accompany all equipment that enters or leaves the National Data Center, regardless of ownership of the equipment. Detailed information can be found in the CBP Physical Security Handbook (HB 1400-02A).	PE-16

Hardware and software responsibilities are provided below.

Hardware and Software Responsibilities

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000219

Hardware and Software Responsibilities

DHS CISO

- Provide guidance in the preparation of secure baseline configuration guides for hardware and software; CISO approves secure baseline configuration guides.

AO

- Ensures new hardware and software products have been approved and documented in the C&A documentation.

ISSOs

- Ensure adequate security measures are in place to protect access to hardware and software.
- Ensure new hardware and software products have been approved in accordance with the configuration management plan prior to installation.

Network/ System Administrators

- Ensure hardware and software is properly secured.
- Ensure maintenance ports are disabled when not in use.
- Ensure unnecessary services are disabled when possible.
- Scan system periodically to identify vulnerabilities and take corrective actions to reduce vulnerabilities.
- Test software security patches on a non-live system prior to implementation on active production systems.
- Ensure new hardware and software products have been approved in accordance with the configuration management plan prior to installation.

Facility Managers

- Ensure adequate physical security measures are in place to protect access to hardware and software.
- Ensure access control policy is enforced.

System Owners/IT Project Managers

- Ensure that the installation of hardware and software products meets the configuration requirements specified in applicable DHS secure baseline configuration guides.

System maintenance requires either physical or logical access to the system. One of the most common methods hackers use to break into systems is through maintenance accounts that still have factory-set or easily guessed passwords. War-dialing techniques will also reveal maintenance ports that are not protected.

Only authorized personnel are to be granted access to system software and hardware in CBP. All authorized personnel must have appropriate security clearances prior to receiving access to system software and hardware. This requirement includes maintenance personnel.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000220

Affected systems are to be backed up before maintenance begins, and changes made to hardware or software during maintenance are to be logged. All new or revised software and hardware must be tested, authorized, and approved in accordance with the configuration management plan. New hardware and software must be documented in the C&A package and approved by the AO. Following IT system upgrades or consolidations, surplus equipment must be secured until it has been prepared for surplus.

As outlined in Section 5.4.9 vulnerability testing must be conducted regularly to identify existing vulnerabilities. Patches are to be installed, after testing in a non-live environment, as they become available. All unnecessary services provided by the operating system must be disabled, if possible. Finally, maintenance ports must be disabled and enabled only during maintenance.

4.8.9 Personal Use of Government Office Equipment and DHS IT Systems/Computers

This section discusses CBP policies applicable to the personal use of Government office equipment and CBP IT systems/computers. Policies governing personal use are derived from several DHS management directives and U.S. Customs Directive 5230-031:

Policy ID	CBP Policy Statements	Relevant Controls
4.8.9.a	CBP employees may use Government office equipment and CBP IT systems/computers for authorized purposes only. "Authorized use" includes limited personal use as described in DHS MD 4600.1, Personal Use of Government Office Equipment, and DHS MD 4900, Individual Use and Operation of DHS Information Systems/Computers and U.S. Customs Directive 5230-031, Limited Personal Use of Government Office Equipment including Information Technology.	---
4.8.9.b	Limited personal use of CBP email and Internet services is authorized for CBP employees as long as this use does not interfere with official duties or cause degradation of network services. Specifically prohibited activities include streaming of audio or video, social networking, peer-to-peer networking, software or music sharing/piracy, online gaming, webmail, Instant Messaging (IM), hacking, and the viewing of pornography or other offensive content. CBP users must comply with the provisions of DHS MD 4500, DHS E-Mail Usage, and DHS MD 4400.1, DHS Web and Information Systems and U.S. Customs Directive 5230-031, Limited Personal Use of Government Office Equipment including Information Technology.	---
4.8.9.c	CBP users do not have any right to or expectation of privacy while using Government office equipment and/or CBP IT systems/computers, including Internet and email services.	AC-8
4.8.9.d	The use of Government office equipment and CBP IT systems/computers constitutes consent to monitoring and auditing of the equipment/systems at all times. Monitoring includes the tracking of internal transactions and external transactions such as Internet access. It also includes auditing of stored data on local and network storage devices as well as removable media.	AC-8

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000221

Policy ID	CBP Policy Statements	Relevant Controls
4.8.9.e	CBP users are required to sign rules of behavior prior to being granted IT accounts or access to CBP IT systems or data. The rules of behavior shall contain a "Consent to Monitor" provision and an acknowledgement that the user has no expectation of privacy.	PL-4
4.8.9.f	Contractors or other non-CBP employees are not authorized to use Government office equipment or IT systems/computers for personal use, unless limited personal use is specifically permitted by the contract or memorandum of agreement. When so authorized, the limited personal use policies of this section and the provisions of DHS MD 4600.1, DHS MD 4900, DHS MD 4400.1, and DHS MD 4500.1 U.S. Customs Directive 5230-031 shall apply.	---

Responsibilities related to personal use of Government office equipment and CBP IT systems/computers are provided below.

Personal Use of Government Office Equipment and CBP IT Systems/Computers Responsibilities

DHS CIO/CISO

- Provide policy and guidance concerning appropriate use of computer resources.
- Establish and implement appropriate enforcement policies for noncompliance with computer resource usage policies.

Assistant Commissioner, Office of Finance

- Establish policy concerning the management and use of Customs office equipment.

Assistant Commissioner, Office of Information and Technology (OIT)

- Establish policy for the management and use of CBP IT equipment. OIT will monitor Internet activity, document usage contrary to this policy and advise the Office of Internal Affairs.

CISO

- Ensure that controls, including awareness training, are in place to minimize or prevent unauthorized use of Government resources.

Office of Internal Affairs

- Investigate alleged violations of this policy as criminal activity or serious misconduct.

Supervisors

- Enforce personal use policies, including remedial training and other sanctions.
- Promptly report unauthorized use of Government resources in accordance with CBP incident reporting procedures (see Attachment F).

ISSOs, Network/System Administrators

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000222

Personal Use of Government Office Equipment and CBP IT Systems/Computers Responsibilities

- As needed, remind users of their system responsibilities and the potential penalties for misuse of system resources; remind users that they do not have any right to or expectation of privacy while using Government office equipment and/or CBP IT systems/computers, including Internet and email services.

Users

- Be aware of the personal use policies described in this section of the handbook and in other references provided by DHS and CBP security officials.
- Adhere to personal use policies established in this section and in other references provided by DHS and CBP security officials.
- Promptly report unauthorized use of Government resources in accordance with CBP incident reporting procedures (see Attachment F).
- Be aware of and understand the disciplinary actions associated with violations of information security policy, including the unauthorized use of Government resources.
- Should NOT have any expectation of privacy in the use of Government computers or computer systems.

Contractors and non-CBP Employee Users

- Understand and abide by the personal use provisions of the contract or memorandum of agreement with CBP.

The use of Government-furnished property, including but not limited to office equipment, supplies, computer equipment, software, telecommunications devices, networks, and IT systems, is for official, authorized purposes only. Some limited personal use is allowed, but only when such use:

1. Involves minimal additional expense to the Government
2. Takes place during the employees non-work time (i.e., time when the employee is not expected to be addressing official business)
3. Does not reduce productivity or interfere with the mission or operations of CBP
4. Does not violate the Standards of Ethical Conduct for Employees of the Executive Branch
5. Does not allow for intermingling of government and personally owned computing systems. Employees are permitted to use a government system in its standard configuration only.

In addition, any limited personal use must be appropriate. Examples of inappropriate use include the following:

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000223

1. Use of Internet sites resulting in an additional charge to the Government.

2. The creation, download, viewing, storage, copying, or transmission of sexually explicit or sexually oriented materials, materials related to illegal gambling, illegal weapons, terrorist activities, or any other illegal or prohibited activities.

3. Use of government office equipment for activities that are illegal, inappropriate, or offensive to fellow employees or the public (e.g., hate speech or material that ridicules others on the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation).

4. Use for other than official Governmental business that results in significant strain on CBP's computer systems (e.g., mass mailings or sending or downloading large files such as programs, pictures, video files, or games).

5. Any otherwise prohibited activity, such as sending out solicitations or engaging in political activity prohibited by the Hatch Act.

6. Modify equipment, including loading personal software or making configuration changes to accommodate personal use.

7. Use of government systems as a staging ground or platform to gain unauthorized access to other systems.

8. The creation, copying, transmission, or retransmission of chain letters or other unauthorized mass mailings regardless of the subject matter.

9. Use of CBP systems for commercial purposes, in support of "for-profit" activities, or in support of other outside employment or business activity (e.g., consulting for pay, sales or administration of business transactions, sale of goods or services).

10. Engage in any outside fund-raising activity, endorsing any product or service, participating in any lobbying activity, or engaging in any partisan political activity prohibited by the Hatch Act.

11. Use of CBP systems for posting agency information to external newsgroups, bulletin boards, or other public forums without authority. This includes any use that could create the perception that the communication was made in one's official capacity as a government employee or representing the government as a vendor.

12. Any use that could generate more than minimal additional expense to the government.

13. The unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information including computer software and data that includes privacy information, copyrighted, trademarked, material with other intellectual property rights (beyond fair use), proprietary data, or export controlled software or data.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000224

14. Open attachments when accessing non-CBP mail systems. Opening attachments in a non-CBP mail system presents a security risk of introducing viruses, Trojans, or other malicious code into the CBP network.

15. Use of official email addresses for other than official CBP business communications and signing up or registering for unapproved mailings or services.

A more complete list of inappropriate uses is contained in DHS MD 4600.1 and U.S. Customs Directive 5230-031.

Inappropriate use is considered a security incident. Depending on its severity, the incident may be deemed a security violation and, as such, be reportable under the CBP SOC/CSIRC provisions of Section 4.9 and Attachment F.

Failure to adhere to CBP personal use policies can also result in sanctions. CBP employees may be subject to disciplinary action for failure to comply with CBP security policy, whether or not the failure results in criminal prosecution. IT security-related violations are addressed on the CBPnet, under CBP Standards of Conduct and Tables of Offenses and Penalties website, URL: http://www.cbp.gov/xp/cgov/careers/neo_kit/additional_info/standards_of_conduct/. Additional violations are listed in the Standards of Ethical Conduct for Employees of the Executive Branch.

Employees should NOT expect privacy when using Government resources. To the extent that employees wish their private activities to remain private, they should avoid using CBP computer systems for such activities. A banner message indicating this policy will be displayed on the login screens of CBP computers. This information will also be included in the Rules of Behavior that users are required to sign on an annual basis.

The use of Government resources constitutes an implied consent to monitoring and auditing of the equipment/systems at all times. Monitoring includes the tracking of internal CBP network transactions and external transactions such as Internet access. It also includes auditing of stored data on local and network storage devices as well as removable media. For example, the CBP is authorized to access email messages or other documents on Government computer systems whenever it has a legitimate Governmental purpose for doing so.

Contractors are not authorized to use Government office equipment or IT systems/computers for personal use under any circumstances, unless limited personal use is specifically permitted by the contract. When so authorized, contractors shall be governed by the limited personal use policies of this section.

4.8.10 Wireless Settings for Peripheral Equipment

Peripheral equipment (printers, scanners, fax machines, etc) often includes capabilities, intended to allow wireless access to these devices. Although convenient, wireless access comes with additional risks. In general, wireless access is not allowed on CBP networks.

Policy ID	CBP Policy Statements	Relevant Controls
4.8.10.a	CBP shall ensure that wireless capabilities for peripheral equipment are disabled. This applies all to peripherals connected to any CBP network or to	CM-7

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000225

Policy ID	CBP Policy Statements	Relevant Controls
	systems processing or hosting CBP sensitive data.	
4.8.10.b	In cases where valid mission requirements or equipment limitations prevent disabling wireless capabilities, CBP shall comply with all requirements outlined in Section 4.6, Wireless Communication and obtain a waiver or exception in accordance with Section 1.10, Exceptions and Waivers.	CM-7

4.9 DHS and CBP Information Security Operations

The DHS SOC is the central coordinating and reporting authority for all Sensitive and National Security computer security incidents throughout the Department. The HSDN SOC will report incidents to the DHS SOC through appropriate channels to protect data classification. The HSDN SOC is subordinate to the DHS SOC, acting as the central coordinating and reporting authority for all SECRET computer security incidents throughout the Department.

Over the last decade both the Government and private industry have become increasingly reliant on computer and networking resources. At the same time, attacks against these automated systems have increased dramatically. As reliance on computer resources has increased, the systems that process the information critical to these organizations have become more vulnerable to attack, viruses, system failure, and user error. These problems have occurred within both high- and low-profile organizations and have occurred regardless of the sensitivity and criticality of the data being processed.

Incidents can be accidental or malicious, can be caused by outside intruders or internal employees, and can cause significant disruptions to mission critical business processes. These incidents can severely disrupt computer-supported operations, compromise the confidentiality of sensitive information, and diminish the integrity of critical data. The effects of security incidents can range from embarrassment, interruption of service, inability to function, and, potentially, to loss of human life. According to a General Accounting Office (GAO) October 2001 report, Information Sharing: Practices that Can Benefit Critical Infrastructure Protection, a significant concern is that terrorists or hostile foreign states could severely damage or disrupt critical operations, resulting in harm to the public welfare.

To help combat the disruptive short- and long-term effects of security incidents, direction from higher authority requires that each Government agency implement and maintain a security incident reporting and handling capability. Examples of this direction include the following:

OMB Circular A-130 specifies that Federal agencies will "Ensure there is a capability to provide help to users when a security incident occurs in the system and to share information concerning common vulnerabilities and threats."

The Federal Information Security Management Act of 2002 (FISMA) directs that a program for detecting, reporting, and responding to security incidents be established in each Department. FISMA also requires the establishment of a central Federal information security incident center. This center is the U.S. Computer Emergency Readiness Team (US-CERT), established in 2003 within DHS.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000226

In addition, OMB M-06-19 (Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments) requires that agencies report all incidents involving personally identifiable information to US-CERT within one hour of discovery of the incident. All incidents involving personally identifiable information in electronic or physical forms are to be reported, and no distinction is to be made between suspected and confirmed breaches. US-CERT will forward all agency reports to the appropriate Identity Theft Task Force point of contact also within one hour of notification by an agency.

Policy ID	CBP Policy Statements	Relevant Controls
4.9.a	It is the policy of CBP that employees and contractors have no privacy expectations associated with the use of any CBP network, system, or application. This policy is further extended to anyone who is granted account access to any network, system, or application in use in CBP. By completing the account log in process the account owner acknowledges their consent to monitoring.	AC-8, PL-4
4.9.b	The SOC shall be operationally subordinate to the DHS SOC.	IR-1
4.9.c	The DHS SOC or CBP SOC shall lead the coordination and administration of department and CBP policy enforcement points, such as firewalls.	SC-7
4.9.d	The DHS SOC shall implement the Department logging strategy, coordinated with the CBP SOC, to enable endpoint visibility and Departmental situational awareness.	---
4.9.e	The CBP SOC shall have the capability to process intelligence information at the collateral level or above. CBP SOC shall have the capability to receive TS/SCI information. The DHS SOC and CBP SOC shall have the ability to process SECRET level information continuously.	IR-4
4.9.f	The SOC shall ensure that personnel are appropriately cleared to access JWICS. The SOC managers are free to determine the number and type of personnel to be cleared, but at least one cleared person should be available per shift. (This person may be on call.) A government officer capability shall be available continuously for incident response and management.	IR-4
4.9.g	The SOC shall establish and maintain a forensic capability as outlined in the Department of Homeland Security (DHS) Security Operations Concept of Operations (CONOPS) (unclassified/classified).	IR-7
4.9.h	Department security operations shall provide a vulnerability management capability. DHS SOC provides Information Security Vulnerability Management (ISVM) messages and vulnerability assessment capabilities. The CBP SOC shall develop their vulnerability management capability to compliment the DHS SOC.	SI-5

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000227

Policy ID	CBP Policy Statements	Relevant Controls
4.9.i	CISO shall ensure that the DHS CISO is kept apprised of all pertinent matters involving the security of information systems and that security-related decisions and information are distributed to the ISSOs and other appropriate persons.	SI-5
4.9.j	CISO shall exercise oversight over all Component security operations functions, including the Component SOCs.	IR-1

Security incident response and reporting responsibilities are provided below.

Security Incident Response and Reporting Responsibilities

DHS CIO

- Determines whether or not security incident information is releasable to the public.

DHS CISO

- Manages the DHS SOC/CSIRC and the incident reporting program.
- Advises the DHS CIO on status of significant incident activity.
- Advises the DHS CIO on the outcome of incident investigations.
- Distributes incident reports to each Component.

DHS SOC/CSIRC

- Serves as the focal point for all DHS incident response activities, to include reporting, incident response, and remediation.

CISO

- Ensures compliance with DHS incident reporting and violation handling policies.

ISSOs

- Ensure that system development and site personnel submit incident reports as specified in this section of the handbook.
- Ensure that system development personnel and system users are trained in the proper procedures for recognizing and reporting security incidents in accordance with the requirements in Attachment F, Incident Response and Reporting.

System/LAN Administrators

- Promptly report computer security incidents n accordance with DHS incident reporting procedures (see Attachment F).

Users

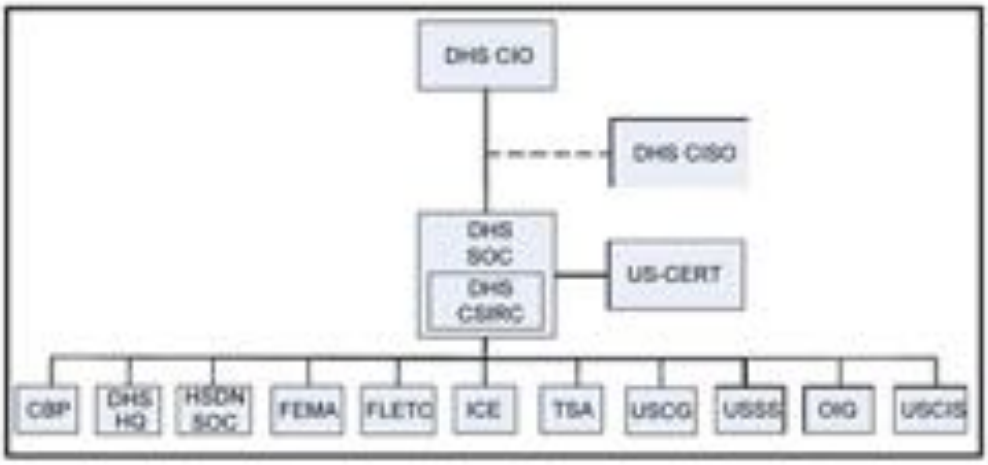
- Promptly report information security incidents in accordance with DHS incident reporting procedures (see Attachment F).

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000228

4.9.1 DHS Security Operations Center Organization

The Security Operations Center (SOC) organization, illustrated in Figure 4.9.1 reflects its operational structure. The DHS SOC reports to the DHS CIO, while the DHS CIO and the DHS CISO provide senior management guidance and direction to the DHS SOC, which in turn provides guidance to Component SOCs, (including CBP).

Figure 4.9.1: DHS Security Operations Center Organization



4.9.2 Logging and Monitoring

The DHS SOC shall maintain visibility into security operations by using logging and monitoring. The DHS SOC logging strategy can be broken into two main components – real-time Security Incident Management (SIM) logging and monitoring, and archive logging designed for offline processing and later retrieval in the event of a security incident.

Effective DHS security event logging capability requires the SOC and component asset integration, requisite event visibility, retention, storage considerations and direction for components to provide logging events into the DHS SOC toolset and relevant security policy reference.

Department logging guidance is documented in the DHS Logging Strategy in the Department of Homeland Security (DHS) Security Operations Concept of Operations (CONOPS).

4.9.3 Authority and Management

Security operations oversight and management is inherently a governmental responsibility, not one that can be outsourced solely to contractors. While the SOC may in-source security operation capabilities from contractors, the responsibility and ultimate authority must lie with a governmental authority. The governmental authority, commonly assigned to a federal SOC manager and one or more Watch Officers, must have the ability to make decisions on behalf of the government to respond to the ever-changing cyber threat landscape. This is not an authority that can be delegated out.

The federal SOC manager and at least one government Watch Officer must be cleared to TS/SCI. Ideally all Watch Officers will be TS/SCI cleared. This is necessary to receive threat intelligence updates at TS and above.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000229

As cyber operations are a continuous activity, governmental authority must be available continuously. This commonly is handled in the creation of three or more watch officers on an 8 hour shift rotation, or governmental authority passed from one SOC to another to cover their watch area during off-hour operations. A DHS Watch Area must never be without governmental oversight within the chain of authority.

4.9.4 Forensics

Computer Forensics is "…the examination of computer systems and the digital information created and stored on such systems to extract and analyze evidence in support of an investigation[3]." Whenever a system compromise occurs, a computer forensic investigation will reveal whether or not the network or system has been used in the commission or become the target of a crime. It will also potentially reveal vectors and methods to protect against future incidents.

The DHS SOC, in cooperation with CBP, will conduct computer forensic examinations as deemed necessary in accordance with the incident response guidelines detailed in Attachment F.

The DHS SOC will coordinate support from CBP with appropriate capabilities for support in handling incidents requiring computer forensics.

Any investigation that reveals potential criminal activity must be turned over to the appropriate authority. Forensic investigations will normally consist of three tiers, as depicted in Table 4.9.4.

Table 4.9.4: Forensic Investigations Tiers

Tier	Action	Resolution
Tier 1	The CBP or DHS SOC initiates the investigation	The CBP or DHS SOC completes the investigation within their own capabilities, expertise, and authority.
Tier 2	CBP or DHS SOC investigators contact the DHS SOC Forensics Response Team for procedural, legal, or forensic capability advice as necessary.	In cases where no criminal activity is found, the SOC investigators will complete their investigation and report results to the DHS SOC. Because the nature and complexity of investigations varies, it is impossible to establish a standard timeline for completion. Investigators must make all attempts to complete investigations as quickly as possible, without sacrificing thoroughness. Status updates shall be provided to the DHS SOC during the weekly conference call.
Tier 3	DHS SOC investigators discover potential criminal	In cases of potential criminal activity, investigators will notify the Forensics

[3] *IT Security Architecture Guidance Volume 2*

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000230

Tier	Action	Resolution
	activity and pass the investigation to the appropriate authority after coordinating with the DHS CIO and DHS CISO.	Response Team and defer investigation management to the team. The appropriate organizational team lead will assume responsibility for the investigation based on the nature suspected criminal activity. CBP and DHS SOC investigators will provide expertise as appropriate.

4.9.5 Vulnerability Management

Vulnerability management is a combination of detection, assessment, and mitigation of weaknesses within a system. Vulnerabilities may be identified from a number of sources, including reviews of previous risk assessments, audit reports, vulnerability lists, security advisories, and system security testing such as automated vulnerability scanning or security tests and evaluations (ST&E).

The DHS SOC/CSIRC takes a proactive approach to vulnerability management including detecting vulnerabilities through testing, reporting through Information Security Vulnerability Management (ISVM) messages, and conducting vulnerability assessments (VA).

A core element of vulnerability management is mitigating the discovered vulnerabilities, based on a risk management strategy. This strategy accounts for vulnerability severity, threats, and assets at risk. Risk calculation will allow CBP to prioritize remediation actions, in accordance with specific situations and risk management strategies. Remediation actions will be captured in CBP's patch management policy.

4.9.5.1 Information Security Vulnerability Management

The DHS SOC/CSIRC will stay abreast of current system vulnerabilities and provide recommendations to CBP through Information Security Vulnerability Management (ISVM) messages. DHS SOC/CSIRC will forward advisories from US-CERT, as appropriate, and ensure that each CBP is alerted. In cases where the alert, advisory or warning is time critical, the DHS SOC/CSIRC may also inform the CIO and POC via telephone. The CBP POCs will be asked to reply to the DHS SOC/CSIRC within a specified time period for instances requiring response to external organizations. Within CBP, the CISO is the POC.

These messages will take three forms:

1. Information Security Vulnerability Alert (ISVA)
2. Information Security Vulnerability Bulletin (ISVB)
3. Technical Advisory (TA)

The characteristics of the vulnerabilities, messages and the required actions are outlined in Table 4.9.5.1.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000231

Table 4.9.5.1: Information Security Vulnerability Management Requirements

	ISVA	ISVB	TAF
Risk	Severe	Medium	Low
Acknowledgement	Yes	Yes	No
Compliance*	Yes	Yes	Yes
Compliance Confirmation	Yes	Yes	No
* Compliance is required if affected systems are present within the Component			

Anyone within DHS may be added to the ISVM distribution list. Those wishing to be added must provide a DHS email address and obtain management approval. ISVMs contain sensitive, "For Official Use Only," information and must not be forwarded to non-DHS email accounts.

Although ISVM messages can be sent to anyone, only the CISO or his/her designated representatives may acknowledge receipt of messages, report compliance with requirements or notify the granting of waivers.

ISVM messages will have the same general format and will contain the following sections, as applicable:

- Message number
- Version
- Related Common Vulnerabilities and Exposures (CVE) numbers
- Release date
- Subject
- Executive summary
- Requirements
    - Acknowledgment (yes/no)
    - Acknowledge by date
    - Compliance (yes/no)
    - Compliance by Date
    - Reporting Instructions
- Affected systems
- Details
- References
- Required actions
- Recommended actions

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000232

- Contact information
- Revision information

See Attachment O for the ISVM Message Template.

Correspondence regarding ISVM notices should be sent via email to dhs.soc@dhs.gov.

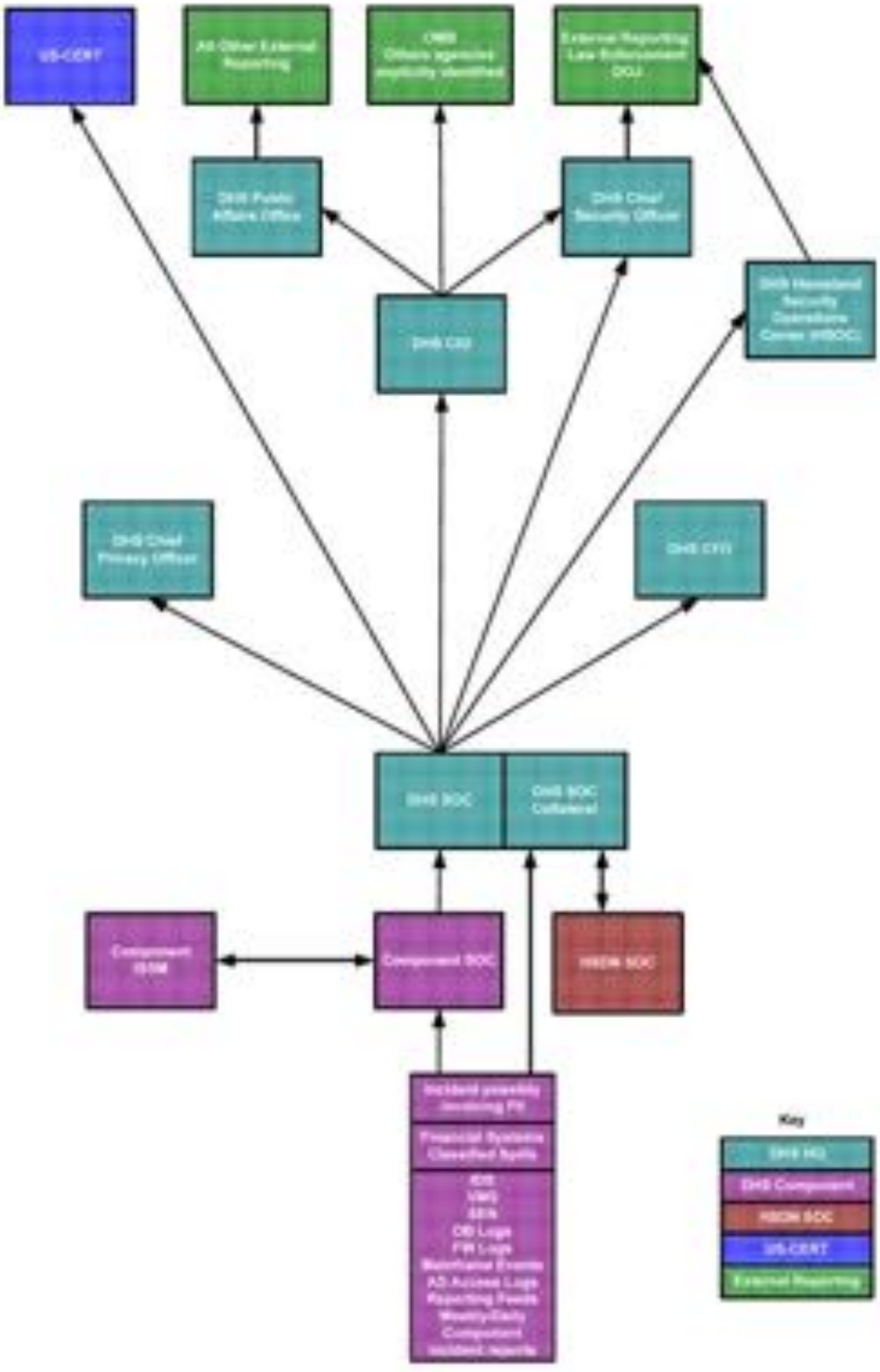
4.9.6 Security Incidents and Incident Response and Reporting

The DHS SOC is the central coordinating and reporting authority for all Sensitive and National Security computer security incidents throughout the Department. The HSDN SOC will report incidents to the DHS SOC through appropriate channels to protect data classification. The HSDN SOC is subordinate to the DHS SOC, acting as the central coordinating and reporting authority for all SECRET computer security incidents throughout the Department.

The DHS Homeland Secure Data Network (HSDN) Security Operations Center (SOC) operates as a separate component, though subordinate to the DHS SOC, in a similar manner to the SOC.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000233

Figure 4.9.6: Incident Reporting Process



epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000234

Policy ID	CBP Policy Statements	Relevant Controls
4.9.6.a	CBP shall establish and maintain a continuous SOC incident response capability.	IR-1
4.9.6.b	CBP shall report significant incidents to the DHS SOC as soon as possible via phone (b)(6),(b)(7)(C) but not later than one hour from "validation" (e.g. a security event being confirmed as a security incident). Other means of communication, such as the SOC ONLINE portal (https://soconline.dhs.gov) (Accessible only via the DHS Intranet), and the HSDN SOC ONLINE portal, are acceptable, but the CBP is responsible for positively verifying that the notification is received and acknowledged by the DHS SOC.	IR-6
4.9.6.c	Significant HSDN incidents shall be documented with a preliminary report that shall be provided to the HSDN Government Watch Officer or DHS SOC within one hour. An initial report detail shall be provided to DHS SOC as soon as possible but not later than one hour from "validation" via secure communications. Subsequent updates and status reports shall be provided to DHS SOC every 24 hours via HSDN SOC ONLINE until incident resolution or when new information is discovered. Significant incidents are reported individually on a per incident basis and shall not be reported in the monthly summary report. Attachment F Section 3.0 for guidance.	IR-6
4.9.6.d	CBP shall report minor incidents on systems in the weekly incident report. SBU systems may report via the DHS SOC portal (https://soconline.dhs.gov) (Accessible only via the DHS Intranet). If there is no portal access, CBP shall report minor incidents via email to dhs.soc@dhs.gov. HSDN incidents or incidents with SECRET information shall be documented in a summary report via the HSDN SOC ONLINE portal.	IR-6
4.9.6.e	All reports shall be classified at the highest classification level of the information contained in the document. Unsanitized reports are to be marked and handled appropriately. Refer to Attachment F for guidance.	IR-1
4.9.6.f	If there are no incidents to report for a given week, a weekly "No Incidents" report shall be sent via the DHS SOC portal (https://soconline.dhs.gov) (Accessible only via the DHS Intranet). If there is no portal access, CBP shall report minor incidents via email sent to dhs.soc@dhs.gov.	IR-6
4.9.6.g	The DHS SOC shall report incidents to US-CERT, in accordance with the Department of Homeland Security (DHS) Security Operations Concept of Operations (CONOPS) (unclassified/classified), as they are reported. CBP shall not send incident reports directly to US-CERT.	IR-6
4.9.6.h	The DHS SOC shall receive classified spillage incident reports, and support the DHS Chief Security Officer (CSO) for containment and cleanup, as documented in Attachment F, Section 6.0. All classified spillages are significant incidents.	IR-6

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000235

Policy ID	CBP Policy Statements	Relevant Controls
4.9.6.i	CBP shall develop and publish internal computer security incident response plans and incident handling procedures, and provide copies to DHS CSIRC. These procedures shall include a detailed CM process for modification of security device configurations.	IR-1
4.9.6.j	Corrective actions shall be taken when security incidents and violations occur and personnel shall be held accountable for intentional transgressions.	IR-1
4.9.6.k	CSIRC shall report incidents only to the DHS SOC and to no other external agency or organization.	IR-6
4.9.6.l	CISO shall ensure Incident Response Testing and Exercises are conducted annually in coordination with the DHS CISO.	IR-3

4.9.6.1 CBP Computer Security Incident Response Center

CBP established a formal Computer Security Incident Response Center (CSIRC) organization. The CSIRC charter requires detection and preliminary investigation of all known or suspected security violations posing a threat to CBP. These threats could be from either internal or external sources. All incidents of misuse of CBP systems must be reported to the CSIRC. NIST SP 800-61 defines a computer security incident as "a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices." This definition can be expanded to "an event that is in violation of explicit or implicit security policies."

Should a computer security incident be suspected or detected, immediately contact the CSIRC and notify your supervisor/manager if it is a significant incident. (See Attachment F for details on incident reporting procedures and definitions of incidents. Table 4.9.6.1 provides contact information to report security incidents.

Table 4.9.6.1: Computer Incident Reporting Contact Information

Contact Group	Phone/Email	Hours
CSIRC	b)(6) (b)(7)(C)	Continuous
CSIRC Email Address	CBP.CSIRC@dhs.gov	
DHS SOC/CSIRC	b)(6) (b)(7)(C)	Continuous

Once the CBP CSIRC has been contacted, the CSIRC staff will ensure that the investigation, analysis, documentation, and resolution of the reported incident are conducted.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000236

Security Incident Response and Reporting Responsibilities
CISO • Ensures compliance with CBP incident reporting and violation handling policies. • Advises the CIO on status of significant incident activity. • Advises the CIO on the outcome of incident investigations. **SOC/CSIRC** • Serves as the focal point for all CBP incident response activities, to include reporting, incident response, and remediation. • Advises the CIO on status of significant incident activity. • Advises the CIO on the outcome of incident investigations. **ISSOs** • Ensure that system development and site personnel submit incident reports as specified in this section of the handbook. • Ensure that system development personnel and system users are trained in the proper procedures for recognizing and reporting security incidents in accordance with the requirements in Attachment V Virus and Malicious Code Procedures. System/LAN Administrators • Promptly report computer security incidents in accordance with CBP incident reporting procedures (Attachment F). **Users** • Promptly report IT security incidents in accordance with CBP incident reporting procedures as documented above.

4.9.7 Law Enforcement Incident Response

The DHS SOC shall notify the DHS Chief, Internal Security and Investigations Division, Office of Security (CISID-OIS) whenever an incident requires law enforcement involvement. Law enforcement shall coordinate with the DHS SOC, the CISID-OIS, CBP, and other appropriate parties whenever a crime is committed or suspected.

Policy ID	CBP Policy Statements	Relevant Controls
4.9.7.a	CBP shall coordinate all external law enforcement involvement through the DHS SOC. Exceptions are only made during emergencies where there is risk to life, limb, or destruction of property. In cases of emergency notification, CBP shall notify the DHS SOC as soon as possible, by the most expedient means available.	IR-6

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000237

Policy ID	CBP Policy Statements	Relevant Controls
4.9.7.b	Security Incidents may include a law enforcement (LE) or counter intelligence (CI) element, such as maintaining a chain of custody. All incidents containing a LE/CI aspect shall be coordinated with the DHS Chief Security Officer (CSO) through the DHS SOC.	IR-6
4.9.7.c	CBP shall obtain guidance from the DHS SOC before contacting local law enforcement except where there is risk to life, health, or destruction of property.	IR-6

Whenever a chain of custody requirement is identified, the DHS Chief, Internal Security and Investigations Division, Office of Security (CISID-OIS), will lead the effort and provide chain of custody guidance. Except in cases where time is critical to protecting lives, CBP should not report directly to law enforcement without first obtaining guidance from the DHS SOC, the CSO, or CISID-OIS. For forensic investigations, the DHS SOC will follow the three-tier process described in 4.9.4.

4.9.8 Definitions and Incident Categories

A security event is a notable, but unassessed, occurrence that may affect a computing or telecommunications system or network. Events may result from intentional or unintentional actions and may include the inappropriate use of CBP computer resources. An event matures into an incident after it has been assessed. The assessment process may be performed by the CSIRC, or the SOC, depending upon its nature and circumstances. Events are investigated individually, but the CSIRC/SOC will review them globally for patterns and tendencies that could identify system vulnerabilities.

An information security incident is an assessed security event. It may even be a simple, inadvertent situation that can be rectified by employee training. Security incidents include the inappropriate use of CBP computer resources. Examples include:

1. Use of Internet sites that result in an additional charge to the Government.
2. Obtaining, viewing, or transmitting sexually explicit material or other material inappropriate to the workplace, this might be considered to contribute to a hostile work environment for some employees.
3. Use for other than official Governmental business that result in significant strain on CBP computer systems (e.g., mass mailings or sending or downloading large files such as programs, pictures, video files, or games).
4. Any otherwise prohibited activity, such as sending out solicitations or engaging in political activity prohibited by the Hatch Act.

Sometimes, the security incident is a clear violation of an explicit or implied security policy in a computing or telecommunications system or network. DHS has identified several categories of

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000238

computer security incident and defined them in Attachment F, Incident Response and Reporting. Examples include:

1. Unauthorized attempts to gain access to information
2. Introduction of malicious code or viruses into an IT system
3. Loss or theft of computer media
4. Categories of incidents include the following:
5. Unauthorized Access (Intrusion). Unauthorized access includes all successful unauthorized accesses and suspicious unsuccessful attempts.
6. Denial of Service. Denial of service attacks include incidents that affect the availability of critical resources such as email servers, Web servers, routers, gateways, or communications infrastructure.
7. Malicious Logic. Malicious logic includes active code such as viruses, Trojan horses, worms, and scripts used by crackers/hackers to gain privileges and/or information, to capture passwords, and to modify audit logs to hide unauthorized activity.
8. Misuse. A user violates Federal laws or regulations, Departmental, and/or CBP policies regarding proper use of computer resources, installs unauthorized or unlicensed software, accesses resources and/or privileges that are greater than those assigned.
9. PII Incident. Incidents involving personally identifiable information in electronic or physical form, including suspected and confirmed breaches.
10. Probes and Reconnaissance Scans. Include probing or scanning networks for critical services or security weaknesses, also include nuisance scans.
11. Classified System Incident. Any incident that involves a system used to process national security information.
12. Alteration/Compromise of Information. Any incident that involves the unauthorized altering of information, or any incident that involves the compromise of information.
13. Multiple Component. Any incident involving events considered significant incidents in more than one of the above categories.

4.10 Documentation (Manuals, Network Diagrams)

Documentation of IT systems involves the collection of detailed information, including functionality, system mission, unique personnel requirements, type of data processed,

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000239

architectural design, system interfaces, system boundaries, hardware and software components, system and network diagrams, cost of assets, system communications and facilities, and any additional system-specific information. This information represents the foundation of the configuration baseline of the system. All proposed changes to the configuration baseline must be analyzed and tested to determine if they have security implications. This includes all proposed configuration changes to operating systems, operating system security features, applications, critical system files, and system devices. Changes must be approved through a formal configuration change control board and documented before they are implemented.

Policy ID	CBP Policy Statements	Relevant Controls
4.10.a	CBP shall ensure that IT systems and networks are appropriately documented in such a way as to allow others to understand system operation and configuration.	CM-8
4.10.b	Documentation shall be updated whenever a system change occurs.	CM-3, CM-8, SA-5
4.10.c	Documentation shall be kept on hand and be accessible to authorized personnel (including DHS auditors) at all times.	CM-3
4.10.d	System documentation may be categorized as Sensitive if deemed appropriate by the CISO. This category shall not be used as a means to restrict access to auditors or other personnel.	CM-3

Documentation responsibilities are provided below.

Documentation Responsibilities
CISO • Ensure that security issues are formally documented and tracked during the SLC process. **IT Project Managers/ISSOs** • Ensure that change control procedures are documented and implemented for all proposed configuration changes to IT systems. • Ensure that all proposed configuration changes to operating systems, operating system security features; applications, critical system files, and system devices are formally approved by the Change Control Board and documented prior to the change being implemented. • Maintain a capability to quickly approve and implement time-sensitive security patches in reaction to late-breaking security vulnerabilities identified by the DHS SOC. • Ensure that all approved changes to the configuration baseline are documented, reviewed for accuracy, and that records are maintained for each IT system for both the current and all

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000240

Documentation Responsibilities
previous configurations. • Ensure that formal system configuration reviews are performed. • Ensure that accurate system documentation and configuration logs are maintained to reflect current and prior configuration baselines.

Change control policies must take into account and have provisions for quickly testing and approving time-sensitive changes that result from newly released vulnerability information. Often in today's climate, severe new vulnerabilities quickly present themselves and the risk of not immediately implementing the vendor-supplied patch exceeds the risk of installing an untested vendor patch. CBP must be able to react quickly as these critical patches are identified and released by the DHS SOC. Documentation of the IT system also encompasses its security features. The software, firmware, algorithms, data structures, processes, and other design mechanisms that satisfy a set of documented security requirements represent the security baseline of the system. Prior to the system being placed in the operational environment, default settings of the security components are to be set to the most restrictive mode for operational systems.

Adequate records of changes to the configuration or security baseline must be reviewed for accuracy and maintained for each system. A historical log of changes for the current and all previous configurations must be maintained. Periodic configuration reviews are to be conducted in conjunction with periodic risk assessments.

4.11 Information and Data Backup

Adhering to requirements regarding data backups can significantly reduce the risk that data will be compromised or lost in the event of a disaster or other interruption of service. A Backup Operations Plan must be included in the Contingency Plan, as discussed in Section 3.5.2, Information Technology Contingency Planning.

Policy ID	CBP Policy Statements	Relevant Controls
4.11.a	The policies in this document, including C&A requirements, apply to any device that process or host CBP data.	---
4.11.b	The CISO shall determine whether or not automated process devices should be included as part of an IT system's C&A requirements.	---
4.11.c	All data will be backed up daily to avoid losing critical data required to support the CBP mission. CBP shall implement and enforce backup procedures a part of their contingency planning. CBP data backup strategies and guidance are detailed in sections 4.11.1 and 4.11.2.	---

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000241

Information and data backup responsibilities are provided below.

Information and Data Backup Responsibilities
CISO • Establish and enforce backup policy. • Provide technical expertise and evaluate the effectiveness of backup approaches. **Certifying Official** • Ensure that a Backup Operations Plan is included in the Contingency Plan. **System Owners** • Ensure that a backup strategy and procedures are established, implemented, and tested in accordance with the contingency plan. **System/Network Administrators** • Ensure that regular (daily, weekly, monthly) backups are performed in accordance with system requirements. • Ensure that analyses are performed to determine the volume of data to be backed up, frequency of data modifications and updates, and access needs of the user community. • Maintain a proper rotation strategy for backups. • Ensure that all backup tapes are properly labeled in accordance with the highest data sensitivity level assigned to the system. • Ensure that on-site and off-site backup storage locations are available. • Ensure that on-site backups are stored in fire and water-proof containers. • Ensure that at least one backup copy of system software is retained off-site. **ISSOs** • Ensure that a Backup Operations Plan is included in the Contingency Plan. • Ensure that the Backup Operations Plan is tested at least annually and more frequently if the risk and magnitude of loss is sufficient to warrant doing so. Ensure that timely corrective actions are taken to address deficiencies discovered during testing. • Ensure that on-site and off-site backup storage locations are available, that on-site backups are stored in fire and water-proof containers and that at least one back-up copy of system software is retained off-site. • Ensure that users are apprised of their responsibilities with regard to backing up any sensitive data residing on their hard drives. • Review the Contingency Plan as part of the accreditation process. • Ensure users and system administrators understand their responsibilities and are aware of negative impacts that can result from failing to adequately back up critical data

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000242

Information and Data Backup Responsibilities
• Ensure the Contingency Plan, including backup procedures, is tested at least annually and that timely corrective action is taken to address deficiencies discovered during testing. • Ensure that all testing is formally documented and ensure that records are maintained as part of the system history. **Users** • Understand the critical nature of backing up sensitive data. • Never keep critical data on individual hard drives unless a backup copy exists, preferably on the network. • Keep supervisors apprised of projects in which critical data may not be adequately backed up.

4.11.1 Backup Strategy

Development of a data backup strategy begins early in the life cycle when the criticality/ sensitivity of the system is first considered. The following factors (derived from the Risk Assessment and documented in the Contingency Plan) will drive the data backup strategy:

- Application restoration priorities based on CBP mission criticality
- The maximum amount of permissible downtime before CBP mission requirements are seriously degraded
- The amount of data updates that can be lost between a service interruption event and the last data backup
- The amount of changes in system configuration settings that can be lost between a service interruption event and the last data backup
- Interdependencies with other systems
- Who the system owners are

Elements that must be considered as part of the backup operations strategy include:

- Specific needs of the site
- People, their roles, responsibilities, and skill levels
- Hardware requirements
- Communications considerations
- Supplies required
- Location and availability of an alternate processing site
- Transportation requirements
- Space requirements of the recovery site
- Power and environmental requirements

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000243

- Backup documentation requirements.

The frequency of backups will depend upon how often the data processed by the system(s) changes and how important those changes are. Again, the risk assessment will drive this element of the backup strategy.

Data backups will be stored on-site temporarily (not to exceed 30 days) in a waterproof, fireproof safe for media until the tapes are sent off-site to a secure facility where they are to be stored in an equivalent waterproof, fireproof safe. For Type II or Type III secure facilities, as defined by the CBP physical security handbook, CIS HB 1400-02A[4] a fireproof and waterproof media safe with a UL class 125 1-hour fire label is required. Local LAN Administrators should determine the size of safe needed by calculating the backup tape storage space required for 30 days on site and the retention period off site.

Data backup and restoration procedures must be tested annually, as a minimum, as an integral part of testing the overall Contingency Plan. This will include testing backup copies to make sure they are actually usable for restoration. More frequent testing may be required commensurate with the risk and magnitude of loss or harm that could result from disruption of information processing support. Testing helps ensure that each person with data backup responsibilities understands and is able to technically fulfill his or her backup and recovery duties. Testing of data backup and restoration procedures needs to be formally documented and records of testing need to be retained as part of the system history.

The same principles that govern backup of system data also apply to individual users. Virtually all CBP employees and contractors will frequently possess critical sensitive data that resides on hard drives on Government-owned personal computers or laptops. Hard drive crashes combined with a failure to save critical files can result in a negative impact to the CBP mission or, at a minimum, result in additional costs and lost time to recover or duplicate lost data. Critical data should never be kept on individual hard drives unless a backup copy exists. The backup should preferably be stored on a network drive where frequent backups are made. CBP system administrators do not have the responsibility or the resources to assist users in recovering lost data resulting from hard drive crashes unless the system owner deems that said data is critical to a CBP mission.

4.11.2 Local Area Network Backup Guidance

System and Local Area Network (LAN) administrators should adhere to the following practices when performing LAN backups:

1. Each CBP office will perform and maintain backups for their respective LANs. A LAN backup includes only file/print servers.

2. All CBP email will be backed up in the common store database and retained indefinitely to meet IA requirements to recover messages for case building.

---

[4] *The standards contained within the 1400-02A shall be applied to all Customs and Border Protection facilities; owned, leased, or occupied space. Compliance is mandatory for all new construction, renovation and relocation projects. Existing CBP facilities are not required to be upgraded unless a risk assessment determines otherwise.*

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000244

3. CBP offices with LAN systems utilizing email will incrementally backup LANs on a daily basis and maintain these backup tapes for three months before recycling.

4. In addition to the required daily backups, CBP offices will perform weekly full backups regardless of which LAN system(s) they utilize.

5. Multiple incremental backups on the same tape are allowed. It is preferred, however, that incremental daily backups be stored off-site, which would prevent multiple incremental backups on the same tape.

6. On a monthly basis, all weekly full and monthly full LAN backup tapes will be moved to an offsite tape storage facility. The weekly tapes will be maintained offsite for 1 month and the monthly tapes will be retained for 1 year. A reciprocal storage arrangement rather than use of a commercial storage site is an acceptable solution (i.e., a Field Office might use the Port Office for their off-site tape storage and the Port Office could use the Field Office). Such a reciprocal arrangement would require an appropriate number of fireproof/waterproof safes for storage of these tapes.

7. When required onsite, LAN administrators (part time, full time, Field Office, or collateral duty), will perform LAN backups, backup tape storage, and file restoration for their respective CBP office.

4.12 Converging Technologies

Advances in technology have resulted in the availability of devices that offer multiple functions. Many devices such as multifunctional desktop computers, copiers, facsimile machines, and heating, ventilation and air conditioning (HVAC) systems may contain sensitive data and may also be connected to data communications networks.

These devices shall be configured to ensure that incoming lines cannot be used to access the data network or any information retained in the memory. CBP shall use only multifunctional devices that have been evaluated and validated through accredited commercial laboratories or by NIST (e.g., the National Security Agency (NSA)/NIST National Information Assurance Partnership (NIAP) Evaluation and Validation Program).

Policy ID	CBP Policy Statements	Relevant Controls
4.12.a	The policies in this document apply to any networked devices that contain information technology, including copiers, facsimile machines, and alarm control systems.	---
4.12.b	CBP shall ensure that network printers and facsimile machines are updated to the latest version of their firmware/software at least annually.	CM-2
4.12.c	CBP shall ensure that network printers, copiers, and facsimile machines shall be configured for least required functionality.	CM-7

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000245

Policy ID	CBP Policy Statements	Relevant Controls
4.12.d	CBP shall ensure that each network printer, copier, and facsimile machine is within the system definition of a DHS information system that has a current ATO.	CM-8
4.12.e	CBP shall ensure that remote maintenance of network printers, copiers, and facsimile machines is conducted only from within DHS networks. If maintenance planning does not include performing remote maintenance, CBP shall ensure that remote maintenance capabilities are disabled.	MA-4
4.12.f	CBP shall ensure that network printers, copiers, and facsimile machines are configured to restrict administrator access to authorized individuals or groups.	MA-5
4.12.g	CBP shall ensure that maintenance/disposal is performed on network printer, copier, or facsimile machine approved for sensitive reproduction only while a properly cleared person escorts the maintenance technician.	MA-5
4.12.h	CBP shall ensure that memory and hard drives do not leave the facility; they are to be replaced and the old part destroyed as sensitive media.	MP-6
4.12.i	CBP shall locate network printers, copiers, and facsimile machines approved to process sensitive information in areas where access can be controlled when paper output is being created.	PE-18
4.12.j	CISO shall determine whether or not automated process devices need to be included as part of an IT system's C&A requirement.	CA-2

Responsibilities related to converging technologies are provided below.

Converging Technologies Responsibilities

ISSOs

- Ensure that nontraditional IT components connected to sensitive systems meet the security requirements detailed in this handbook and are certified and accredited for that purpose.
- Ensure media storage devices included in copiers, facsimile machines, printers, etc., are properly sanitized before leaving CBP control.
- Ensure audit logs are maintained and reviewed for nontraditional IT components that store or process sensitive information.

Network/System Administrators

- Protect and monitor network connections to nontraditional IT devices such as facsimile machines and copiers.

Facility Managers

- Notify and coordinate with the ISSO when facility systems (*e.g.*, HVAC and alarm systems)

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000246

Converging Technologies Responsibilities
require connectivity to sensitive systems. • Ensure proper physical security is afforded to infrastructure equipment that processes, stores, or connects to a sensitive system.

The use of nontraditional IT components without appropriate safeguards presents risks to CBP organizations in part because these devices are typically not thought of as IT systems.

Wireless devices must be secured as specified in Section 4.6, Wireless Communications. Copiers with the capability to process sensitive documents must be secured in the same manner as facsimile machines (see Section 4.5.2). Sanitization of media included in high-end copiers (or other devices) must be carried out in the manner prescribed in Section 4.3.3, Media Sanitization and Disposal. If the device is a multifunction device, the facsimile functions must be secured in the same manner as stand-alone facsimile machines. Printing functions must be secured in accordance with the provisions in Section 4.3.4, Production, Input/Output Controls.

HVAC, fire suppression, and power equipment (including emergency power backup) are to be secured in accordance with the requirements specified for PBXs, as described in Section 4.4.1. If these do not have internal auditing functions, manual audit/access logs are to be maintained by a trusted employee who accompanies any individual who performs maintenance, upgrade or repair on the indicated systems.

The devices discussed in this section that have the capability to process or store sensitive data, whether or not such devices are connected to CBP networks, shall be clearly documented in the Security Plan and certified and accredited for that functionality. The risks of using such devices shall be identified along with countermeasures employed to mitigate these risks. This information shall also be included in applicable rules of behavior and addressed in awareness training orientation and refresher sessions

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000247

5.0 TECHNICAL CONTROLS

The design of IT systems that process, store, or transmit sensitive information shall include the automated security features or technical controls discussed in this section. Security safeguards shall be in place to ensure that each person who has access to sensitive IT systems is individually accountable for their actions while utilizing the system.

Technical controls focus on security controls that a computer system executes. These controls can provide automated protection from unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data. For example, user access is controlled and limited based on positive user identification and authentication mechanisms that support the minimum requirements of access control, least privilege, and system integrity.

5.1 Identification and Authentication

Identification is the process of telling a system the identity of a subject. Usually this is done by entering a name or presenting a token to the system via a smart card. The identity of each user must be established prior to authorizing access to the system, and each system user must have his or her own unique User ID.

Authentication is the process of proving that a subject is who the subject claims to be. Authentication is a measure used to verify the eligibility of a subject and the ability of that subject to access certain information. There are three ways of authenticating oneself:

- Something you know (e.g., password)
- Something you have (e.g., a smart card)
- Something you are (e.g., a biometric such as a fingerprint)

CBP systems must be designed to ensure that each user is authenticated before access is permitted. Concurrent logins to the same system or application using the same authentication credentials are not allowed, unless a specific business or operational need is documented and approved by the Authorizing Official (AO).

Policy ID	CBP Policy Statements	Relevant Controls
5.1.a	Ensure that user access is controlled and limited based on positive user identification and authentication mechanisms that support the minimum requirements of access control, least privilege, and system integrity.	IA-1, IA-2
5.1.b	For IT systems requiring authentication controls, the IT system shall ensure that each user is authenticated before IT system access occurs.	IA-1, IA-2
5.1.c	For systems with low impact for the confidentiality security objective, disable user identifiers after 90 days of inactivity; for systems with moderate and high	IA-4

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000248

Policy ID	CBP Policy Statements	Relevant Controls
	impacts for the confidentiality security objective, disable user identifiers after 45 days of inactivity.	
5.1.d	Users shall not share identification or authentication materials of any kind, nor shall any user allow any other person to operate any CBP system by employing the user's identity.	IA-5
5.1.e	All user authentication materials shall be treated as sensitive material and shall be rated as high as the level of the most sensitive data to which that user is granted access using that authenticator.	IA-7
5.1.f	CBP shall implement strong authentication on servers, for system administrators and significant security personnel, within six (6) months of the CBP's implementation of HSPD-12.	IA-2
5.1.g	User-IDs and passwords must be removed by the system administrator whenever a user is transferred, departs the work area for more than sixty days, has a change in need-to-know, terminates employment, or no longer maintains the required BI.	PS-4 PS-5
5.1.h	User credentials (user-ID plus password) must be unique for each system to which a user is granted access. If the [redacted] ID is required as the user-ID for each system, then the password for each system must be unique.	IA-2
5.1.i	Guest/guest accounts are prohibited from being installed.	AC-2
5.1.j	No accounts will be named anonymous, ftp, telnet, www, host, user, bin, nobody, etc.	AC-2
5.1.k	All User IDs must be revalidated at least annually by the IT system owner or manager.	AC-2

Identification and authentication responsibilities are provided below.

Identification and Authentication Responsibilities
CISO • Establishes and enforces identification and authentication policy. • Provides technical expertise and evaluates the effectiveness of identification and authentication approaches. • Considers and assesses technology opportunities that have the potential to enhance compliance with identification and authentication requirements. • Ensure that systems limit user access based on the identification and authentication of each user prior to certifying the system.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000249

Identification and Authentication Responsibilities
System Owners/IT Project Managers • Ensure adequate resources are budgeted for information assurance; assess identification and authentication technology opportunities for potential application to CBP systems. **System/Network/LAN Administrators/Field Technology Officers** • Ensure that the system identifies every user as unique. • Enforce strong passwords or other more effective means (e.g., PKI-based keys or smartcards). • Secure and administer privileged accounts using authentication technology stronger than passwords. **ISSOs** • Brief users on identification and authentication procedures and protection requirements. • Monitor/enforce compliance with identification and authentication requirements. • Review and approve the initial password distribution plan which must be contained in the system security plan (SSP). • Shall obtain a list of users containing Username and Full-name as part of the system self assessment to determine compliance with the approved initial password distribution mechanism. • Perform system audits to verify compliance. **Users** • Comply with identification and authentication guidance, specifically guidance pertaining to password management (see Section 5.1.1.1). • Report violators of identification and authentication security policies as a security incident to the CSIRC and notify your supervisor/manager if it is a significant incident. (See Attachment F for details on incident reporting procedures and definitions of incidents.)

Privileged accounts are to be secured by authentication technology stronger than that based only on a User ID and password. All actions taken by privileged users with respect to systems and applications should be encrypted to prevent "playback" attacks; they must also be logged for auditing purposes. All passwords, algorithms, keys, certificates, codes, or other schemes that are used by the system for authentication purposes must be stored in a manner that prevents unauthorized individuals from gaining access to them. A system can be compromised without proper, secure storage.

5.1.1 Passwords

The least expensive method for authenticating users is a password system in which authentication is performed each time a password is used. More sophisticated authentication techniques, such as smart cards and biological recognition systems (e.g., retina scanner, handprint, voice recognition), shall be cost-justified through the risk assessment process.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt2 000250

A password is a sequence of characters used for authentication purposes. Passwords are often used to authenticate the identity of a system user and, in some instances, to grant or deny access to private or shared data. Passwords are important because they are often the first line of defense against hackers or insiders who may be trying to obtain unauthorized access to a computer system. Passwords provide a reasonable degree of authentication that the entity is the authorized user of the User ID, username, or logon ID. They are one of the most common methods used for controlling system access. To be used effectively, strong password policies must be implemented, and users and system administrators must follow the CBP password guidelines (specific guidelines are provided in Attachment L).

Policy ID	CBP Policy Statements	Relevant Controls
5.1.1.a	In those systems where user identity is authenticated by password, the system ISSO shall determine and enforce appropriate measures to ensure that strong passwords are used.	IA-5
5.1.1.b	The ISSO shall determine and enforce the appropriate frequency for changing passwords but in no case shall the frequency be less often than every 90 days.	IA-5
5.1.1.c	Users shall not share personal passwords. They shall not provide their passwords to anyone, including system/network/LAN administrators or FTOs.	IA-5
5.1.1.d	Group accounts are not permitted. For operational necessity or criticality for mission accomplishment, group password usage may be considered[5]. Use of a group User ID and password must be approved by the CISO and the AO via formal policy exception request and documented within the System Security Plan (SSP).	IA-4
5.1.1.e	Passwords are prohibited from being embedded in scripts or source code.	IA-5
5.1.1.f	Passwords may not be stored in clear text. Passwords stored on CBP systems will be encrypted.	IA-5
5.1.1.g	Passwords may not be reused for at least 8 iterations.	IA-5
5.1.1.h	Login account passwords may not be used that is the same string as the User ID or that contains the User ID.	IA-5
5.1.1.i	Users may not have more than one User-ID and password for a single system and must not log into the system more than once, generating concurrent sessions.	AC-10

5 The use of a personal password by more than one individual is prohibited throughout CBP. However, it is recognized that, in certain circumstances such as the operation of crisis management or operations centers, watch team and other duty personnel may require the use of group User IDs and passwords.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000251

Policy ID	CBP Policy Statements	Relevant Controls
5.1.1.j	When possible, initial distribution of passwords should be accomplished in person by the administrator or the help desk personnel. When this is not possible and the initial password must be provided either over the telephone or via email, the following policy should be considered: • Vendor default passwords should never be used as initial passwords. • Initial password should be programmed to expire after a 72 hour period. • As possible, initial password should be designed as one-time only password that automatically triggers the user to update by creating their new password. • As with all passwords, the initial password must be encrypted whether in transit or storage. The exception is one-time passwords that may be distribute in clear text as long as there is no associated user ID contained in the same message. • When initial password is distributed by email, only the user should be addressed with no one else carbon copied. • The initial system password should be randomly generated to conform to policy. If the initial password must be provided over the telephone, the system administrator or help desk analyst must seek to authenticate the user identity by requiring either the verification of the user's identify by the user's supervisor or manager OR by having the user successfully answer two questions based on their profile.	IA-5
5.1.1.k	Passwords may never be set equal to the null string which is equivalent to no password at all.	IA-5

5.1.1.1 Selecting Strong Passwords

Users must select well-constructed passwords. When selecting a password, use the following CBP password guidelines to ensure that the password chosen is in compliance with CBP requirements. For guidance on how to change passwords for a variety of CBP systems, (see Attachment L).

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000252

Required Action	Benefit Gained
Passwords shall— • Be at least (b)(7)(E) in length. • Contain a combination of alphabetic, numeric, and special characters. • Not be the same as the previous 8 passwords	These requirements make it more difficult for a password guesser to obtain passwords. They increase the set of combinations that must be guessed and provide a mixture to defeat a dictionary attack.
Passwords shall not contain any dictionary word.	Prevents dictionary type of attacks.
Passwords shall not contain any proper noun or the name of any person, pet, child, or fictional character. Passwords shall not contain any employee serial number, Social Security number, birth date, phone number, or any information that could be readily guessed about the creator of the password.	Helps prevent a password guess based on a hacker's personal knowledge of the user.
Passwords shall not contain any simple pattern of letters or numbers, such as "qwerty" or "xyz123".	Protects against dictionary attacks
Passwords shall not be any word, noun, or name spelled backwards or appended with a single digit or with a two-digit "year" string, such as 98xyz123.	Protects against dictionary attacks
Pass phrases, if used in addition to or instead of passwords, should follow the same guidelines.	Consistent application of guidelines.
Passwords shall not be the same as the User ID.	Risk of unauthorized access is reduced, as hackers initially try "obvious" passwords such as username and User ID.

5.1.1.2 Results of Weak Passwords

Weak passwords can allow internal users and external hackers, who achieve access to the internal network, to gain greater access to CBP systems. Because hackers and other unauthorized users know that passwords are the key to gaining access to systems, there have been a variety of methods and tools that have been created to crack passwords, including guessing.

Hackers have access to a variety of password-cracking tools. While tools provide a means for hackers to obtain passwords, often password information is given directly to hackers. For example, a hacker may be able to disguise himself as an authorized user and call the user's system administrator or help desk and ask that a password be reset. If the system administrator

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000253

and/or help desk staff has not implemented stringent user identification controls, it would be very easy for a hacker to gain access to an authorized user account with the new password. As a result, the authorized user will be locked out of his or her own system because the hacker had the password changed.

Brute force attacks involve manual or automated attempts to guess valid passwords. Simple password-guessing programs can be easily created and there are numerous password-guessing programs available on the Internet. Most hackers have a "password hit list," which is a collection of default passwords automatically assigned to various system accounts whenever they are installed. For example, the default password for the guest account in most UNIX systems is "guest."

Many hackers will try to guess passwords using personal information of a user, such as the birth date, name of spouse/children, pets, employee ID number, etc. Often, hackers will practice what they call "social engineering," which involves talking with employees to find out things about the systems in their office, and, more importantly, personal information that will help them guess passwords.

Users tend to choose passwords that are easy to remember such as the name of a family member or pet, a birth date, or a word that may mean something to the user. Unfortunately, these types of passwords are the easiest for others to guess.

People are the key to constructing good passwords. Poorly constructed passwords make it much easier and faster for someone to find out a password. The longer it takes hackers to get a password, the more likely they are to move onto other methods of gaining access to the system.

It should be noted that many computer systems use auditing features that keep a record of actions initiated by the users while on the system. Thus, once a hacker cracks a password and gains access to the system using the appropriate User ID, the system audit logs will record that the User ID was used in taking harmful actions on the system. Authentication is the basis for control and accountability of the users on the system.

5.2 Access Control

Network and system administrators ensure that access controls operate as intended. The authority delegated to these roles to add, change, or remove component devices, dial-up connections, network addresses and protocols, or to remove or alter programs should be tightly controlled. This authority should be divided among more than one administrator, supervisor or root password holder.

Users are responsible for protecting all CBP information to which they are granted access. Access controls restrict access to system objects such as files, directories, and devices based upon the identity of the user, or the group to which the user belongs. Subverting access controls violates this policy (more in Attachment X). Access controls protect against the unauthorized disclosure, modification, or destruction of the data residing in these systems, as well as the applications themselves. They offer alternative means to restrict activities of the general user population.

Automated systems are vulnerable to fraudulent or malicious activity by individuals who have the authority or capability to access information not required to perform their job-related duties. Access control policy is designed to reduce the risk of an individual acting alone from engaging

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000254

in such fraudulent or malicious behavior. The Principle of Least Privilege states that users should only be able to access the system resources needed to fulfill the user's job responsibilities.

Principle of Least Privilege: Requires that each user in a system be granted the most restrictive set of privileges (or lowest clearance) needed for performance of authorized tasks.
The application of this principle *limits the damage that can result from an accident, error, or unauthorized use.*

Policy ID	CBP Policy Statements	Relevant Controls
5.2.a	CBP shall implement access control measures that provide protection from unauthorized alteration, loss, unavailability, or disclosure of information.	AC-1
5.2.b	Access control shall follow the principles of least privilege and separation of duties and shall require users to use unique identifiers. *Social Security Numbers shall not be used as login IDs.*	AC-2, IA-1
5.2.c	Users shall not provide their passwords to anyone, including system/network/LAN administrators and/or Field Technology Officers.	IA-5
5.2.d	Emergency and temporary access authorization shall be strictly controlled and must be approved by the CBP Chief Information Security Officer (CISO) or his/her designee prior to being granted.	AC-2
5.2.e	System Owners shall ensure that users are assigned unique account identifiers.	AC-2, IA-4
5.2.f	The Lock Workstation button should be used to lock the computer when leaving the workstation unattended, except for overnight. (See Attachment X)	AC-11
5.2.g	Screen savers integral to the operating system may be used to restrict access to workstations and servers. Users must engage the password protection feature of their screen savers when leaving workstations or servers unattended.	AC-11
5.2.h	Servers using screen savers are advised not to use open 3GL-type screen savers that use an undue amount of processing resources.	AC-11
5.2.i	CBP systems with a FIPS 199 confidentiality categorization of high shall limit the number of concurrent sessions for any user to one (1).	AC-10

Access control responsibilities are provided below.

Access Control Responsibilities
CISO
• Establish and enforce access control policy.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000255

Access Control Responsibilities
• Provide technical expertise and evaluate the effectiveness of access control approaches. • Certify that adequate access controls are in place. • Directly approve, or delegate authority to a strictly controlled group, emergency and temporary access prior to being granted. **System/Network/LAN Administrators/Field Technology Officers** • Ensure that access controls are in place and functioning as intended. • Ensure that access controls provide the security features outlined in this document. • Ensure that systems prevent users from having multiple concurrent active sessions for one identification unless the AO has granted authority based upon operational business needs. **ISSOs** • Ensure that access controls are in place and functioning as intended. • Ensure that access controls provide the security features outlined in this document.

System/network/LAN administrators/Field Technology Officers and ISSOs are responsible for ensuring that access controls are in place and operating as intended. It is especially critical that the authority to add, change, or remove component devices, dial-up connections, and network addresses and protocols, or to remove or alter programs be tightly controlled with access limited to only a select group of authorized personnel.

- **Initial User Access**

  Users who require access to CBP systems and networks must have completed a Background Investigation (BI) prior to being granted access. However, users with a Limited BI may be given access to email, the Internet, and Development and Systems Acceptance Testing (SAT) environments.

  The user's supervisor or government project manager must determine the system user's need to access a system and the levels of access required. User access will vary depending upon the position held. This authorization becomes critical to maintaining correct security measures. The system owner or designated representative must approve user access privileges.

- **Review of Access Privileges**

  User data access requirements will change over time. Therefore, supervisors or ISSOs should review access control lists to verify that they reflect who has access to what data and ensure that access control list are up-to-date. This applies to vendors who support systems and other non-CBP personnel with access to any systems. These actions are reviewed as part of the C&A process and during annual self-assessments.

  Access control policies and procedures need to be written down and stored in an off-site location. They need to be accessible in the event of an emergency. This information also needs to be included in the Contingency Plan.

- **Terminated and Departing Employees**

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000256

System/Network/LAN administrators and ISSOs must ensure that all departing employees have their access privileges terminated immediately. No former employee should have any ability to access system resources after their term of employment has ended. Procedures vary depending on whether the separation is voluntary or involuntary. Termination of access privileges also applies to employees whose job functions have changed such that they no longer require access to the level of sensitive information to which they were previously granted. See Section 4.1.4, Separation of Duties, for detailed guidance on this subject.

- **Secure Remote Access**

  Hardware security tokens, such as cryptographic smartcards, can be issued to CBP employees and contractors who have a valid need to remotely access CBP systems and data.

5.2.1 Automatic Account Lockout

CBP shall configure each IT system to lock a user's account for a specified period following a specified number of consecutive failed logon attempts. Users shall be locked from their account for a minimum period of 20 minutes after three consecutive failed logon attempts during a 24 hour time period. CBP shall configure systems to require the system administrator to unlock a user's account after three consecutive failed logon attempts for systems rated as High or designated as financial systems. All failed logon attempts must be recorded in an audit log and periodically reviewed.

Policy ID	CBP Policy Statements	Relevant Controls
5.2.1.a	CBP shall implement and enforce an account lockout policy that limits the number of consecutive failed logon attempts to three during a 24 hour time period. Systems should lock out a user account after three consecutive failed logon attempts. All failed logon attempts must be recorded in an audit log and periodically reviewed. (See Attachment X)	AC-7
5.2.1.b	CBP shall configure systems to lock a user's account for a minimum of 20 minutes after three consecutive failed logon attempts.	AC-7
5.2.1.c	CBP shall configure systems to require the system administrator to unlock a user's account after three consecutive failed logon attempts for systems rated as High or designated as financial systems.	AC-7

Automatic account lockout responsibilities are provided below.

Automatic Account Lockout Responsibilities
CISO • Establishes and enforces automatic account lockout policies. **System/Network/LAN Administrators/Field Technology Officers** • Ensure that systems are configured to lock a user's account for 20 minutes after 3 unsuccessful logon attempts during a 24 hour time period. • Unlock a user's account after three consecutive failed logon attempts once the user is

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000257

Automatic Account Lockout Responsibilities
properly identified and authenticated for systems rated as High or designated as financial systems.
ISSOs
• Ensure that systems are configured to lock a user's account for 20 minutes after 3 unsuccessful logon attempts.

5.2.2 Automatic Session Termination

A session refers to a connection between a terminal device (workstation, laptop, PED, etc) and a networked application or system. (This does not include a direct connection to a CBP network, such as authenticating from a device that is directly connected to a CBP network.) A session also refers to accessing an application or system through the CBP network, such as a database or networked application.

Each CBP IT system shall be configured to deactivate any user session immediately and automatically following 20 minutes of inactivity, in such a way that will require the user to re-authenticate his identity before resuming interaction with the system. The session is not terminated, but the user will need to log on again in order to activate the session. Sessions shall automatically be terminated after 60 minutes of inactivity.

For IT systems that require more than the 20 minute minimum to run queries or complete other functions, the system owner and ISSO may submit an exception to policy request justifying the extended period necessary and including other security controls in place to safeguard access control.

System owners and/or ISSO may establish a more stringent automatic session lockout policy than the minimum CBP 20 minute limit.

Policy ID	CBP Policy Statements	Relevant Controls
5.2.2.a	Network applications or systems shall be configured to automatically deactivate or lock any user session following 20 minutes of inactivity. (See Attachment X for details.)	AC-11
5.2.2.b	Locked sessions shall remain locked until the user re-authenticates.	AC-11
5.2.2.c	Sessions shall automatically be terminated after 60 minutes of inactivity.	AC-12

Automatic session lockout responsibilities are provided below.

Automatic Session Lockout Responsibilities
CISO
• Establishes and enforces automatic session lockout policies.
• Approve any request for policy exception to extend automatic session lockout to any period beyond 20 minutes for specific IT systems with mission justification.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000258

Automatic Session Lockout Responsibilities
System/Network/LAN Administrators/Field Technology Officers • Ensure that systems are configured to deactivate or lock any user session that has remained idle for 20 minutes. • Ensure that systems are configured to terminate any user session that has remained idle for 60 minutes. **ISSOs** • Ensure that systems are configured to deactivate or lock any user session that has remained idle for 20 minutes. • Ensure that systems are configured to terminate any user session that has remained idle for 60 minutes. • Submit request for policy exception to extend automatic session lockout to any period beyond 20 minutes for specific IT systems with mission justification.

5.2.3 Warning Banner

The DHS CISO mandates that a warning banner statement be displayed on all DHS IT systems during logon. The most current language can be found on the DHS CISO's web page on DHS Online located at https://dhsonline.dhs.gov/portal/jhtml/dc/sf.jhtml?doid=117934. The approved DHS warning banner language is also included in the CBP Policy box below.

The use of the warning banner serves as a reminder to all users that the computers they are accessing are Government computers and must be used in accordance with good security practices.

Policy ID	DHS Policy Statements	Relevant Controls
5.2.3.a	IT systems accessible to the public shall provide both a security and privacy statement at every entry point.	AC-8
5.2.3.b	IT systems internal to the DHS and CBP network shall display the approved department warning banner. This notification must inform potential users that: • *You are accessing a U.S. Government information system, which includes (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only.* • *Unauthorized or improper use or access of this system may result in disciplinary action, as well as civil and criminal penalties.* • *By using this information system, you understand and consent to the following:* o *You have no reasonable expectation of privacy when you use this*	AC-8

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000259

Policy ID	DHS Policy Statements	Relevant Controls
	information system; this includes any communications or data transiting or stored on this information system. At any time, and for any lawful government purpose, the government may, without notice, monitor, intercept, search, and seize any communication or data transiting or stored on this information system. ○ *The government may disclose or use any communications or data transiting or stored on this information system for any lawful government purpose, including but not limited to law enforcement purposes.* ○ *You are NOT authorized to process classified information on this information system.*	
5.2.3.c	CBP IT externally facing websites accessible by the public shall display a warning banner during logon and before granting users system access. This notification must inform potential users that: *You are about to access a Department of Homeland Security computer system. This computer system and data therein are property of the U.S. Government and provided for official U.S. Government information and use. There is no expectation of privacy when you use this computer system. The use of a password or any other security measure does not establish an expectation of privacy. By using this system, you consent to the terms set forth in this notice. You may not process classified national security information on this computer system. Access to this system is restricted to authorized users only. Unauthorized access, use, or modification of this system or of data contained herein, or in transit to/from this system, may constitute a violation of section 1030 of title 18 of the U.S. Code and other criminal laws. Anyone who accesses a Federal computer system without authorization or exceeds access authority, or obtains, alters, damages, destroys, or discloses information, or prevents authorized use of information on the computer system, may be subject to penalties, fines or imprisonment. This computer system and any related equipment is subject to monitoring for administrative oversight, law enforcement, criminal investigative purposes, inquiries into alleged wrongdoing or misuse, and to ensure proper performance of applicable security features and procedures. DHS may conduct monitoring activities without further notice.*	AC-8
5.2.3.d	The current language for Secret and Top Secret Computer Log-On Banners can be found on the DHS-CISO's web page on DHS Online located at https://dhsonline.dhs.gov/portal/jhtml/community.jhtml?index=10&community=MGMT&id=2002980003.	AC-8
5.2.3.e	CBP approves the IT system use notification message before its use in production	AC-8
5.2.3.f	The system use notification message remains on the screen until the user takes explicit actions to log on to the information system.	AC-8

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000260

Warning banner responsibilities are provided below.

Warning Banner Responsibilities
DHS CISO • Establishes and enforces the use of appropriate standard Warning Banner for all internal DHS and CBP IT systems. • Establishes and enforces the use of a standard Warning Banner and Privacy Statement for display at all publicly accessible entry points to DHS and CBP IT systems. **CISO** • Establishes policy compliant with DHS policy for use of appropriate standard Department Warning Banner applicable to all CBP IT systems **System/Network/LAN Administrators/Field Technology Officers** • Ensure that internal IT systems under their controls are configured to display the approved Department Warning Banner. • Ensure publicly accessible IT systems under their control are configured to display the approved Department Warning Banner and Privacy Statement. **ISSOs** • Ensure that internal IT systems under their controls are configured to display the approved Department Warning Banner. • Ensure publicly accessible IT systems under their control are configured to display the approved Department Warning Banner and Privacy Statement.

5.3 Auditing

A fundamental computer security principle is that each person is to be individually accountable for his or her actions while using the system. By providing the ability to track a user's activities while accessing an automated system, auditing tools are an effective method of enforcing this principle. Audit trails maintain a record of system activity by both system and application processes as well as by individual user activity.

CBP personnel shall use system audit features to review CBP system and network events and security activities recorded in log files for unauthorized or inappropriate activities. The type of security events contained or captured within the audit log must be reviewed annually with additional security events being considered as necessary.

Audit trails maintain a record of system activity by both system and application processes as well as by individual user activity. In conjunction with appropriate tools and procedures, auditing can further several security-related objectives including:

- Individual accountability
- Reconstruction of events

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000261

- Intrusion detection
- Problem identification

Audit trails can track the identity of each subject attempting to access the system, the time and date of access, and the time of log off. In addition, audit trails can capture all activities performed during a session and can specifically identify those activities that have the potential to modify, bypass, or negate the system's security safeguards. The auditing technique used must be able to support after-the-fact investigations of how, when, and why normal operations ceased.

Audit trail records must be maintained online for at least 90 days, thereby allowing rapid access to recent information. Audit trails should be preserved for a period of seven years as part of managing records for each system to allow audit information to be placed online for analysis with reasonable ease. Preservation of the audit information should be part of the IT Contingency and business continuity plans, so that events preceding a disaster or interruption of service can be reconstructed.

The need to review the information captured by the auditing process is of paramount importance. To be effective, audit trails must be periodically reviewed and analyzed. In many cases, it is only through the review process that incidents of unauthorized access, modification, or destruction are uncovered. Audit trails also need to be secured to prevent tampering and backed up regularly. Procedures that support CBP audit policy are detailed in Attachment T.

Policy ID	CBP Policy Statements	Relevant Controls
5.3.a	Audit records shall be sufficient in detail to facilitate the reconstruction of events if compromise or malfunction occurs or is suspected. Audit records shall be reviewed as specified in the IT System Security Plan (SSP). The audit record shall contain at least the following information: • Identity of each user and device accessing or attempting to access an IT system • Time and date of the access and the logoff • Activities that might modify, bypass, or negate IT security safeguards • Security-relevant actions associated with processing • All activities performed using an administrator's identity	AU-3
5.3.b	Audit records for financial systems or for systems hosting or processing PII shall be reviewed by the system administrator monthly. Unusual activity or unexplained access attempts shall be reported to the system owner, CISO, and the SOC.	AU-6
5.3.c	CBP shall ensure that their audit records and audit logs are protected from unauthorized modification, access, or destruction.	AU-9
5.3.d	CBP shall ensure that audit logs are recorded and retained in accordance with the CBP or DHS's Record Schedule. At a minimum audit trail records shall be maintained online for at least 90 days or for a time period necessary for the	AU-11

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000262

Policy ID	CBP Policy Statements	Relevant Controls
	review of events when system compromise occur, whichever is longer.	
5.3.e	The system risks associated with extracts of PII from databases shall be evaluated. If the risk is determined to be sufficiently high, a procedure shall be developed for logging computer-readable data extracts. If logging these extracts is not possible, this determination shall be documented, and compensating controls identified in the SSP.	AU-1, AU-2, AU-3
5.3.f	The Component Security Operations Center (SOC) shall implement both general and threat-specific logging.	AU-1
5.3.g	SSPs for individual applications must specifically address audit requirements and retention periods for system log files. Audit requirements for individual systems may specify more detailed information than the minimum listed above	PL-2
5.3.h	Computer-readable extracts (CREs) involving PII shall be erased within 90 days unless the information included in the extracts is required beyond the 90 days. Permanent erasure of the extracts or the need for continued use of the data shall be documented by the System Owner and audited periodically by the CBP Privacy Officer.	PL-5
5.3.i	CBP systems must provide mechanisms to associate an individual with a single, unique identity, which also associates a user with security-relevant events.	AU-3
5.3.j	System administrators should be assigned one account for root system tasks and a second account for routine access.	AC-6
5.3.k	Audit trail requirements cannot be waived except in extreme circumstances, and then only by the Assistant Commissioner of Office of Information and Technology (OIT). Where this requirement is waived, other security controls such as user authentication, file passwords, magnetic media control procedures, and a logging mechanism to record terminal usage must be verified implemented.	AU-2

Auditing responsibilities are provided below.

Auditing Responsibilities
Assistant Commissioner, Office of Information Technology
• Authority to waive Audit Trail requirements, only in extreme circumstances.
CISO
• Ensure that all CBP IT systems maintain an audit record sufficient to reconstruct security relevant events.
• Evaluate auditing requirements; budget for and select appropriate auditing tools.
• Establish policy for retention of audit logs.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000263

Auditing Responsibilities
• Ensure auditing is performed independently of system/network administration. **System Owners** • Ensure adequate resources are budgeted for implementing and maintaining an effective auditing capability. • Work with IT managers to identify critical functions to be subjected to auditing and keep apprised of auditing findings. • Ensure auditing is performed independently of system/network administration. **System/Network/LAN Administrators/Field Technology Officers** • Maintain an audit record sufficient to reconstruct security relevant events. • Ensure that the audit record includes: o The identity of each person and device accessing or attempting to access the system. o The time and date of the access and when the user logged off. o Activities performed using an administrator's identification. o Activities that could modify, bypass, or negate the system's security. o Sufficient detail to facilitate reconstruction if compromise or malfunction occurs. o Security-relevant actions associated with processing. • Protect audit records against unauthorized access, modification, or destruction. • Retain audit records for a minimum of 90 days or in accordance with the Security Plan and ensure that audit records are regularly backed up. **ISSOs** • Ensure that the Security Plan addresses accountability and auditing. • Ensure that the risk analysis documents the rationale and justification for any CBP IT system that does not implement an auditing capability. • Ensure that audit records include all required elements. • Review audit records at least once per week or in accordance with the Security Plan. • Ensure that audit collection and review procedures contain adequate separation of duties provisions. • Report security-relevant events to the CSIRC.

5.4 Network and Communications Security

This section addresses vulnerabilities inherent in network security and the technical controls needed to mitigate the risks associated with these vulnerabilities. Network security encompasses remote access, network monitoring, external connections, boundary protection, Internet usage, email security, and vulnerability scanning. This section focuses on CBP policies governing

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000264

security of network access, devices, and usage. (Refer to Attachment U for procedures and details.)

5.4.1 Remote Access and Dial-In

Remote access technology allows trusted employees to access CBP networks by dialing in via modem or accessing via the Internet. This allows mobile employees to stay in touch with the home office while traveling away from their normal work locations. However, there are significant security risks associated with remote access and dial-in capabilities. Proper procedures can help mitigate these risks.

Note: Remote access solutions that do not comply with the requirements of FIPS 140-2 are not authorized.

Virtual Private Networks

Secure Virtual Private Network (VPN) communications access capabilities must provide strong identification and authentication, audit logging, and integrity controls; and they must be implemented using a CBP-approved session level encryption mechanism designed to protect the identification and authentication process as well as data transmission. Remote access request forms are found in Attachment W.

VPNs are alternative methods for access to CBP networks and are permitted under specific circumstances, which primarily consist of an assurance that the FIPS 140-2 standard is followed and encryption will exist to protect data transmission across unsecured networks into the CBP network. CBP-owned desktops and laptops using VPNs require CBP-approved personal firewalls to be installed. (See Section 5.7.1 on Encryption and Section 5.4.4 for details on Firewalls.)

VPNs are primarily designed to assure secure transmission between a client desktop or laptop and a server inside CBP. Where possible, the elements of this arrangement must be owned and operated by CBP, not by a vendor company unless specifically contracted for that purpose and with prior approval of the CISO. Under such circumstances where VPNs are used to connect to external networks, an Interconnection Security Agreement (ISA) is required (See 5.4.3 and Attachment N). All VPNs require a technical review by an ISSO, Certification Agent (CA), and approval by the CISO.

Other Remote Access Methods

Other methods to secure communication within and to CBP networks are authorized. The use of Public Key Infrastructure (PKI)-enabled smartcards, proprietary tokens (e.g., PassKey or SecurID token), or similar methods is authorized for use. These remote access methods must also comply with both CBP and DHS policies regarding standards-based encryption methodologies and management. If the chosen solution is PKI-based, the appropriate federal standards (e.g., FIPS or NIST) must be used in its certification.

Alternative forms of remote access methods are not authorized. Remote access methods that include either hardware or software solutions not approved by CBP, and which have not been documented and certified by the appropriate federal authority, are also not authorized for use within or to the CBP trusted network.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000265

Policy ID	CBP Policy Statements	Relevant Controls
5.4.1.a	Data communication connections via modems shall be limited and shall be tightly controlled as such connections can be used to circumvent security controls intended to protect CBP networks. Data communication connections are not allowed unless they have been authorized by the CISO.	AC-4, AC-17, AU-2 SC-7, SC-8, SC-9
5.4.1.b	Components shall ensure that remote access and approved dial-in capabilities provide strong authentication and access control and audit and protect sensitive information throughout transmission. In addition, remote access solutions shall comply with the encryption requirements of FIPS 140-2, *Security Requirements for Cryptographic Modules*. Dial-up connections shall be centrally managed to ensure integrity of network security. Strong authentication for remote access shall use two-factor authentication.	AC-4, AC-17, AU-2 SC-7, SC-8, SC-9
5.4.1.c	Remote access of PII shall comply with all CBP requirements for sensitive systems, including strong authentication. Strong authentication shall be accomplished via virtual private network (VPN) or equivalent encryption and two-factor authentication. CBP has an immediate goal that remote access should only be allowed with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access. Any two-factor authentication shall be based on CBP-controlled certificates or hardware tokens issued directly to each authorized user.	AC-4, AC-17, AU-2 SC-7, SC-8, SC-9
5.4.1.d	Remote access of PII shall not permit the download and remote storage of information unless the requirements for the use of removable media with sensitive information have been addressed. All downloads shall follow the concept of least privilege and shall be documented with the SSP.	—
5.4.1.e	CBP systems shall not be connected to any non-CBP systems via modem.	AC-17, AC-20
5.4.1.f	The Public Switched Telephone Network (PSTN) shall not be connected to OneNet at any time.	—
5.4.1.g	The Risk Assessment and SSP shall document any remote access of PII, and the remote access shall be approved by the CISO, CBP Privacy Officer, and AO prior to implementation.	RA-3 PL-2

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000266

The following security policies apply to the approved use of modems in CBP-owned computers operating within or interfacing with non-CBP-owned systems and environments:

Policy ID	CBP Modem Policy Statements	Relevant Controls
5.4.1.h	For all dial-up connections, use a CBP-approved session-level encryption mechanism such as a smartcard, designed to protect both the identification and authentication process as well as data transmission. Unencrypted legacy dial-up systems, if in existence, must be replaced.	AC-17
5.4.1.i	Workstations that have a physical connection to any network, mainframe, server, or other CBP device must not be used to dial-up to non-CBP systems, unless such a dial-up is performed through a secured modem-pool authorized in writing by the CISO.	AC-17
5.4.1.j	If a requirement exists to use an on-board modem for dial-up capability, only a standalone workstation that does not contain sensitive information and that will never be physically connected to any other CBP system or network may be used.	AC-17
5.4.1.k	When located at an external site, standalone systems with their own dial-out capability to a CBP system require an Interconnection Security Agreement (ISA) authorizing an interconnection. An ISA template is available from the DHS Risk Management System (RMS). Contact your system's ISSO for details and assistance in obtaining the template.	AC-17

Remote access and dial-in responsibilities are provided below.

Remote Access and Dial-In Responsibilities
CISO
• Establish and enforce remote access control policy for CBP.
• Provide technical expertise and evaluate the effectiveness of remote access control approaches.
System/Network/LAN Administrators/Field Technology Officers
• Ensure that remote access controls are in place and functioning as intended.
• Ensure that remote access controls provide strong identification and authentication.
ISSOs
• Ensure that remote access controls are in place and functioning as intended.
• Ensure that remote access controls provide the security features outlined in this document.
Users
• When remotely accessing DHS systems, ensure that the equipment used to gain access is protected from viruses and other malicious code and that the protection software is kept current.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000267

Unauthorized access is the biggest risk associated with remote access facilities. If untrusted or uncleared persons obtain unauthorized access, they can violate the integrity, confidentiality, and availability standards of CBP. An unsecured modem or other dial-in facility could provide a backdoor for unauthorized users (inside or outside of CBP) to the entire CBP network. Malicious individuals can exploit improperly configured remote control software.

There are commercially available products that can be used in conjunction with other network protection mechanisms to reduce the risks of unauthorized access. These require the use of authentication methods stronger than passwords and user IDs. Only approved hardware and software products already contained within the Technical Review Model (TRM) can be purchased and operated without the need for additional approval of the CBP Architecture review function.

5.4.2 Network Security Monitoring

Security monitoring, detection and analysis are key functions and are critical to maintaining the security of CBP information systems. Monitoring and analysis is limited to observing network activity for anomalies, malicious activities and threat profiles. Content analysis is not within the scope of network monitoring.

CSIRC leads the effort in monitoring network security. CISO, ISSOs, and system/network/LAN administrators/field technology officers respond to and participate in intrusion alerts and SOC/CSIRC-led incident response investigations. They also evaluate the impact of each event on the system and implement any necessary corrections.

Policy ID	CBP Policy Statements	Relevant Controls
5.4.2.a	The CBP SOC shall provide continuous monitoring of their networks for security events or outsource this requirement to the DHS EOC. Monitoring includes interception and disclosure as required for the rendition of service or to protect the Department's or Component's rights or property. Service observing or random monitoring shall not be used except for mechanical or service quality control checks. (As per the Electronic Communications Privacy Act) In this instance, "rights" refers to ownership or entitlements or property or information as in intellectual property.	SI-4
5.4.2.b	CBP SOC shall administer and monitor Component IDS sensors and security devices.	SI-4
5.4.2.c	The CBP SOC shall report any event that is a security incident to the DHS SOC.	SI-4

Network security monitoring responsibilities are provided below.

Network Security Monitoring Responsibilities
CISO
• Establish policy and implement and manage a viable intrusion detection program within each Component.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000268

Network Security Monitoring Responsibilities
• Provide guidance, as needed, when responding to intrusion alerts from the DHS and/or CBP SOC. **SOC** • Monitor CBP systems and networks using various network security technologies. • Initiate computer security incident procedures when incidents are discovered. **ISSOs/System Administrators** • Respond to intrusion alerts when notified by DHS and/or CBP SOC. • Participate in SOC-led incident response investigations. • Evaluate the impact of the event on the system. • Implement necessary corrective actions.

5.4.2.1 What Is Intrusion Detection?

Intrusion detection is the art of detecting inappropriate, incorrect, or malicious activity. Systems that operate on a host to detect malicious activity on that host are called host-based intrusion detection systems (HIDS). Those that operate on a network are referred to as network intrusion detection systems (NIDS). Intrusion detection is viewed as an integral part of a layered security model/defense-in-depth strategy.

Intrusion detection operates on the principle that any attempt to penetrate a system can be detected in real time as opposed to actually stopping the penetration, as is the case with firewalls. This principle is based on the assumption that it is virtually impossible to close every potential security breach. NIDS are designed to identify break-in attempts and stop them, in some cases working in conjunction with firewalls to alter the access control lists to halt an incursion. HIDS can offer the equivalent of a software firewall installed on the host, stopping or preventing would-be intruders.

Intrusion prevention systems (IPSs) are closely related to IDSs. Some IDS technologies currently provide intrusion protection by halting malicious data transmissions and disconnecting communication from the host from which they originate. Others take the additional step of reconfiguring firewalls to permanently block attacking hosts from sending data into the network.

Firewalls are designed to prevent unauthorized entry, but firewalls can fail or be compromised by an intruder. Intrusion detection systems supplement firewalls by alerting the organization that an attack may have occurred or be occurring. Firewalls are also incapable of protecting a network from internal compromise, but IDSs can alert network and system managers of such an attack.

5.4.2.2 Methods and Techniques

The most common approaches to intrusion detection are statistical anomaly detection and pattern matching (signature) detection. Statistical anomaly involves tracking system use and establishing a baseline of what is “normal” and setting an acceptable range of parameters to which the system normally adheres. When the system goes beyond the statistical ranges, an

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000269

intrusion may have occurred and an alarm is given. Pattern matching is simply what its name implies. Patterns of known attacks are part of the IDS database. Attack patterns for denial of service attacks, buffer overflow attacks, and backdoors are well known. These are known as signatures. When these signatures are detected, an alarm is given. When alarms are given, those monitoring the IDS investigate to determine if an intrusion has in fact occurred and react accordingly. Event correlation systems can compare information from various security devices and reduce the likelihood of unnecessary response to "false positives," which may arise from an attack signature matching allowed activities. Such systems can also reduce the likelihood that the monitoring staff is distracted from noticing an actual attack by a flurry of alarms raised by relatively innocuous activities.

5.4.2.3 Network Monitoring

The Computer Security Incident Response Center (CSIRC) shall accomplish the monitoring of CBP systems and networks. Upon receipt of an alarm, operators shall investigate to determine the validity of the alarm. Once confirmed, the operator shall notify the ISSO and/or the system administrator for corrective action. If the problem is deemed critical, senior management shall be notified and involved to determine the appropriate course of action.

5.4.3 Network Connectivity

A system interconnection is the direct connection of two or more information systems for the purpose of sharing data and other information resources. This applies to systems that pass data between each other via a direct system-to-system interface without human intervention. Any physical connection that allows other systems to share data (pass thru) also constitutes an interconnection, even if the two systems connected do not share data between them. It does not include instances of a user logging on to add or retrieve data, nor users accessing web-enabled applications through a browser.

A number of management, operational, and technical controls impact network connectivity. These include identification and authentication controls, audit logging, integrity controls, and periodic reviews of programs/systems to ascertain whether or not changes that could adversely affect security have occurred.

Policy ID	CBP Policy Statements	Relevant Controls
5.4.3.a	Components shall ensure that appropriate identification and authentication controls, audit logging, and access controls are implemented on every network component.	AC-1, AC-2 AU-1, AU-2, IA-1, IA-2
5.4.3.b	Interconnections between CBP and non-CBP IT systems shall be established only through controlled interfaces and via approved service providers. The controlled interfaces shall be accredited at the highest security level of information on the network. Connections with other Federal agencies shall be documented based on interagency agreements, memoranda of understanding, service level agreements or interconnection security agreements. The	CA-3,

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000270

Policy ID	CBP Policy Statements	Relevant Controls
	document vehicle chosen must still contain such information as the interface characteristics, security requirements, nature of information communicated and monitoring procedures for verifying enforcement of security requirements.	
5.4.3.e	CBP shall document its interconnection to the DHS OneNetwork (OneNet) with an Interconnection Security Agreement (ISA), signed by the OneNet AO and by the CBP AO.	CA-3
5.4.3.d	ISAs shall be reissued every three years or whenever any significant changes have been made to any of the interconnected systems.	CA-3
5.4.3.e	ISAs shall be reviewed and updated as needed as a part of the annual FISMA self-assessment.	CA-3
5.4.3.f	CBP may complete a master ISA, (which includes all transitioning systems) as part of their initial OneNet transition. After transition, each additional system or GSS shall be required to have a separate ISA. Interconnections between CBP and other DHS Components (not including DHS OneNet) shall require an ISA whenever there is a difference in the security categorizations for confidentiality, integrity, and availability between the systems or when the systems do not share the same security policies. In this context, 'security policies' refers to the set of rules that controls a system's working environment and not to DHS information security policy. ISAs shall be signed by each organization's respective AO.	---
5.4.3.g	Connections with other Federal agencies shall be documented based on interagency agreements, memoranda of understanding, service level agreements or the interconnection security agreements. A single ISA may be used for multiple connections provided that the security accreditation is the same for all connections covered by that ISA.	CA-3
5.4.3.h	CBP shall document interconnections between the CBP network and external (Non-DHS) networks with an ISA for each connection.	CA-3
5.4.3.i	CBP shall implement a Trust Zone with DHS through Policy Enforcement Points, as defined in the DHS Security Architecture and documented in Section 5.4.3.2.	SC-7
5.4.3.j	DHS OneNet shall provide secure Name/Address resolution service. DNSSec has been designated as the DHS service solution.	SC-20, SC-21, SC-22
5.4.3.k	All DHS systems connected to OneNet and operating at moderate or high level shall utilize secure Name/Address resolution service provided by DHS OneNet.	SC-20, SC-21, SC-22
5.4.3.l	The appropriate CCB shall ensure that documentation associated with an approved change to an information system is updated to reflect the appropriate	CM-3

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000271

Policy ID	CBP Policy Statements	Relevant Controls
	baseline. CBP systems that interface with OneNet shall also be subject to the OneNet CCB.	
5.4.3.m	Interconnections between two accredited DHS systems do not require an ISA if the interface characteristics, security requirements, nature of information communicated and monitoring procedures for verifying enforcement of security requirements are accounted for in the SSPs or are described in another formal document, such as an SLA or contract, and the risks have been assessed and accepted by all involved AOs.	CA-3
5.4.3.n	Granting the ability to log into one DHS system through another DHS system (such as through OneNet trust) does not require an ISA, when the requirements from Section 5.4.3.m are met.	—

Network connectivity responsibilities are provided below.

Network Connectivity Responsibilities

AO or Designated Official

- Review, approve, and sign the Interconnection Security Agreement (ISA).
- Ensure that ISAs are reissued every three years or whenever significant changes are made to any of the interconnected systems.

CISO

- Provide guidance and enforce management, operational, and technical controls that apply to network and system security configuration and monitoring.
- Evaluate the risks associated with external connections.
- Review programs/systems periodically to ascertain if changes have occurred that could adversely affect security.

System Owners

- Establish the requirement for the external connection and assess the associated risks.
- Ensure that all connections to the system are identified and addressed by an active ISA document.

Network Administrators

- Ensure technical controls governing use of the external connection remain in place and function properly.
- Assist in development of the ISA as necessary.
- Ensure that any new connection and/or system access was justified and validated by the system owner and the system ISSO.
- Ensure that there is a valid ISA in place prior to any connection going being activated.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000272

Network Connectivity Responsibilities
Certifying Agents • Review Mission ISAs developed by the ISSOs before the ISA is sent for signature approve. **ISSOs** • Coordinate with the external agency in development of the ISA. • Ensure that a validated list of connections and supporting ISAs is included in the System Security Plan and is also available as necessary by CISO in support of Secure Internet Gateway (SIG) requests. • Assist in preparation of both Trade and Mission ISAs and ensure all external connections are documented in the System Security Plan, Risk Assessment, and security operating procedures. • Review ISAs as a part of the annual FISMA self-assessment. • Monitor compliance. **Users** • When connecting to CBP networks, ensure the equipment used to access these networks is protected from viruses and other malicious code and the protection software is kept current.

5.4.3.1 Interconnection Security Agreements

Proper management of network connections is vital to ensuring the confidentiality, integrity, and availability of the data processed by a system. Interconnections of systems must be established in accordance with NIST SP 800-47 (*Security Guide for Interconnecting Information Technology Systems*). An ISA is required whenever the security policies of the interconnected systems are not identical or the systems are not administered by the same entity. The ISA documents the security protections on the interconnected systems to ensure only acceptable transactions are permitted. ISAs must be reissued every three years or whenever significant changes have been made to any of the interconnected systems. CBP ISSOs must review their ISAs as part of the annual FISMA self-assessment.

All external connections must be identified and documented in the System Security Plan, the risk assessment, and other C&A documentation as necessary. The risk associated with these connections must be addressed during the C&A process.

An ISA should address the following areas:

1. Purpose: This section should explain the rationale for the interconnection and contain a one- or two-paragraph statement that justifies the need to interconnect the two systems.

2. Interconnection Statement of Requirements: This section documents the formal requirement for connecting the two systems. The following items should be addressed in this section:

    a. The requirement for the interconnection, including the benefits derived

    b. The names of the systems being interconnected

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000273

c. The type of connection (Frame Relay, T1, etc.)

d. Physical location of connection equipment, including addresses and room numbers

e. Primary Points of Contact (POC) for both systems

f. The agency name(s) or organization that initiated the requirement.

3. System Security Considerations: This section documents the security features in place to protect the confidentiality, integrity, and availability of the data and the systems being interconnected. This includes such areas as incident reporting and personnel clearances. Technical representatives from each organization need to discuss the contents of this section and come to a mutual agreement as to which items are to be included.

4. Topological Drawing: Each ISA must include a topological drawing depicting the end-to-end interconnectivity in a clear and readable manner. The drawing should include:

   a. All data communications paths (not program system paths), circuits, etc., used for the interconnection beginning with the DHS-owned system(s) traversing through all interconnected systems to the non-DHS end-point

   b. The logical location of all components (mainframe computers, host processors, hubs, firewalls, encryption devices, routers, frame relay devices, secure frame units [SFU], communications service units [CSU], data service units [DSU], and customer personal computers).

5. Signatures and Comments: Each ISA must be signed by the CBP AO of each connecting system and/or organization or by the official designated by the AO to have signatory authority for ISAs. This section acknowledges that the ISA is subject to change, will be reviewed annually, and will be modified as circumstances warrant. This section must include a statement that the ISA may not be unilaterally modified and that any changes must be reviewed and jointly agreed upon.

Details on completing an ISA are contained in Attachment N, *Preparation of Interconnection Security Agreements*.

5.4.3.2 Trust Zones

Information and services sharing between the DHS SOC and CBP occurs through Trust Zones. A Trust Zone consists of a group of people, data systems, and networks subject to a shared security policy or set of rules governing access to data and services. (For example, a Trust Zone may be set up between different network segments that require specific usage policies based on information processed, such as law enforcement information.) The DHS SOC must be aware of CBP-security requirements, as defined by Trust Zones, to accurately perform DHS SOC duties.

DHS Trust Zones have the following characteristics:

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000274

1. A set of networked hosts protected from unconstrained access by one or more security perimeter devices
2. Provide the basis for placement and configuration of firewalls, Virtual Private Networks (VPN), and remote access protection devices
3. May consist of a single host, one or more LANs at a site, or a group of networks connected via a network provider or backbone
4. OneNet provides a layer of trust through subnetting, firewalls, and other policy enforcement mechanisms
5. Network Admission Control permits dynamic assignment of information systems and users to basic Trust Zones. Medium and High assurance models are another mechanism that permits assignment to Trust Zones

Application based Trust Zones permit organization managed Trust Zones.

5.4.3.3 Domain Membership

This policy is required to improve the manageability and security of Windows desktops and devices connected to the network. Adherence to this policy shall ensure that CBP is in a position to detect and remediate vulnerable windows systems. Workstations are the largest attack surface within DHS and require many controls to ensure they are properly managed. This has become even more critical in the wake of recent attacks, as unmanaged systems are easy to exploit via well-known avenues. These exploits have subsequently caused significant disruption to the CBP mission.

Policy ID	CBP Policy Statements	Relevant Controls
5.4.3.3.a	All computers and mobile devices running a Microsoft Windows operating system connecting to CBP's Networks shall be required to join one of the five managed Windows Domains, which are listed as follows: (b) (7)(E) (b) (7)(E)	TBD
5.4.3.3.b	Only "approved" CBP Windows (Workstations/Servers) versions shall be permitted. Please note that the requirement to join one of the CBP managed domains does not grant approval for unauthorized operating systems, software or configuration therein.	TBD

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000275

Policy ID	CBP Policy Statements	Relevant Controls
5.4.3.3.c	All computers and mobile devices that are members of the Active Directory Windows Domain shall have the "Domain Admins" group as a member of the local Administrators group. When Windows computers join the domain, this group is automatically added and it must not be removed.	TBD
5.4.3.3.d	In cases where computers and mobile devices do not require access to central resources such as file or print servers, e-mail or Internet access, then an exemption to domain membership needs to be sought through the assigned Information System Security Officer (ISSO) and/or the Security and Technology Policy Branch. Such an exemption would be conditional upon the department involved accepting responsibility for maintaining adequate patching and virus protection levels. Exemptions may also be conditional upon the limitation of network access to the non-domain computer equipment.	TBD
5.4.3.3.e	Non-CBP equipment that cannot join the Active Directory Windows domain shall be subject to a separate Waiver covering the responsibilities of the department or owner. This level of access is required in order to verify service pack and patch levels, virus definitions, software versions and (where necessary) to purge or remove virus infections.	TBD

5.4.4 Firewalls and Policy Enforcement Points

Within the CBP, boundary protection of IT resources is accomplished by the installation and operation of firewall systems. Firewalls, when used in concert with a variety of additional security controls such as intrusion detection systems, personnel background checks, security guards, data encryption, and physical security barriers, provide an added level of assurance that unauthorized personnel will be unable to access CBP's automated systems.

Policy Enforcement Points (PEPs) separate Trust Zones as defined by the DHS Security Architecture. Boundary protection between DHS and external networks is implemented by firewalls at Trusted Internet Connections (TICs) and other approved direct system inter-connections. DHS TICs are provided by OneNet and monitored by the DHS SOC. CBP SOC may protect CBP boundaries across the DHS Trust Zones.

By tracking and controlling data, and deciding whether or not to pass, drop, reject, or encrypt the data, firewalls have proven to be an effective means of securing a network.

Policy ID	CBP Policy Statements	Relevant Controls
5.4.4.a	CBP shall restrict physical access to firewalls and Policy Enforcement Points (PEP) to authorized personnel and ensure that all firewalls are located only in a physically secure area.	AC-4, SC-7

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000276

Policy ID	CBP Policy Statements	Relevant Controls
5.4.4.b	Components shall implement identification and strong authentication for administration of the firewalls and PEPs.	AC-4, SC-7
5.4.4.c	Components shall encrypt remote maintenance paths to the firewalls and PEPs.	MA-4, SC-7
5.4.4.d	Components shall conduct quarterly firewall and PEP testing to ensure that ensure that most recent policy changes have been implemented and that *all* applied policies and controls are operating as intended.	SC-7
5.4.4.e	Component SOCs shall ensure reports on security operations status and incident reporting are provided to the CISO Security Operations Program Director as required.	IR-6
5.4.4.f	All Department and Component firewalls and PEPs shall be administered in coordination with DHS security operation capabilities, through the DHS SOC or Component SOCs.	SC-7
5.4.4.g	All DHS Policy Enforcement Points (PEP) shall provide protection against denial-of-service attacks.	SC-5
5.4.4.h	CBP shall determine protocols and services permitted through the CBP PEPs. CBP may restrict traffic sources and destinations at the CBP PEPs.	SC-7
5.4.4.j	The DHS SOC shall oversee all enterprise PEPs, including the CBP PEPs.	---
5.4.4.k	Certification and/or accreditation in accordance with the procedures established in this handbook	CA-2
5.4.4.l	Configured to prohibit any protocol or service that is not explicitly permitted by CBP LAN standards and security certified configurations	AC-6, CM-3, and CM-7
5.4.4.m	The DHS SOC provides a central coordination and reporting point to integrate the efforts of CBP and other component SOCs (including the HSDN SOC), creating a "community of the whole." While SOCs are localized, specialized, and operational within each Component, the central reporting structure enables Department-wide coordination and collaboration	PM-1
5.4.4.n	Audit capabilities of the system must be enabled to collect the following information, at a minimum: • Source and destination IP address • Time and date of event • Uniform Resource Locator (URL)	AU-2

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000277

Policy ID	CBP Policy Statements	Relevant Controls
	• Access attempts to network services • Rejected source-routed addresses • Use of Internet Control Message Protocol (ICMP) • Redirects	
5.4.4.o	Archived audit logs will be maintained for a minimum of five years	AU-11
5.4.4.p	Provide intrusion detection capability, either as an integral part of the firewall or through a separate, add-on appliance. This Intrusion Detection System (IDS) must provide for a scalable response to attacks and remote notification.	AC-6, IR-4, and SI-4
5.4.4.q	The System Administrator (SA) for any CBP-owned firewall or server accessible from the Internet or an Extranet should not be the same person that is the SA for the internal system or network connected to the Internet or the Extranet by the firewall or server.	AC-5
5.4.4.r	The transmission of CBP-owned, non-public information from a CBP server over private networks, the Internet, or Extranet to any user must use a secure protocol that provides FIPS 140-2 compliant cryptographic protection	SC-13
5.4.4.s	Any CBP-owned firewall or server for which Internet or Extranet connectivity is approved must prohibit the login of a SA from the Internet or Extranet.	SC-11
5.4.4.t	Any CBP-owned firewall or server accessible from the Internet or an Extranet must provide an intrusion detection capability that will provide an immediate alert when an attack or attempt to bypass system security occurs.	SI-4, SI-5,
5.4.4.u	Any CBP-owned firewall or server accessible from the Internet or an Extranet must maintain audit records of all transactions, and such records must be stored on tamper-proof media or routed to a host that is not accessible from the Internet or Extranet.	AU-9
5.4.4.v	The operating system and all associated software of any CBP-owned firewall or server accessible from the Internet or any Extranet must be kept current with respect to security-related patches, modifications, fixes, etc. Patch updates must follow the guideline set forth within the Information Security Vulnerability Management (ISVM) notice published by DHS-SOC. The Change Control Board (CCB) prior to deployment must approve all patches. In the case of emergency patches to mitigate a known, immediate threat to the CBP network, the CCB may be bypassed with written approval of the CISO.	CM-2, SI-2
5.4.4.w	The implementation and use of Common Gateway Interface (CGI) scripts on any firewall or server must be monitored and controlled. Scripts must not allow users to activate command-level instructions or to perform any system administrator function. All scripts must be limited to performing their functions from within their own directory with all Server Side Includes (SSIs)	SA-9

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000278

Policy ID	CBP Policy Statements	Relevant Controls
	disabled.	

Responsibility for the future deployment and management of firewalls will be determined at a later date. General responsibilities are included below.

Firewall Responsibilities
CISO
• Develop procedures and schedules for deploying firewall systems.
ISSOs and ADP Support Personnel
• Assist CBP teams in the installation and configuration of firewall systems.
Site Managers
• Ensure that the installation team receives necessary support during and after firewall installation.
SOC
• Manage firewalls in accordance with DHS and CBP firewall policies.
• Maintain change control over firewalls and maintain proper firewall configuration.
• Evaluate, process, and approve changes to firewall configuration.

5.4.4.1 Firewall Basics

A firewall is a system or group of systems that enforce an access control policy between two networks. The actual means by which this is accomplished varies widely. Associated with the basic capabilities of access control, firewalls can authenticate the source and destination of a given data path, provide network address translation (NAT) and port address translation (PAT) and log all traffic passing through them. The logging is either done on the machine on which the firewall software runs on, or is logged to a separate machine for audit and intrusion forensic analysis.

Firewalls are often associated with filtering devices, which screen incoming (and possibly outgoing) data traffic for viruses and malware in the form of mobile code. By offloading these responsibilities to ancillary machines, the firewall can allow higher rates of data transmission.

Mobile (downloadable) code is software that is transmitted from a remote source across a network to a local system and then executed on that local system (e.g., personal computer, PDA, mobile phone, Internet appliance). Examples include ActiveX controls, Java applets, script run within the browser, and HTML email. Although mobile code is a legitimate method for distributing application software, it is most frequently associated with "malicious mobile code" (e.g., viruses, worms, Trojan horses) that executes without the permission of or any explicit action by the local system's owner/user.

Firewalls also have two facets with respect to encryption. A frequently used mechanism is the SSHv2 protocol (Secure Shell version 2). This facility can provide for authentication by a digital

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000279

certificate or a two-factor authentication mechanism, as well as strong encryption. Such a connection should only be allowed from the protected (internal) side of a firewall, so that unauthorized outsiders are unable to affect a change.

Firewalls often have the capability to implement encrypted data communications. Although this approach might be slightly more economical, it is more prudent to have a system that functions as a firewall serve a single purpose. A separate encryption server (behind the firewall) is afforded the extra protection of being shielded by a firewall. Encryption, moreover, involves a substantial amount of computational power, which would slow down the operation of the firewall. Lastly, if the firewall system is compromised, the encryption facility is not automatically compromised at the same time.

NIST SP 800-10, *Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls*, and NIST SP 800-41, *Guidelines on Firewalls and Firewall Policy*, offer guidance with respect to firewalls and the functions they can serve.

5.4.4.2 Firewall Deployment

Firewall systems have been deployed to various CBP sites, and additional systems are scheduled for deployment as part of the continuing effort to provide necessary security safeguards.

Firewalls are not used solely to provide boundary protection from the outside world. In commercial environments, for example, the fiscal processing systems may be protected from the remainder of the network by firewalls. In a similar manner, CBP can use firewalls to segment systems that have various levels of sensitivity, unless they are so classified that connection to the network should be prohibited.

5.4.4.3 Firewall Management

All firewalls for unclassified and collateral classified systems shall be under the control of the DHS and CBP SOCs, who are responsible for providing direction and guidance for firewall settings and rule sets. The actual application of all firewalls shall be under the DHS SOC.

5.4.4.4 Unauthorized Firewall Protocols and Services

All unused firewall and gateway ports will be disabled. Use of the following firewall protocols and services are unauthorized, and the associated ports will be disabled.

Table 5.4.4.4: Unauthorized Firewall Protocols and Services

Unauthorized Firewall Protocols and Services		
BFTP	NFS	RLP
Chargen	NNTP	SNMP*
Echo	POP	SunRPC
Finger	POP2	Supdup

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000280

Unauthorized Firewall Protocols and Services		
Link	POP3	Syslog
LPD	Portmap	GOPHER
Name	RCF	UUCP
Netbios	RIP	X Protocols
ICMP Redirects	NIS	R Commands
UDP Boot Services	RIP Daemon, Routed	FTP
TelNet		

(b) (7)(E)

Use of any unauthorized service must have formal approval of the AO. A waiver or exception must be obtained before implementing any of these services. Approval may not be granted unless it can be demonstrated that the selected firewall configuration provides adequate security in accordance with CBP Certification and Accreditation (C&A) security requirements and CBP system hardening guidance in accordance with CBP-developed protection profiles.

5.4.4.5 Authorized Protocols and Services

Secure protocols and services, such as Secure Shell (SSH), Secure File Transfer Protocol (SFTP), and Transport Layer Security (TLS)[6], may be permitted where it can be demonstrated that they do not negatively impact the security of network operations or other interconnecting systems. Hardening guidelines must be followed for implementation and maintenance of such systems. Use of such protocols or services must be approved by the AO and fully documented in C&A documentation of systems employing these technologies.

5.4.4.6 Virtual Private Network Personal Firewalls

CBP-owned laptops or desktops requiring broadband connections must be equipped with a CBP-approved personal firewall. The required security configuration of the personal firewall must include the following features:

1. The personal firewall shall block externally originated incoming network requests. An exception is permitted for TIVOLI and CBP trusted security-monitoring systems.

[6] *In accordance with NIST guidelines (SP 800-52), Transport Layer Security v 1.0, when properly configured is approved for use with federal information. Secure Sockets Layer 3.0 (SSL v 3.0) is not approved for federal information because the cryptographic algorithms used are not FIPS-Approved.*

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000281

2. Users will not have the capability to disable the personal firewall. Any command line scripts associated with firewall activity shall be hidden from user view or access.

3. The personal firewall shall be used with and within the DHS/CBP trusted networks.

4. An outgoing Virtual Private Network (VPN) connection is only permitted via personal firewall. Incoming broadband connections to the host are permitted only through a VPN tunnel.

5. Personal firewall outgoing, IP-initiated communications shall be permitted only to DHS/CBP trusted sub-nets. An exception is permitted for Dynamic Host Configuration (DHCP)-initiated requests required to establish the VPN tunnel.

6. The personal firewall must operate with CBP network firewall systems.

7. The personal firewall shall not allow users to initiate communications directly to the Internet. All Internet communications, if any, shall be established through direct connection with the LAN at a DHS/CBP trusted site or through the CBP VPN.

8. The personal firewall is required for the broadband VPN overlay product on the certified CBP Standard Desktop Operating System.

9. The personal firewall will be initiated when the desktop or laptop system is powered on and remain on until the system is powered off.

10. CBP systems using broadband VPN must be configured to automatically disable any capability to bridge traffic from other network connections via modem or wireless access points. Users must not have the capability to change this configuration.

5.4.4.7 Firewall Exceptions and Waivers

Exceptions and waivers for CBP firewall policy and the configuration requirements in this section require formal written requests to and approval from the CBP AO and the CISO prior to changing currently authorized configurations to operate unauthorized ports and services. Any such changes to approved configurations must be fully documented.

Requests for an exception or waiver must be first submitted to the CISO and must provide the following information:

1. A description of the desired exception and waiver

2. A detailed business case to justify use of the unauthorized service

3. A risk assessment associated with implementing the service

4. Actions taken to mitigate identified risks

Exceptions or waivers that have been approved by the CBP AO must be included in an updated accreditation package reflecting the new services and their associated risks. New services must

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000282

not become operational until the CBP AO has re-approved the system and granted Approval-To-Operate (ATO) with use of those services.

5.4.5 Router Device Management

The following practices should be followed in order to maintain the security posture and availability of the CBP networking devices:

1. Communications between devices must be secured by restricting communication to known authorized IP addresses at a minimum.

2. All network management ports must be disabled except those needed to support the operational commitments of the site.

3. The router administrator will manage devices through out-of-band or direct connection. If out-of-band management is not feasible the use of "in-band" management will be limited to situations where the use of out-of-band management would hinder operational commitments or in an emergency situation. The CISO will approve the use of " in-band" management on a case-by-case documented basis

4. All security-related patches applied for out-of-band access will use the currently supported version of Secure Shell (SSH).

5. Where management of remote site devices is impractical using the direct connection method, secure dial-up method via an encryption utility is acceptable. Termination of the secure dial-up must be at the Terminal Access Controller Access Control System+ (TACACS+) server inside the secure enclave.

6. Authenticated access control using out-of-band management must be used for access via remote access devices. This will be enforced with strong two-factor authentication, encryption of management session, and auditing. This method ensures only authorized network administrator access via remote devices.

7. Due to bandwidth limitations, use of "in-band" management will be restricted to a limited number (less than 10) of authorized IP addresses, including the System Administrator (SA) and his backup. This may be accomplished through the vendor's Network Management System (NMS) or by using an access control list.

8. In-band connections will use strong two-factor authentication for all managed communications devices.

9. Where port management and port protection services are available on communication devices, they will be activated on all authorized port connections.

10. Banners warning users that their computer activity may be monitored must be displayed on all network management devices allowing Hyper-Text Transfer Protocol (HTTP) access. All devices that do not support warning banners must be documented.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000283

5.4.6 Internet Security

Over the past few years, government, private industry, and academia have developed security techniques, practices, and tools to reduce the ever-growing risks associated with interconnected networks. The policy contained in this section establishes minimum-security requirements to connect CBP information systems with the Internet, the CBP Intranet, and any Extranet. In some cases, business needs will determine the necessity of more stringent connectivity requirements.

Any CBP-owned Internet Web site providing public information, regardless of the ownership of the service provider, must conspicuously display the Security Notification, documented in Section 5.2.3, either in full text on the first page or with a button containing the words "Legal & Privacy Notices" located conspicuously on the first page.

This section provides specific CBP technical policy regarding the use and proper configuration of firewalls and the management of dial-up connections and other protocols.

Policy ID	CBP Policy Statements	Relevant Controls
5.4.6.a	Any direct connection of CBP networks to the Internet or to extranets must occur through firewalls and PEPs that have been certified and accredited.	SC-7
5.4.6.b	Firewalls and PEPs shall be configured to prohibit any protocol or service that is not explicitly permitted.	CM-7, SC-7, SC-8, SC-9
5.4.6.c	CBP shall ensure that all executable code, including mobile code (e.g., ActiveX, JavaScript), is reviewed and approved by an appropriate senior official prior to the code being allowed to execute within the CBP environment. [Note: When the technology becomes available and code can be vetted for security, the policy will be "Ensure that all approved code, including mobile code (e.g., ActiveX, JavaScript), is digitally signed by the designated CBP authority and that only signed code is allowed to execute on CBP IT systems."]	SC-18
5.4.6.d	Telnet shall not be used to connect to any CBP computer. A connection protocol such as Secure Shell (SSH) that employs secure authentication (two factor, encrypted, key exchange, etc.) and is approved shall be used instead.	CM-7, SC-7, SC-8, SC-9
5.4.6.e	File Transfer Protocol (FTP) shall not be used to connect to or from any CBP computer. A connection protocol that employs secure authentication (two factor, encrypted, key exchange, etc.) and is approved shall be used instead.	CM-7, SC-7, SC-8, SC-9
5.4.6.f	Remote Desktop connections, such as Microsoft's Remote Desktop Protocol (RDP), shall not be used to connect to or from any CBP computer without the use of an authentication method that employs secure authentication (two-factor, encrypted, key exchange, etc).	AC-17, IA-2

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000284

Policy ID	CBP Policy Statements	Relevant Controls
5.4.6.g	To ensure the security and availability of CBP information and information systems the CBP CIO or CISO may direct for specific Internet websites or categories to be blocked at the CBP Trusted Internet Connections as advised by US-CERT, the DHS and CBP SOCs, or other reputable sources.	---
5.4.6.h	All users accessing Internet Hyper-Text Transfer Protocol (HTTP) sites must use a CBP-approved available HTTP browser. Such browsers must incorporate all vendor-provided security patches, modifications, fixes, etc. Patch updates must follow the guideline set forth within the Information Security Vulnerability Management (ISVM) notice published by DHS-SOC. All HTTP browsers will be configured securely according to CBP security standards set by the CISO. Security settings on HTTP browsers are not to be modified by CBP users at any time for any reason.	SC-7
5.4.6.i	All files obtained from the Internet or an Extranet must be scanned upon receipt before they are opened or used. CBP-approved and properly updated anti-virus scanning and detection software must be used.	SI-3
5.4.6.j	CBP-owned sensitive information shall not be stored on or distributed via publicly accessible Web hosting.	MP-1
5.4.6.k	Electronic mail traffic between the Internet and internal networks must be implemented with centrally managed Simple Mail Transfer Protocol (SMTP) gateways.	AC-13
5.4.6.l	Proxy applications must be used to route mail through firewalls.	AC-4
5.4.6.m	No CBP data (in any form including "mail box" data, other than the account information necessary to operate the system) will be located on application gateways or firewall devices.	AC-4
5.4.6.n	All network switch ports (i.e. network jacks) in public spaces such as primary and secondary inspection areas must have security controls to prohibit unauthorized access.	PE-1, PE-2, PE-3, and PE-7
5.4.6.o	Any CBP-owned Internet Web site providing public information, regardless of the ownership of the service provider, must conspicuously display the approved legal and privacy notices. It must be displayed either in full text on the first page or with a button containing the words "Legal & Privacy Notices" located conspicuously on the first page. The accepted language is located in Section 5.2.3	AC-8

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000285

Internet security responsibilities are provided below.

Internet Security Responsibilities
CBP AO • Ensures all external network connections are protected by a firewall and possibly other boundary protection devices that have been certified and accredited at a level commensurate with the sensitivity of the information to be protected. • Ensures dial-up connections are addressed in the C&A documentation. **ISSOs** • Ensure all external network connections are addressed in the risk assessment and System Security Plan. • Ensure all external network connections are protected by a firewall and possibly other boundary protection devices. • Ensure all boundary protection devices are properly configured and monitored. • Ensure dial-up connections are properly configured and secure. **Network/System Administrators/Field Technology Officers** • Ensure all boundary protection devices are properly configured and monitored. • Ensure firewall ports that allow file and printer sharing, whether through Microsoft NetBIOS, Common Internet File Service (CIFS), Network File Services (NFS), or TCP SMB (Server Message Block) protocols, are closed. • Ensure firewalls are configured to prohibit any protocol or service that is not explicitly permitted. • Ensure the following are prohibited: o Telnet (clear text) connections. o FTP unsecured (clear text) file transfers. o SNMP protocols that can be used to monitor and control systems o Cross boundary routing broadcasts o Address Resolution Protocol (ARP) messages o DNS communications across the boundary (by using split DNS with zone transfer authentication) o Unsecured file transfers o Mobile code (e.g., ActiveX, JavaScript) that has not been reviewed and digitally signed by an appropriate DHS authority. • Ensure dial-up connections are properly configured and secure.

Sound network security practice dictates that all network connections are identified and the threats and vulnerabilities associated with these connections be analyzed. The guidance

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000286

provided in Section 5.4, *Network and Communications Security*, specifically with regard to ISAs, also applies to connections to Internet and extranet connections.

An extranet is a private network encompassing that portion of an organization's intranet that it chooses to securely share—via the Internet and the public telecommunication system—with external suppliers, vendors, or customers. An extranet requires security and privacy and may involve firewalls, digital certificates, message encryption, and virtual private networks that can tunnel through the public network.

All external connections, including extranets, must be identified and documented in the Security Plan, the risk assessment, and other C&A documentation as necessary. The risks associated with these connections must be addressed during the C&A process. Additionally, external network connections are to be reviewed annually by ISSO and documented in the annual information security assessment.

Adequate protection requires the proper selection and installation of firewalls and other boundary devices, Intrusion Detection Systems, and ancillary encryption or filtering devices. These devices must be certified and accredited prior to their use on DHS networks. Implementation guidance for firewalls is discussed in Section 5.4.4. Intrusion Detection Systems are covered in Section 5.4.2.1 and encryption is addressed in Section 5.7.1. The adequacy of these devices must be monitored and reviewed as part of periodic information security assessments.

Firewalls must be configured to prohibit any Transport Control Protocol (TCP), User Datagram Protocol (UDP) service, or other protocol that is not explicitly permitted. Of particular concern is the need to close ports that allow file and printer sharing, whether through Microsoft NetBIOS, Common Internet File Service (CIFS), Network File Services (NFS), or TCP Server Message Block (SMB) protocols. The use of file and printer sharing is associated with numerous vulnerabilities related to everything from enumeration of devices and user accounts to anonymous control of systems without authorization.

Telnet, which is prohibited on CBP systems and networks, is a utility program and protocol that allows one computer to connect to another computer on a network. After providing a username and password to login to the remote computer, a user can enter commands that will be executed as if entered directly from the remote computer. Telnet transfers all information in "clear text" (human readable text), which allows Internet service providers (ISPs) and other users on the Internet, intranet, or LAN to intercept the traffic it creates. This could allow unauthorized users to get user IDs and passwords, capture information or commands that are being sent, and potentially alter the information in the telnet connection. Telnet uses a commonly known port, which makes it easy for someone to "sniff" telnet traffic. The approved solution for this functionality is to use Secure Shell (SSH). SSH is an IETF protocol that provides encrypted connections and supports authentication with digital certificates and other secure methods of authentication.

FTP is a means of transferring files from one computer to another. FTP transfers all information in clear text (human readable text), which allows ISPs and other users on the Internet, intranet, or LAN to intercept the traffic it creates. This allows unauthorized users to capture information or commands and possibly alter the information in the FTP connection. FTP generally uses a commonly known port, which makes it easy for someone to "sniff" FTP traffic. The approved solution for this security risk is to use the Secure File Transfer Protocol (SFTP) component of Secure Shell (SSH). SSH is a FIPS 140-2-approved Internet Engineering Task Force (IETF)

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000287

protocol, which provides encrypted connections and supports authentication with digital certificates and other secure methods of authentication.

Use of the following is expressly prohibited:

- Telnet
- File Transfer Protocol (FTP)
- Simple Network Management Protocol (SNMP), which can be used to monitor and control systems
- Address Resolution Protocol (ARP) messages

The following have significant risks and shall be used only in conjunction with appropriate countermeasures and risk-reduction procedures:

- Cross boundary routing broadcasts
- DNS communications across the boundary (by using split DNS with authentication of zone transfers)
- Mobile code (e.g., ActiveX, JavaScript) that has not been reviewed and digitally signed by an appropriate DHS authority.

Implementation guidance for securing dial-up connections is addressed in Section 5.4.1, Remote Access and Dial-In. If a dial-in connection can be justified, it must be strictly controlled.

5.4.6.1 Securing Internet Connections

Internet connectivity exposes CBP systems to damage caused by adversaries exploiting CBP vulnerabilities (e.g., malicious code). In order to limit the risk, users at a minimum must follow the Rules of Behavior listed below:

1. CBP Internet connections are for official business and use of the Internet must be within the scope of duties of the individual unless access has been approved for Limited Personal Use. (See Section 4.8.9)

2. CBP equipment capable of providing Internet connectivity will not be used for any activity that would adversely affect the confidence and public integrity of the CBP service, even when used for approved "Limited Personal Use."

3. The STP Branch reserves the right to review, audit, intercept, access, and disclose information on all Web sites visited by any user during his/her Internet connectivity. The page contents of Internet Web sites obtained for any purpose may be disclosed within the CBP domain without the permission of the employee. Supervisors are responsible for ensuring that employee use of CBP-owned office equipment for non-government purposes is in accordance with the CBP Limited Use Policy.

4. CBP sensitive information must not be transmitted via the Internet without using approved security controls, such as encryption, and obtaining authorization.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000288

5. Users may accept session "cookies," which are small text files that some Web sites store on your hard-drive temporarily. Government sites will provide clear and conspicuous notice that "cookies" are used, but these are deleted at the end of the session.

6. Browser configuration settings will not be set to accept permanent cookies unless explicitly approved for official purposes by the CISO.

7. The Internet should not to be used to send (upload) or receive (download) copyrighted materials, trade secrets, proprietary financial information, CBP law enforcement data or similar materials without the express permission of the data owner. The confidentiality of Internet traffic is not guaranteed.

8. CBP users are not authorized to download copies of data or software systems from the Internet unless the activity is associated with an approved/official procurement process or approved by the CISO. All authorized downloads must be scanned for viral infection before installing the software.

9. Remote Desktop connections, such as Microsoft's Remote Desktop Protocol (RDP), shall not be used to connect to or from any DHS computer without the use of an authentication method that employs secure authentication (two-factor, encrypted, key exchange, etc).

10. The following Internet, Intranet, and Extranet activities are unauthorized:

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000289

Table 5.4.6.1: Unauthorized Network Activities

Unauthorized Service	Reason
Chat/Instant Messaging	Security Vulnerability
ICQ - "I Seek You" - Internet chat paging program	Security Vulnerability
IRC - Internet Relay Chat	Security Vulnerability
mIRC - Windows online chat program	Security Vulnerability
Net Meeting	Security Vulnerability
Realvideo	Excessive Bandwidth Usage
Quick Time	Excessive Bandwidth Usage
Peer-to-Peer (P2P) File Sharing[7]	Security Vulnerability and Excessive Bandwidth Usage

CBP-owned standalone computers may be used to connect to the Internet if the computers do not contain sensitive information and will not, at any time, be connected to a CBP network. In such cases, they are exempt from the Internet inter-connectivity policy. Other than standalone computers, the following rules apply for any connectivity of a CBP-owned system or network to the Internet or an Extranet:

1. Any connection of a CBP-owned system or network to the Internet or any approved Extranet must occur through an OIT-provided secure gateway or firewall.

2. Connection of any CBP-owned classified system to the Internet or Extranet is strictly forbidden.

3. Any CBP-owned Intranet must be isolated and safeguarded from connectivity to the Internet or any Extranet.

4. Any CBP-owned server that stores non-public information for which an Internet or Extranet connection is approved must perform user identification and authentication for each user before allowing access. Identification and authentication will be performed in

[7] *This is unauthorized for workstations. Network file sharing may be approved if it is justified and documented.*

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000290

a secure manner not subject to disclosure or capturing. All passwords must be encrypted across the Internet or any Extranet.

5.4.6.2 Securing Web Clients

Web technology is the part of network communications that allows parties to communicate using Hyper-Text Transfer Protocol (HTTP) or some variant of HTTP. Many of the security requirements of network communications apply directly to the use of Web technology, because Web technology is essentially an enhanced form of network communications.

The Web client and associated workstation must be appropriately configured to provide adequate security. At a minimum, the following requirements must be met:

1. All certificates must be protected with passwords that adhere to guidelines provided by the CISO. (A certificate is an association between an identity and a public key). Certificates are used as a way to verify the authenticity of an organization or individual.

2. Only certification authorities approved by the CISO may issue certificates that are installed on information systems that process sensitive or classified information. (A certification authority is an organization that issues public-key certificates.)

5.4.6.3 Securing Servers

Various Web technologies provide a convenient means for sharing information. Such technologies are examples of push/pull technology, which allow one entity to push information into a location and another entity to pull it from that location. Documents that an organization wishes to share with other organizations could be placed on (pushed out to) an external web and then anyone able to access the server could download (pull off) the information. Documents that an organization wishes to share internally could be placed on an internal (within an organization's system) Web, allowing authorized individuals within the organization to access the server download (pull off) the information. All servers must follow the guideline set forth within the Information Security Vulnerability Management (ISVM) notice published by DHS-SOC.

Servers can be separated into two broad categories: public or general access servers and restricted access servers. Descriptions of both types of servers are provided below.

Public or General Access Servers

Information placed on a public server is available to anyone authorized to access the Internet, Intranet, or a Local Area Network (LAN) on which the server resides. General user accounts are not permitted on public or general access servers.

Restricted Access Servers

Data placed on a restricted access server will only be accessed by authorized and authenticated users. In addition to the requirements stated earlier in this section, restricted access servers must also implement the following security requirements:

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000291

1. At a minimum, the underlying operating system must comply with the DHS security requirements for confidentiality, integrity, availability, and non-repudiation.

2. Strong authentication is required for all users accessing restricted servers; and all such accesses will be audited.

3. Web servers shall support secure Web technology. Unapproved web services on any device supporting such services shall be disabled in accordance with approved, standard CBP security configuration.

4. Web servers may not be enabled on routers, switches, printers or workstations that are not authorized web servers configured to CBP standards. Any such operational web servers identified shall be disabled.

5.4.6.4 Mobile Code

Mobile code is Web-based code downloaded onto a user's client and run by the user's browser. Examples of such Web-based mobile code include Java, JavaScript, and ActiveX. A large set of mobile code normally involves an explicit decision to execute, either by the user or by an application. Examples of mobile code directly executed by the user include: Perl, TCL/TK, REXX, Python, VB, Java, and platform-specific executables, such as those with the filename suffix "com" or "exe."

Indirect execution of mobile code presents a significant security risk to systems connected to the Internet or external systems. Users may not even be aware that a separate executable has been downloaded on their machine. Examples of mobile code indirectly executed by an application include MS Office macros, ActiveX, PostScript, and FileMaker. Hostile mobile code or executable content can introduce viruses or other malicious code to modify programs, allow unauthorized access, corrupt data, or deny service. Hostile mobile code or executable content is completely different from the more traditional malicious codes, such as viruses and worms. Moreover, they are probably not as detectable by standard antiviral software. Therefore, to reduce the risk of introducing hostile mobile code to the environment, CBP must implement security controls and policy for this technology.

Per DHS policy: "All mobile code (e.g., ActiveX, JavaScript) shall be reviewed and approved by an appropriate senior official before it is allowed to execute on DHS IT systems. [Note: When the technology becomes available, the policy will be "Ensure that all approved mobile code (e.g., ActiveX, JavaScript) is digitally signed by the AO and that only signed code is allowed to execute on DHS IT systems.] "

The CISO has approved a mobile code policy that enables web-based access to external government (e.g. federal, state, and local law enforcement) systems that use mobile code when it enhances the user's ability to perform his/her job. This can be accomplished by adding the agency owning the web application to the user's list of trusted sites. However, these systems must undergo a review of their security controls. This could be accomplished via a review and/or testing by the LAN Engineering Team. In addition, an Interconnection Security Agreement (ISA) must be in place with the external government agency owning the web-based application, which documents the security controls.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000292

The table below categorizes types of mobile code based upon decreasing associated risk, with Category 1 representing the highest risk.

Table 5.4.6.4: Mobile Code Risk Categories

Mobile Code Category	Risk Level	Description	CBP Authorization Level
Category 1	Most dangerous	Includes ActiveX and script languages interpreted at the operating system command level, as well as newly emerging code not yet categorized.	Not allowed unless authorized by CBP management and additional security controls are in place. Signed code only, when technology is available.
Category 2	Moderately dangerous	Includes Java mobile code, PostScript, and various scripting languages running within the confines of a desktop application.	Authorized limited use, as permitted by workstation configuration security standards. Signed code only, when technology is available.
Category 3	Least dangerous	Includes Shockwave Flash content, PDF, VBScript, and ECMA script-variant scripting languages interpreted within the confines of a browser.	Authorized limited use, as permitted by workstation configuration security standards. Signed code only, when technology is available.

1. Mobile code in new applications should be written and controlled so it can only be invoked as intended.

2. Internet Explorer must be configured to prevent the execution of unsigned Active-X code.

3. Use of mobile code in application development requires security review early in the design phase and potentially the submittal of a detailed request with justification to the Director, Security and Technology Policy (STP) Branch. The CISO will review the associated risks with the designed implementation of this code and request approval from the AO, if appropriate.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000293

5.4.7 Electronic Messaging and Email Security

All CBP personnel are reminded that there is no right of privacy in any CBP computer network system. CBP may access and disclose the contents of any electronic messages without consent of the owner/user when there is a legitimate business need, including but not limited to, the following circumstances:

1. In the course of an investigation or inquiry
2. For the protection and safety of CBP personnel
3. To prevent interference with the CBP mission
4. To locate information required for CBP business that is not more readily available by some other means

Email Bulletin Boards

Email Bulletin Boards are an approved method to provide information and notices to CBP personnel. Informational notices may include general notices, training seminars, facility information (e.g., power outages, system upgrades, training), office information (i.e., parties, death notices, leave share), medical services (i.e., flu shots, blood drives, health screenings), employee benefits (i.e., Thrift Saving Plan open season, Combined Federal Campaign), and Equal Employment Opportunity. The Help Desk, Technical Operations Division, will provide any assistance required in the operation or maintenance of a Bulletin Board.

The CBP email gateway provides email monitoring for spam and virus activity at the gateway.

A relationship has been established with the SOC to enable communications. SOC personnel shall be trained to respond to incidents pertaining to email security and shall assist the email Steward as necessary.

Email is the most commonly used application for exchanging data electronically. The email process can be divided into two main components: (1) mail servers, which deliver, forward, and store mail, and (2) clients, which interface with the user and allow them to read, compose, send, and store messages.

Instant messaging (IM) and "I Seek You" (ICQ) tools provide similar capabilities to email, but are inherently less secure; the technology to secure IM and ICQ tools is still being developed. IM and ICQ tools possess all of the risks associated with unsecured email, including the capability to install software or malware on a recipient's system without their knowledge. If IM and ICQ tools are to be used, they should not include or communicate with publicly available IM or ICQ tools provided by several Internet Service Providers. Any such tools employed need to be capable of blocking any format except pure text. This specifically includes blocking executable code, Web links, video or still images, and audio. The use of Instant Messaging and ICQ is not currently authorized for use on sensitive systems and networks.

Second only to Web servers, mail servers are the host on a network that is most often targeted by intruders. Mail servers are targeted because they communicate, to some degree, with untrusted third parties. Additionally, email has been an effective method of passing malicious code

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000294

(viruses). As a result, mail servers, mail clients, and the network infrastructure that supports them must be protected. Email security issues include:

1. Flaws in the email application software have been used as the means of compromising the server and subsequently the associated network.
2. Denial of service (DoS) attacks may be directed to the mail server.
3. Sensitive information on the mail server may be read by unauthorized individuals or changed in an unauthorized manner.
4. Unencrypted sensitive information transmitted between a mail server and email client could be intercepted.
5. Information within the email may be altered at some point between the sender and recipient.
6. Viruses and other types of malicious code may be distributed throughout an organization via email.
7. The sending of inappropriate, proprietary, or other sensitive information via email could expose an organization to legal action.

Policy ID	CBP Policy Statements	Relevant Controls
5.4.7.a	Components shall correctly secure, install, and configure the underlying email operating system.	---
5.4.7.b	Components shall correctly secure, install, and configure mail server software.	---
5.4.7.c	Components shall secure and filter email content.	---
5.4.7.d	Components shall deploy appropriate network protection mechanisms, such as: Firewalls Routers Switches Intrusion detection systems.	---
5.4.7.e	Components shall secure mail clients.	---
5.4.7.f	Components shall conduct mail server administration in a secure manner. This includes: Performing regular backups Performing periodic security testing Updating and patching software	---

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000295

Policy ID	CBP Policy Statements	Relevant Controls
	Reviewing audit logs at least weekly	
5.4.7.i	Auto-forwarding or redirecting of DHS email to address outside of the .gov or .mil domain is prohibited and shall not be used. Users may manually forward individual messages after determining that the risk or consequences are low.	---
5.4.7.j	Classified information may not be posted in CBP unclassified environments or systems. Classified electronic messages will only be transmitted through a secure data network approved for classified data.	---
5.4.7.k	Only personnel who have at least a completed Limited Background Investigation (BI) will be granted access to the CBP email system. All email accounts will be created, using at a minimum, the official last name as stated within the BI package.	---
5.4.7.l	Email addresses of CBP employees will not be given to anyone without the express permission of the owner. Additionally, the requesting individual must substantiate that he/she has a valid need to obtain the information.	---
5.4.7.m	All material sent or received on the email system remains the property of CBP, not the property of the employee.	---
5.4.7.n	Everyone is responsible for preventing virus infections. Do not open attachments originating from unknown non-CBP addresses. Call your System Administrator (SA) for assistance.	---
5.4.7.o	Electronic messages will not be used to send (upload), receive (download), or disseminate any material that is considered to be of a sensitive nature, without the express approval of its data owner.	---
5.4.7.p	Exercise care when using email to send extremely large files to distribution lists. Such a practice could lead to flooding of the network or denied services. There is a 10 MB size limit for email messages.	---
5.4.7.q	Email will be available on-line for 90 days. After 90 days, messages that have not been archived will be automatically purged from the active email system.	---
5.4.7.r	All email must be recorded or archived. Archived email will be retained on CBP centralized storage devices in accordance with statutory requirements for the retention of electronic data. Direct user access to the archived data on the centralized storage devices is authorized for 1 year.	---
5.4.7.s	Email lists may be established to distribute mail to specific CBP populations. The mailing list owner is responsible for maintaining the list. The appropriate CBP management must approve all messages addressed to 100 or more recipients before distribution. Personnel who do not adhere to this will be subject to disciplinary action. Mass email lists of 500 people or more are only	---

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000296

Policy ID	CBP Policy Statements	Relevant Controls
	authorized for use under the following conditions: • National or CBP security, • Facility emergencies (e.g., facility closures, building evacuation), or • Announcements from CBP executive management.	
5.4.7.t	Users may establish personal email lists. For organizational level email lists, a request must be submitted through the Help Desk outlining the names, email addresses to be included, and a point of contact from the requesting office to act as the administrator for the maintenance of the list.	---
5.4.7.u	Report suspected violations of electronic messaging policy to the CSIRC and notify your supervisor/manager if it is a significant incident. (See Attachment F for details on incident reporting procedures and definitions of incidents.)	---
5.4.7.v	Creating, copying, transmitting, or retransmission of chain letters is strictly prohibited.	---
5.4.7.w	Transmitting sexually explicit or sexually oriented materials is strictly prohibited.	---
5.4.7.x	Disseminating offensive or disruptive messages that address topics such as a person's age, sexual orientation, religious or political beliefs, national origin, or disability is strictly prohibited.	---
5.4.7.y	Running a business from email is strictly prohibited.	---
5.4.7.z	Setting up personal accounts on the Internet and forwarding the information to a CBP email system is prohibited.	---
5.4.7.aa	Using a CBP email address as a personal email address to receive advertisements is prohibited.	---
5.4.7.bb	Sending documents in violation of copyright laws is strictly prohibited.	---
5.4.7.cc	Unauthorized viewing of electronic messages is strictly prohibited.	---
5.4.7.dd	Constructing electronic communication so it appears to be from someone else is strictly prohibited.	---
5.4.7.ee	Obtaining access to the files or messages of others with no substantial CBP business purpose is strictly prohibited.	---
5.4.7.ff	Attempting to breach security measures on any electronic messaging system is strictly prohibited.	---
5.4.7.gg	Attempting to intercept any electronic messaging transmissions without proper	---

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000297

Policy ID	CBP Policy Statements	Relevant Controls
	authorization is strictly prohibited.	
5.4.7.hh	Forwarding email to home email accounts is prohibited.	---
5.4.7.ii	The use of Internet webmail (Gmail, Yahoo, AOL, etc.) or other personal email accounts is not authorized over DHS furnished equipment or network connections.	---
5.4.7.jj	All DHS email systems are required to use the common naming convention with distinguishing identifiers for military officers, contractors, foreign nationals, and U.S. Government personnel from other Departments and agencies.	---

Electronic Messaging and Email security responsibilities are provided below.

Electronic Messaging and Email Responsibilities
CISO • Establishes policy to secure CBP email systems. • Advise on methods for securing CBP email systems. • Enforce CBP email security policies. **Certifying Agents** • Certify that adequate security controls are in place for email systems. **AO** • Ensure that adequate email security controls are in place prior to accreditation of the system. **System/Network Administrators** • Ensure email security controls are in place and functioning as intended. • Ensure email security controls provide the security features outlined in this document. • Correctly securing, installing, and configuring the underlying operating system • Correctly securing, installing, and configuring mail server software • Securing and filtering email content • Updating and patching software must follow the guideline set forth in the Vulnerability Management section of 1400-05D. • Remove or disable unneeded services and applications on email servers. • Configure user authentication for email systems. • Review and analyze audit log at least weekly. • Performing periodic security testing

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000298

Electronic Messaging and Email Responsibilities

• Perform regular backups as required by the system security plan.
• Protect email systems against malicious code.
• Deploy the following network protection mechanisms:
  o Firewalls
  o Routers
  o Switches
  o Intrusion detection systems.
ISSOs
• Schedule semiannual/quarterly appointments with the SOC or IV&V team to scan the email system with a vulnerability assessment tool.
• Ensure that email system security controls are in place and functioning as intended.
• Ensure that email system security controls provide the security features outlined in this document and the system security plan.
• Ensure a tested IT Contingency Plan is in place.

Securing a mail server is a two-step process. The first step is to secure the underlying operating system. Many security issues can be avoided if the operating systems are configured appropriately. The second step is to configure the email application. Administrators must configure their servers to apply the organization's security policy. Securing a mail server includes the following steps:

- Apply patches as they become available after first testing them in a lab environment
- Remove or disable unneeded services and applications
- Configure user authentication
- Scan the operating system with a vulnerability assessment tool.

Components must consider encryption technologies to protect their email systems. Most standard mail protocols default to unencrypted user authentication and send email data in the clear. Sending data in the clear allows a hacker to compromise a user's account and/or intercept emails.

When a PKI system is properly integrated into the client email facility, it is possible to "hash" a message to determine that it has not been altered or otherwise tampered with. It is also possible to encrypt sensitive data in an email using the employee's digital certificate encryption key and digitally sign an email using the digital certificate's signing key. This establishes integrity, confidentiality, and non-repudiation with regard to sensitive information.

The infrastructure that supports the network plays a vital role in the security of the email system. The network infrastructure is the first line of defense between the Internet and a mail server. However, network design alone cannot protect a mail server. The following steps need to be accomplished on a regular recurring basis:

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000299

- Review and analyze log files
- Back up data daily (or in accordance with the system security plan)
- Protect against malicious code (e.g., viruses, worms, Trojan horses)
- Have a recovery plan in the event of a disaster
- Test and apply patches in a timely manner
- Scan the system for vulnerabilities with a vulnerability-scanning tool.

NIST SP 800-45, *Guidelines on Electronic Mail Security*, and NIST SP 800-49, *Federal S/MIME V3 Client Profile*, have valuable information detailing how to secure email. NIST SP 800-45 gives detailed technical guidance for Microsoft Exchange, Linux, and UNIX mail services and contains general guidance on how to secure mail servers.

5.4.8 Personal Email Accounts

As discussing sensitive information on a cell phone in a crowd can expose the information to untrusted ears, sending sensitive email to a personal account can expose that information to a large number of unauthorized individuals.

Policy ID	CBP Policy Statements	Relevant Controls
5.4.8.a	The use of Internet webmail (Gmail, Yahoo, AOL, etc.) or other personal email accounts is not authorized over DHS furnished equipment or network connections.	---
5.4.8.b	When sending email to an address outside of the .gov or .mil domain, users shall ensure that any sensitive information, particularly privacy data, is attached as an encrypted file.	---
5.4.8.c	I will not provide personal or official DHS information solicited by e-mail.	---

Personal email responsibilities are provided below.

Electronic Messaging and Personal Email Responsibilities
CISO • Establishes policy concerning the transmittal of sensitive CBP information. • Evaluates the risks associated with the transmittal of sensitive information. • Evaluate the risks and recommend solutions to counter the risk of transmitting sensitive DHS information. **System Owners and Managers/Supervisors** • Enforce CBP policy prohibiting the transmittal of sensitive CBP information to personal email accounts. **System Administrators**

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000300

Electronic Messaging and Personal Email Responsibilities
• Ensure technical controls are in place and properly functioning to prohibit and/or deter the transmission of sensitive CBP information to personal email accounts. **ISSOs** • Ensure technical controls are in place and properly functioning to prohibit and/or deter the transmission of sensitive CBP information to personal email accounts. • Monitor compliance. **Users** • Comply with CBP policy prohibiting the transmission of sensitive CBP information to personal email accounts.

Sending email to a personal account has the following vulnerabilities:

1. Because personally owned computers are not authorized for use in CBP, they are not likely to have the appropriate encryption software installed, resulting in information sent in "clear text."

2. Because the route the email travels cannot be predicted, untrusted persons at ISP sites may read the sensitive information.

3. Because the email travels over unprotected communication links, it can be "sniffed" in transit and read by an unauthorized user.

4. Web browsers are often used to access private email accounts. Such access is inherently not secure.

5. Many worms and viruses (which could exist on the employee's personal computer) propagate themselves by mailing copies of existing emails or other text on a victim's computer to unknown individuals.

6. Instant Messaging and ICQ channels are a frequent source of viruses and mechanisms for attack of personal computers.

7. So-called "spy ware" programs transmit information from personal computers to sites unknown to the computer's owner. Many programs (both freeware and commercial) install these programs to harvest marketing information and other information from a user's computer.

Any unauthorized person who acquires sensitive information in this manner could post it on the Internet, deliver it to a news bureau, or forward it to individuals who could use the information to compromise national security.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000301

5.4.9 Testing and Vulnerability Management

The DHS and CBP SOCs take a proactive approach to vulnerability management including detecting vulnerabilities through testing, reporting through Information Security Vulnerability Management (ISVM) messages, and conducting Vulnerability Assessments (VA).

Vulnerability management is a combination of detection, assessment, and mitigation of weaknesses within a system. Vulnerabilities may be identified from a number of sources, including reviews of previous risk assessments, audit reports, vulnerability lists, security advisories, and system security testing such as automated vulnerability scanning or security tests and evaluations (ST&E).

A core element of vulnerability management is mitigating the discovered vulnerabilities, based on a risk management strategy. This strategy accounts for vulnerability severity, threats, and assets at risk. Risk calculation allows Components to prioritize their remediation actions, in accordance with their specific situation and risk management strategy. Remediation actions are captured in each Component's patch management policy.

The DHS Information Security Vulnerability Management Program (ISVM), managed through the DHS CSIRC, provides the CISO and security and operational personnel (e.g., CAs, ISSOs, LAN Administrators, System Administrators, Field Technology Officers) with bulletins, alerts, and technical advisories related to emerging vulnerabilities and threats. The ISVM is modeled on the Department of Defense's Information Assurance Vulnerability Assessment (IAVA) program but generally does not prescribe the mitigation options nor centrally manage software patching. The following ISVM tools are available:

- CBP Top 20 Critical Vulnerabilities List
- DHS Vulnerability Assessment Team (VAT) – Red Team for Components without internal capabilities and for independent verification as necessary
- DHS Vulnerability Assessment Request Form (see Attachment O)

The DHS Vulnerability Management Program is described in Attachment O. Testing and vulnerability assessments can be accomplished by a combination of scanning and manual techniques. Plans call for DHS to field an automated C&A tool with a built-in vulnerability assessment capability. In addition, Plans of Action and Milestones (POA&Ms) will be prepared and used in conducting periodic vulnerability testing and assessments of information security controls and techniques.

Policy ID	CBP Policy Statements	Relevant Controls
5.4.9.a	CBP shall conduct vulnerability assessments and/or testing to identify security vulnerabilities on IT systems containing sensitive information annually or whenever significant changes are made to the IT systems. This shall include scanning for unauthorized wireless devices. Evidence that annual assessments have been conducted shall be included with Security Assessment Reports (SAR) and with annual security control assessments.	---
5.4.9.b	The CISO and the SOC shall approve and manage all activities relating to requests for Vulnerability Assessment Team (VAT) assistance in support of	---

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000302

Policy ID	CBP Policy Statements	Relevant Controls
	incidents, internal and external assessments, and on-going SLC support.	
5.4.9.c	Anyone within CBP may request to be added to the ISVM distribution list. Those wishing to be added must provide a DHS email address and obtain management approval. ISVMs contain sensitive, "For Official Use Only," information and must not be forwarded to non-DHS email accounts. • Although ISVM messages can be sent to anyone, only the CISO or their designated representatives may acknowledge receipt of messages, report compliance with requirements or notify the granting of waivers.	SI-5
5.4.9.d	CBP shall report compliance with the ISVM message within the specified timeframe. CBP must submit documentation of a waiver request via the DHS SOC Online Portal (https://soconline.dhs.gov) if unable to meet the designated compliance timeframe.	SI-5
5.4.9.e	CISO shall ensure coordination among the DHS SOC, CBP SOC, and the Information Security Vulnerability Management (ISVM) Program when vulnerability assessment responsibilities encompass more than just CBP.	RA-3
5.4.9.f	The DHS and CBP SOCs shall be notified before any ISVM scans are run on a CBP Network.	RA-5
5.4.9.g	System Owners shall report the security alert and advisory status of the information system to the CISO, AO, and DHS CISO upon request and on a periodic basis.	SI-5

Testing and vulnerability assessment responsibilities are provided below.

Testing and Vulnerability Assessment Responsibilities
CISO and CBP SOC • Develop and follow POA&M procedures for implementing vulnerability assessments on sensitive systems. • Approve and manage all activities relating to requests for Vulnerability Assessment Team (VAT) assistance in support of incidents, internal and external assessments, and on-going SLC support. • Ensure coordination among the DHS SOC, CBP SOC/CSIRC, and the Information Security Vulnerability Management (ISVM) Program when vulnerability assessments cross multiple Component responsibilities. **ISSOs and IT Support Personnel** • Support SOC/CSIRC vulnerability assessments.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000303

Vulnerability Scanning

Vulnerability scanning is the process of identifying known vulnerabilities of computing systems operating on a network for the purpose of determining if and where a system can be compromised. Vulnerability scanning often employs software that contains a database of known flaws, tests systems for the occurrence of these flaws, and generates a report of the findings that the organization can use to tighten the network's security.

Vulnerability scanning typically refers to system audits on internal networks that are not connected to the Internet, as well as systems that are visible on the Internet, in order to assess the threat of rogue software and malicious or incompetent employees in an enterprise. Its purpose is to identify weaknesses in a system (or system security procedures, hardware design, internal controls, etc.) that could be exploited to gain unauthorized access to sensitive information or affect system availability or data integrity. Internal staff members who are part of the security staff performing this type of testing should have clearance levels commensurate with that of the system. These people shall intimately know the weaknesses of CBP IT systems and networks.

Expanded Vulnerability Scanning

The type of security testing performed by general-purpose vulnerability scanning tools may uncover weaknesses in the underlying components of systems that host CBP intranet or Internet web sites. A special class of scanning tools explores weaknesses in components of web systems for vulnerabilities related to the content and functionality of such systems. Examples of such vulnerabilities include the ability of unauthorized persons to examine or alter files, to establish cross-site scripting (which redirects users of a web site to another web site), or to directly access a database from which data is displayed on the web site.

A similar class of vulnerability tools exists for databases that have the capability of exploring inherent and design-induced weaknesses. Common vulnerabilities include default passwords that have not been removed, authentication bypass errors, and the ability to alter data without authentication.

Thorough vulnerability scanning expands upon the "canned" tools to include manual testing of potentially vulnerable systems and network components. For example, firewalls may provide barriers to standard discovery techniques. However, specialized scanning tools can utilize normally open ports (e.g., 80 for HTTP) and configurable timing parameters to discover internal systems in such a manner that neither a firewall nor a Network Intrusion Detection System (NIDS) can detect the scan. Such vulnerability assessments should also include both "war dialing" to find unauthorized dial-in modems, and "war driving" to detect unauthorized or misconfigured wireless network equipment.

Gap Analysis

One type of assessment is referred to as a "gap analysis". Such testing measures the deviations in installed systems and networks from the organization's stated policies and procedures. This type of analysis requires that the testers have access to internal information such as security policy and procedure documents and specific networks or systems that should be assessed. Internal staff or, preferably, third parties can perform gap analyses.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000304

Penetration Testing

Penetration testing is a different process. Third-party personnel who have no knowledge of the security policies or the internal structure of the network typically perform penetration tests. Penetration testing assesses weaknesses of a computer facility or network to attack by amateur or professional "hackers." A thorough penetration test will include social engineering, dumpster diving, identification of networks through public sources (e.g., WhoIs and RwhoIs searches of the Regional Internet Registries) as well as manual techniques for finding weak points in an organization's perimeter. Once internal systems have been identified, a search of the NIST ICAT database can provide a laundry list of possible vulnerabilities in the hardware, operating systems, middleware, or applications discovered.

5.4.9.1 Scope of Vulnerability Assessments

All equipment attached to the CBP Network Infrastructure is subject to security vulnerability scanning. In today's changing environment, vulnerable and/or unprotected systems can easily be overlooked. Systems that are not properly managed can become a potential threat to the health of the CBP infrastructure.

Proactive security scanning allows for a meaningful assessment of system security against known risks and provides a roadmap of effective countermeasures for improving security. Proactive scanning can also identify authorized and unauthorized devices on the internal network (e.g., unauthorized wireless access points, modems or high-speed [DSL] links installed by employees for their personal convenience without adequate security controls). Proactive scanning can lead to faster detection of vulnerabilities and can reduce damage to breached systems.

Reactive security scanning allows for threat quantification and assessment, accelerated damage control, and an assessment of systems against reasonable control measures during the repair/ rebuilding process.

Any system identified in conjunction with a security incident shall be subject to a comprehensive security scan. Random network scans shall not be advertised. Network and host scans shall be conducted by authorized DHS and/or CBP personnel using pre-designated scanning machines in order to be easily recognizable as benign activity in system log files. Because vulnerability scanning can be resource intensive, routine scanning is to be done during periods of low network activity when feasible.

5.5 Scanning and Monitoring Policy

CBP-owned systems must be protected from all intrusions. Intrusions range from potentially damaging exploitation by adversaries to simple intrusion by inquisitive hackers. Occasionally, when the incident requires further action, monitoring of some type may be performed to both protect the critical system and to identify the perpetrator attempting to violate the security of the system. Any monitoring activities will be accomplished under the authority of the Office of Internal Affairs (IA). This section defines the policy on approved and prohibited actions involved with monitoring. It applies to all computer systems and networks within CBP. No matter which type of monitoring activity is being conducted, all personnel associated with the monitoring activity must be aware of the policies contained in this section.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000305

IMPORTANT NOTICE

Unauthorized target monitoring is a violation of federal law and a subject's rights, and could jeopardize any investigation or prosecution.

1. The CSIRC shall monitor the CBP network for security events using vulnerability scanners and Intrusion Detection System (IDS) technology.

2. A log-on warning banner is required on all networked and standalone CBP systems, regardless of the user. The warning banner must inform the user that he/she is subject to monitoring simply by using a government-owned system and as such there is no expectation of privacy. If the user does not consent to being monitored, he/she must be given the opportunity to exit before the log-on is completed.

3. Monitoring of a particular individual or group is prohibited without prior permission from the local IA Officer. Official procedures to initiate target monitoring are maintained and conducted by the Office of Professional Responsibility. Unless permission has been granted by IA to monitor a particular person, any monitoring must be broad-based, capturing all information on the monitored network, not just filtered information.

4. The requesting organization, usually IA, Chief Counsel, Labor and Employee Relations, or the Inspector General, will submit a written request for permission to conduct target monitoring. The SA must sign the request. It will then be sent through the local organization's Director and the local IA Officer, to the CISO. Approval must be obtained before target monitoring can begin. If there is an immediate need to begin monitoring because of acute mission requirements, the ISSO/SA shall honor the request and obtain the written permission after the fact. However, this is considered an exception to the policy; and the written request must be submitted as soon as possible. Please note, exceptions should only be granted when the requestor is one of the four organizations listed above, and the local IA Officer approves the action. All requests will include the following information:

    a. The date and time of the proposed monitoring

    b. Description of the planned activity including the identification of the network tool to be used

    c. A detailed explanation of the reason for the monitoring

    d. The anticipated results

    e. Signature of the SA

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000306

5. Target monitoring should always be conducted for the minimum amount of time. The System/Network/LAN Administrator, Field Technology Officer or the ISSO must send a notification message to the CISO informing him/her of the monitoring activity. Any output provided by the monitoring shall be provided to the individual who requested the monitoring. The following information will be recorded by the SA and provided to the ISSO:

    a. When monitoring started and stopped

    b. A description of the activity with the identification of the monitoring tool used

    c. A detailed explanation of the reason for the monitoring

    d. Results of the monitoring

    e. Signature of the SA and ISSO

6. The SOC may conduct scheduled or unscheduled vulnerability assessments of any CBP asset at the direction of the CISO. The SOC is not required to obtain prior approval or notification for this type of vulnerability assessment.

7. The DHS-SOC shall be notified before any ISVM scans are run.

5.5.1 Authorized/Approved Monitoring

Actions to be taken when monitoring has been approved/authorized by the CISO:

Care must be taken NOT to destroy evidence, to implicate the innocent, or cause a subject to become aware of a planned monitoring activity. The ISSO (if available) and SA should make every effort to ensure that the following actions are performed in an orderly fashion.

1. Although backing up files may alter the associated properties (i.e., date last accessed), backup whatever files are deemed necessary in order to secure evidence.
2. Formally report the monitoring activity by sending an Incident Report in accordance with the Computer Security Incident Response Center (CSIRC) guidelines.
3. Initiate action to obtain permission from the CISO to implement monitoring procedures. The CISO is responsible for informing the AO.
4. Begin monitoring only after approval has been granted by the CISO.

Each person involved should be instructed to keep notes documenting the following items:

1. Names of people who have been briefed on the incident.
2. Names of people who may know about the incident without having been briefed.
3. A chronology of events from your personal knowledge.
4. Records of any correspondence generated on the incident.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000307

5. Using the certification documentation and the accreditation package, review the functionality and structure of the system and document its location(s), hardware configuration, software applications, network connectivity, numbers of users, etc.
6. Keep a file of all correspondence relating to the incident.
7. Continually perform periodic backups as long as the activity continues.
8. Preserve the backups under lock and key as potential evidence.

5.5.1.1 Review System-Specific Features

The investigators will want full documentation on many aspects of the system being violated during the incident. The following questions are samples of those that may be used in the investigation. Not all of them apply to each incident, but all need to be reviewed to determine applicability. The ISSO and SA will make every effort to answer the following questions and document the information without arousing suspicion:

1. What event(s) triggered the suspicion of improprieties?
2. Does the system have a warning banner? Is the banner displayed before the first keystroke? Capture a copy of banner that was probably displayed.
3. Are any local operating procedures being violated?
4. Is there a copy of the security Certification and Accreditation (C&A) Package available?
5. What is the function of the system?
6. What are the known system vulnerabilities?
7. Where the hardware is physically located?
8. What is the sensitivity level of the data processed on the system?
9. What organization/activity is supported by the system?
10. What internal and external connections are authorized to the system?
11. Are any of the connections supported by modems?
12. Is dial-in access authorized? If so, is it encrypted?
13. What are the baud rates of the modems used on the system?
14. What security software, if any, is used on the system?
15. What file transfer protocols are used on the system?
16. Are audit trails running normally; and have they been reviewed regularly?
17. Have vendor-supplied passwords been eliminated?
18. Are passwords machine-generated or selected by the user?
19. Have system passwords or the password file been stolen? Document the name of the password file, whether it was encrypted, and its location within the system.
20. How many failed log-on attempts were made in the last thirty days?

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000308

21. Who performs maintenance on the system; and do maintenance personnel have access to the system?

5.5.1.2 Review Actions of the Subject

The investigators will want information on the suspect. The ISSO and SA will make every effort to answer the following sample questions. Not all of the questions apply to every investigation. Review each question to determine its applicability. Document information on the following items without arousing suspicion:

1. Is the incident a repetitive act?
2. Is there a repetitive pattern to the time of the activity?
3. Is the subject an outsider? Is it possible to identify the person's nationality and affiliation?
4. If an insider, is the subject civil service, government contractor, etc?
5. What is the subject's level of competency?
6. What is the subject's education level?
7. What is the subject's experience level?
8. What are the subject's responsibilities?
9. Does the subject have root-access privileges to the system?
10. Is there a current access control document signed by the subject?
11. What is the motive of the subject: amusement, competition, cover-up, financial or personal gain, protest, revenge, superiority, academic challenge, free-flow of information, or other?
12. What computer protection schemes are used by the subject: automated batch files, encrypted files, RAM disks, modified operating systems, trap doors in operating systems, archived or zipped files, bulk erasure, hidden files or directories, text files renamed as ".COM" or ".EXE" files, split files, files stashed on other computers, files stored in file slack areas of existing files, or any others?
13. What actions were taken by the subject to avoid identification: looping, stolen accounts, false accounts, deactivating audit trails, social engineering, manipulated programs, operating systems, or systems functions?
14. Did the subject download any of his/her own software to assist in his/her activities?

5.5.2 Sniffer Devices

A sniffer is a software program or hardware device, also known as a network or protocol analyzer, that intercepts routed data and can be used to examine each packet in search of specified information. Sniffers can be used for legitimate network management functions such as monitoring traffic for intrusion events and analyzing network problems. They can also be used to steal information from a network such as passwords transmitted in clear text. Unauthorized sniffers can be extremely dangerous to a network's security because they are virtually impossible to detect and can be inserted almost anywhere.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000309

Any employee wishing to use sniffers must receive approval from the CISO or the AO. Currently, the CISO has limited the usage of sniffers within the CBP enterprise to the Computer Security Incident Response Center (CSIRC) and the CBP Network Engineering Branch. Please consult the EDME Enterprise Architecture (EA) team to obtain a list of CBP approved sniffers.

5.6 Peer-to-Peer Technology

Peer-to-peer (P2P) technology is a phrase coined to apply to individual PCs acting as servers to other individual PCs. Made popular by the music file-swapping service Napster, peer-to-peer technology allows users to share files with each other through a network of computers that use the same peer-to-peer client software. Each computer on the network has the ability to act as a both a server, by hosting files for others to download, and a client by searching other computers on the network for files the client wants to access.

P2P applications circumvent most enterprise security systems. This provides malicious users easy access to a system, allowing them to install malware on participating systems, identify IP addresses and user names of internal machines, steal classified data, launch a denial of service attack (e.g., through bandwidth consumption, filling hard disks), or gain control of network resources.

P2P technology introduces a significant risk to Government data and exposes Government agencies to legal liability for copyright infringement. Use of this technology can also decrease productivity and use large amounts of bandwidth.

P2P computing or "file sharing" allows individual Internet users to connect to one another remotely with the intent of trading or sharing files. The use of external P2P software on CBP computers or on any computer or information system that might be connected to CBP networks is prohibited. However, if the P2P connection is to a computer that is owned and managed by CBP, then the connection is permitted.

Although there are many appropriate uses of P2P computing, in its popular, more-common forms (e.g., Napster, Kazaa, and Grokster) studies have proven that a significant portion of shared files within P2P connections contain pornography and illegally obtained, copyrighted, music files. Further downloading P2P files can cause the CBP network to become vulnerable to a virus attack caused by downloading an infected file.

Instant Messaging is another common form of P2P networking. Use of commercial Instant Messaging applications such as AOL, MSN, and Yahoo is prohibited on CBP systems.

Policy ID	CBP Policy Statement	Relevant Controls
5.6.a	Software enabling publicly accessible peer-to-peer file sharing technology is not authorized on any DHS information system.	CM-7, SA-6

Peer-to-peer responsibilities are provided below.

Peer-to-Peer Technology Responsibilities
CISO

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000310

Peer-to-Peer Technology Responsibilities
• Establishes CBP policy regarding the unauthorized use of IT technology and software. • Ensure that controls, including awareness training, are in place to minimize or prevent unauthorized use of unauthorized IT technology and software. **Supervisors** • Enforce unauthorized use policies including remedial training and other sanctions. • Promptly report unauthorized use of IT technology in accordance with CBP Computer Security Incident reporting policy (Attachment F). **ISSOs, System/Network/LAN Administrators/Field Technology Officers** • Ensure that controls are in place including the use of monitoring and auditing to detect unauthorized use or installation of software. • Promptly report unauthorized use of IT technology in accordance with CBP Computer Security Incident reporting policy (Attachment F). **Users** • Be aware of the prohibition against the use of unauthorized IT technology and software. • Adhere to the unauthorized use policies established in this section and in other references provided by CBP security officials. • Promptly report unauthorized use of IT technology in accordance with CBP Computer Security Incident reporting policy (Attachment F). • Be aware of and understand the ramifications of penalties involving infractions of the rules regarding inappropriate use of Government resources.

For additional information on inappropriate use of CBP resources, see Section 3.15, Information Technology Security Policy Violation and Disciplinary Action; Section 4.8.4, Personally Owned Equipment and Software; Section 4.8.9, Personal Use of Government Office Equipment and DHS Information Technology Systems/Computers; and Section 4.9.6, Security Incidents and Incident Response and Reporting.

5.7 Cryptography

Cryptography provides a means for two or more parties to communicate securely. Cryptography is a branch of mathematics, which deals with the transformation of ordinary text (plain text) into coded form (cipher text) by encryption and the transformation of cipher text into plaintext by decryption. Cryptography relies on two basic components: an algorithm (e.g., Advanced Encryption Standard [AES]) and a key. The algorithm is the mathematical function used for encryption or decryption, and the key is the parameter used in the transformation.

There are two basic types of cryptography: secret key systems (also called symmetric systems) and public key systems (also called asymmetric systems). In secret key systems, the same key is used for both encryption and decryption; that is, all parties participating in the communication share a single key. In public key systems, there are two keys: a public key and a private key. The public key used for encryption is different from the private key used for decryption. The

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000311

two keys are mathematically related, but the private key cannot be determined from the public key and the public key cannot be determined from the private key.

Refer to NIST SP 800-21, *Guideline for Implementing Cryptography in the Federal Government*, for more in-depth information on cryptography.

A digital signature is an electronic analogue of a written signature in that the digital signature can be used in proving to the recipient or a third party that the originator did in fact sign the message. Digital signatures may also be generated for stored data and programs so that the integrity of the data and programs may be verified at any later time. Signature generation makes use of a private key to generate a digital signature. Signature verification makes use of a public key that corresponds to, but is not the same as, the private key. The security of a digital signature system is dependent on maintaining the secrecy of users' private keys.

5.7.1 Encryption

Encryption is the process of changing plaintext into ciphertext for the purpose of security or privacy. It is a reliable and achievable way to help ensure confidentiality for sensitive data by converting plain text information into an unreadable form using approved algorithms. CBP employs encryption technologies to implement security requirements of certain data and in use of various devices, for example: passwords, symmetric and asymmetric keys, certain activities performed by system administrators and maintenance personnel, data packets transmitted on a wireless network, and data stored on laptop devices.

Encryption is the process of changing plaintext into ciphertext for the purpose of security or privacy. System specific encryption is addressed within the C&A documentation using CBP-approved encryption methodologies.

Policy ID	CBP Policy Statements	Relevant Controls
5.7.1.a	Identify all IT systems transmitting sensitive information and determine if the system requires protection via encryption based on a risk assessment. If encryption is required, the following methods are acceptable for encrypting sensitive information: • Products using Advanced Encryption Standard (AES) algorithms that have been validated under FIPS 140-2 (Note: The use of triple DES [3DES] and FIPS 140-1 is no longer permitted. A waiver is required for systems where AES cannot currently be used). • NSA Type 2 or Type 1 encryption.	IA-7, SC-13
5.7.1.b	All Major Applications (MAs) or General Support Systems (GSSs) with sensitive applications under their authority shall develop encryption plans for those information systems.	IA-7, SC-13
5.7.1.c	CBP shall use only cryptographic modules that are FIPS 197 (AES-256) compliant and have received FIPS 140-2 validation.	IA-7, SC-13
5.7.1.d	Application-level encryption or an encrypted virtual private network link must be used for any sensitive data that is transmitted over the Internet or other	IA-7, SC-13

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000312

Policy ID	CBP Policy Statements	Relevant Controls
	public network	

CBP Encryption responsibilities are provided below:

CBP Encryption Responsibilities
AO • Ensure sensitive or classified encryption applications under their authority have developed encryption plans for IT systems prior to accreditation. • Ensure personnel implementing encryption requirements are technically qualified and adequately trained in encryption technologies and specific methodologies employed. **CISO** • Ensure CBP encryption policy is implemented and enforced. • Advise project managers on the implementation of CBP encryption standards. **ISSOs** • Ensure CBP encryption methodology is properly implemented and configured on all required CBP IT systems. • Assist system owners in identifying sensitive CBP data that requires encryption.

Encryption is a reliable and achievable way to help ensure confidentiality for sensitive data. It involves converting plain text information into an unreadable form using approved algorithms. DHS employs encryption technologies to implement requirements. These requirements include encryption of passwords, symmetric and asymmetric keys, certain activities performed by system administrators and maintenance personnel, data packets transmitted on a wireless network, and data stored on laptop devices.

Components shall ensure that encryption is addressed in the C&A documentation using DHS-approved encryption methodologies.

5.7.2 Public Key Infrastructure

In the past, communications involving sensitive data could not be conducted securely through purely electronic means. With the advent of Public Key Infrastructure (PKI), securing the exchange of sensitive messages while providing limited access to public information networks became available. DHS implemented a PKI program that consists of products and services to provide standard public key certificates for use throughout the organization. DHS mandated the use of PKI throughout its Components. The E-Gov Act also requires such use of PKI to improve network authentication.

A public key infrastructure (PKI) is an architecture that provides the means to bind public keys to their owners' private keys and helps in the distribution of reliable credentials in large heterogeneous networks. Public keys are bound to their owners by public key certificates. These certificates, which contain information such as the owner's name and the associated public

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000313

key, are issued by a reliable certification authority (CA). Reliable identification of individuals is an inherently Governmental activity. In order to establish and maintain the trust required to support DHS missions, the root certificate must be controlled by the DHS. DHS implemented a PKI program that consists of products and services to provide standard public key certificates for use throughout the organization. DHS mandated the use of PKI throughout its Components. The E-Gov Act also requires such use of PKI to improve network authentication. The DHS PKI shall be governed by a DHS X.509 Certificate Policy (DHS CP).

Any DHS Component that implements a PKI or CA for a PKI must ensure that its CA is subordinate to the DHS Root CA. The use of self-signed certificates has minimal security value and violates Executive Office Directives. The use of any non-DHS service provider for CA or PKI support is inconsistent with DHS Mission requirements and must be approved by the CISO.

PKI provides the means for an organization to meet four critical security objectives:

1. Authentication
2. Non-Repudiation
3. Data Integrity
4. Confidentiality

PKI usually consists of:

1. A Certificate Authority that issues and verifies a digital certificate. A certificate includes the public key or information about the public key.
2. A Registration Authority (RA) that acts as the verifier for the Certificate Authority before a digital certificate is issued to a requestor.
3. One or more directories where the public key portion of the certificate resides.
4. A certificate management system.

PKI systems enable users of an unsecured network to securely and privately exchange information using private and public key pairs. In public key cryptography, a public key and a private key are created simultaneously using the same algorithm. Public keys are bound to their owners by public key certificates. These certificates, which contain information such as the owner's name and the associated public key, are issued by a reliable certification authority (CA). The Certificate Authority gives the private key only to the requesting party and makes the public key available (as part of a digital certificate) in a directory that all parties can access. The authorized owner uses a private key to decrypt text that has been encrypted with the public key by someone else. PKI also provides a digital certificate that can be used to electronically 'sign' documents.

All CBP departments, employees, and contractors are considered 'Relying Parties' who:

1. Check each digital certificate for its validity or revocation prior to issuance.
2. Verify the receipt of the digital signature of a digitally signed message.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000314

3. Verify the digital signature of the Certificate Authority who issued the certificate.

DHS Certification Practices Statements (CPS) and the corresponding DHS Certificate Policy mandate guidelines on the intended use of PKI certificates. All CBP employees, and contractors are required to follow the enrollment and registration procedures set forth in these DHS PKI policy documents.

Employees and contractors obtain sponsorship for certificates through their respective managers. PKI enrollment procedures for CBP require completion of the following forms before an individual is issued a digital certificate:

1. Pre-Enrollment Subscriber Form
2. Human Subscriber Agreement Form
3. Local Registration Authority (LRA) Nomination Form
4. Sponsor Form
5. In person identity proofing (with two forms of identification)
6. On-line Certificate Request application and key pair generation

The CISO nominates trusted individuals for trusted roles before subscriber registration can begin. Local Registration Authorities (LRAs) and Trusted Agents (TAs) obtain smartcards and smartcard readers to implement this technology. Smartcards are able to store and process information. Users are issued a smartcard that stores data such as the PKI private key, personal ID with photo, building access card, and parking permit.

Policy ID	CBP Policy Statements	Relevant Controls
5.7.2.a	PKI policy oversight shall be provided at the Department level by a PKI Policy Authority (PKI PA). The DHS CISO shall be the PKI PA.	SC-17
5.7.2.b	PKI operational oversight shall be provided at the Department level by a PKI Operational Authority (PKI OA) appointed by the PKI PA.	SC-17
5.7.2.c	The DHS PKI shall be governed by a DHS X.509 Certificate Policy (DHS CP). The DHS CP shall be approved by the PKI PA.	SC-17
5.7.2.d	The DHS CP must comply with the U.S. Federal PKI Certificate Policy for the Federal Bridge CA, at the high, medium, and basic assurance levels.	SC-17
5.7.2.e	DHS shall have a single High Assurance Root CA. All additional CAs within DHS must be subordinate to the DHS Root CA. The requirements and process for becoming a subordinate CA to the DHS Root CA shall be specified in the DHS CP.	SC-17
5.7.2.f	The DHS CA shall have a trust path resolving to the Federal Bridge CA and the PKI SSP Root CA at the high, medium, and basic assurance levels.	SC-17
5.7.2.g	Every DHS CA shall operate under an X.509 Certificate Practices Statement (CPS). The CPS for each CA must comply with the DHS CP. The DHS PKI	SC-17

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000315

Policy ID	CBP Policy Statements	Relevant Controls
	PA must approve each CPS.	
5.7.2.h	All DHS CAs shall undergo a compliance audit on a regular basis as required by CP. The DHS PKI PA shall specify a DHS PKI Auditor to review compliance audits.	SC-17
5.7.2.i	All operational PKI facilities shall be established in accordance with the requirements commensurate with the CA's assurance level as well as its intended use. Location/protection of the authority shall be determined by its level of assurance. Measures to ensure continuity of operations of the certificate authority shall be taken that are at least equal to the measures of the system being supported.	SC-17
5.7.2.j	A DHS PKI archive facility shall be established to store PKI records, as required by the CP and CPSs.	SC-17
5.7.2.k	Certificates that are issued by test, pilot, third party, or other CAs in DHS and that are not established as a subordinate CA to the DHS Root CA shall not be used to protect sensitive CBP data, or to authenticate to CBP operational systems containing sensitive data.	SC-13
5.7.2.l	PKI will consist of: • A Certificate Authority that issues and verifies a digital certificate. A certificate includes the public key or information about the public key. • A Registration Authority (RA) that acts as the verifier for the Certificate Authority before a digital certificate is issued to a requestor. • One or more directories where the public key portion of the certificate resides. • A certificate management system	SC-13
5.7.2.m	PKI enrollment procedures for CBP require completion of the following forms before an individual is issued a digital certificate: • Pre-Enrollment Subscriber Form • Human Subscriber Agreement Form • Local Registration Authority (LRA) Nomination Form • Sponsor Form • In person identity proofing (with two forms of identification) • On-line Certificate Request application and key pair generation	SC-17
5.7.2.n	The DHS PKI PA shall ensure that the CPS for each CA complies with the DHS CP prior to approval.	SC-17
5.7.2.o	The PKI OA shall ensure that every DHS CA operates under its approved CPS.	SC-17

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000316

PKI responsibilities are provided below.

Public Key Infrastructure Responsibilities
DHS AOs • Ensure DHS encryption policy is addressed in the security plans for IT systems that process sensitive information.
DHS CISO • Provides PKI oversight at the Department level. • Serves as the DHS PKI Policy Authority. • Appoints a DHS PKI Operational Authority. • Creates and maintains a DHS CP that complies with the U.S. Federal CP for the Federal Bridge CA. • Establishes and maintains the DHS PKI High Assurance Root Certificate Authority (CA). • Ensures that all DHS CAs are subordinate to the DHS Root CA. • Specifies the requirements and process for becoming a subordinate CA. • Authorizes subordinate CAs. • Ensures the DHS Root CA cross certifies with the Federal Bridge CA at the High, Medium and Basic Assurance levels. • Ensures that all DHS CAs operate under an approved Certification Practices Statement (CPS) that complies with the DHS CP. • Approves the Certification Practices Statements for all DHS CAs. • Ensures that all DHS CAs undergo a compliance audit at least annually, and specifies a DHS PKI Auditor to perform the compliance audits. • Specifies the DHS PKI Auditor to conduct the compliance audits. • Ensures that appropriate facilities are available for hosting DHS certificate authorities as appropriate for their level of assurance and associated mission. Ensures that appropriate continuity planning is established for all infrastructures that distributes, houses, or stores public keys. • Ensures that a DHS PKI archive facility is established to store PKI records. • Ensures that certificates issued by test, pilot, or other CAs in DHS that are not established as a subordinate CA to the DHS Root CA shall not be used to protect sensitive DHS operational data, or to authenticate to DHS operational systems containing sensitive data.
DHS PKI Operational Authority • Provides oversight of PKI operations at the Department level. • Creates and maintains all PKI CPSs pertaining to the DHS PKI.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000317

Public Key Infrastructure Responsibilities

- Creates and manages DHS PKI Operating Procedures.
- Oversees and reviews management of DHS PKI Operations for each authority certified subordinate to the DHS Root CA. Works with DHS and Component physical security entities and/or local registration authorities to oversee the issuance and management of certificates across the DHS enterprise.
- Ensures that all aspects of DHS PKI services, operations and infrastructure related to certificates issued under the DHS CP are in accordance with the requirements, representations, and warranties of the CP.

DHS Office of Security

- Ensures that PKI registration activities under its purview are performed in compliance with the applicable CPSs.

AO

- Ensure CBP encryption policy is addressed in the security plans for IT systems that process sensitive information.

CISO

- Ensure that PKI registration activities under their purview are performed in compliance with the applicable Certificate Practice Statements (CPSs) as defined in DHS x.509.
- Nominates trusted individuals for trusted roles before subscriber registration can begin

ISSOs

- Ensure adequate security measures are in place to protect access to hardware and software
- Ensure new hardware and software has been approved in accordance with the configuration management plan prior to installation.

System/Network/LAN Administrators/Field Technology Officers

- Ensure CBP cryptographic systems are properly configured and functioning properly.

Local Registration Authorities (LRAs) and TrustedAgents

- Obtain smartcards and smartcard readers to implement this technology. Smartcards store and process information. Users are issued a smartcard that stores data such as the PKI private key, personal ID with photo, building access card, and parking permit.

Relying Parties (All CBP departments, employees, and contractors)

- Check each digital certificate for its validity or revocation prior to issuance.
- Verify the receipt of the digital signature of a digitally signed message.
- Verify the digital signature of the Certificate Authority who issued the certificate.

Users

- Obtain sponsorship for certificates through their respective managers.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000318

Implementation of public key infrastructure (PKI) technology, utilizing data encryption, ensures that cryptographic security goals are met. When used either separately or in conjunction with PKI, a virtual private network (VPN) greatly enhances secure data transmission, especially when encryption techniques are employed.

5.7.3 Public Key/Private Key

The recipient of public key certificates is referred to as a subscriber. A subscriber can be a human (e.g., an employee or contractor), an organization, an application, a code signer (e.g., digitally signs released software to enable users to authenticate its source, legitimacy, and integrity), or a device (e.g., a web server or VPN server). Registrars are trusted PKI officials who administer the process that results in a CA issuing or revoking public key certificates for each subscriber. As part of the PKI registration process, a public key/private key pair is generated in a hardware or software cryptographic module that is under the control of the subscriber. The private key remains under the sole possession of the subscriber. A CA enters the public key into an electronic public key certificate that also identifies the owner of the key, i.e. the subscriber. The trusted CA digitally signs the certificate thereby binding the public key to the to the subscriber, and makes the signed certificate available for use by other subscribers.

A subscriber's public key certificate is used by other subscribers, referred to as relying parties, to obtain the subscriber's public key in a trusted manner. Once obtained, the public key is then used: (1) to encrypt data for that subscriber so that only that subscriber can decrypt it with their private key, or (2) to verify that digitally signed data was signed by that subscriber using their private key, thereby authenticating the identity of the signing subscriber, and the integrity of the signed data.

Policy ID	CBP Policy Statements	Relevant Controls
5.7.3.a	Separate public/private key pairs must be used for encryption and digital signature by human subscribers, organization subscribers, application subscribers, and code-signing subscribers.	SC-12
5.7.3.b	Separate public/private key pairs must be used for encryption and digital signature by device subscribers whenever supported by the protocols native to the type of device.	SC-12
5.7.3.c	A human sponsor shall represent each organization, application, code-signing, and device subscriber when it applies for one or more certificates from a DHS CA.	SC-12
5.7.3.d	A mechanism shall be provided for each DHS CA to enable PKI registrars to determine the eligibility of each proposed human, organization, application, code signer, or device to receive one or more certificates.	SC-12
5.7.3.e	A mechanism shall be provided for each DHS CA to enable PKI registrars to determine the authorized human sponsor for each organization, application, code signer, or device.	SC-12

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000319

Policy ID	CBP Policy Statements	Relevant Controls
5.7.3.f	Human subscribers shall not share private keys and shall be responsible for their security and use. If a human subscriber discloses or shares his or her private key, the subscriber shall be accountable for all transactions signed with the subscriber's private key.	---
5.7.3.g	Sponsors for non-human subscribers (organization, application, code-signing, or device) shall be responsible for the security of and use of the subscriber's private keys. Every sponsor shall read, understand, and sign a "DHS PKI Subscriber Agreement for Sponsors" as a pre-condition for receiving certificates from a DHS CA for the non-human subscriber.	SC-12
5.7.3.h	The only private keys authorized for use by more than one person are those that correspond to a public key for an organization or code-signing subscriber. If more than one person is authorized to use the key, auditable records shall be kept to maintain individual accountability.	SC-12
5.7.3.i	Every human subscriber shall read, understand, and sign a "DHS PKI Subscriber Agreement for Human Users" as a pre-condition for receiving certificates from a DHS CA. These signed agreements shall be maintained by the DHS PKI MA.	SC-17
5.7.3.j	Every sponsor shall read, understand, and sign a "DHS PKI Subscriber Agreement for Sponsors" as a pre-condition for receiving certificates from a DHS CA for the nonhuman subscriber they sponsor.	SC-12

Public key/private key responsibilities are provided below.

Public Key/Private Key Responsibilities
DHS CISO • Ensures that the DHS CP and CPSs enforce the use of separate public/private key pairs for encryption and digital signature by human subscribers, organization subscribers, application subscribers, code-signing subscribers, and also by device subscribers whenever supported by the protocols native to the type of device. • Ensures that the DHS CP and CPSs require that a human sponsor shall represent each organization, application, code-signing, and device subscriber when it applies for one or more certificates from a DHS CA. • Ensures that DHS CPSs require that a mechanism is provided for each DHS CA to enable PKI registrars to determine the eligibility of each proposed human, organization, application, code signer, or device subscriber to receive one or more certificates. • Ensures that DHS CPSs require that a mechanism is provided for each DHS CA to enable PKI registrars to determine the authorized human sponsor for each organization, application, code signer, or device.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000320

Public Key/Private Key Responsibilities
• Ensures that controls are implemented to hold human subscribers accountable for the security of their private key and for all transactions signed with their private key. • Ensures that controls are implemented to hold the sponsor of an organization, application, code signing, or device subscriber responsible for the security of and use of the subscriber's private keys. • Ensures that controls are implemented to maintain individual accountability for each use of a shared organizational or code signing private key. • Ensures that a DHS PKI Subscriber Agreement for Human Users and a DHS PKI Subscriber Agreement for Sponsors are created and maintained, and that DHS CPSs require human subscribers and sponsors to read, understand, and sign them as a pre-condition for receiving certificates. **DHS PKI Operational Authority** • Ensures that the DHS CPSs and operating procedures enforce the use of separate public/private key pairs for encryption and digital signature by human subscribers, organization subscribers, application subscribers, code-signing subscribers, and also by device subscribers whenever supported by the protocols native to the type of device. • Ensures that the DHS CPSs and operating procedures require that a human sponsor shall represent each organization, application, code-signing, and device subscriber when it applies for one or more certificates from a DHS CA. • Verifies that that a mechanism is provided for each DHS CA to enable PKI registrars to determine the eligibility of each proposed human, organization, application, code signer, or device subscriber to receive one or more certificates. • Verifies that a mechanism is provided for each DHS CA to enable PKI registrars to determine the authorized human sponsor for each organization, application, code signer, or device. • Verifies that controls are implemented to hold human subscribers accountable for the security of their private key and for all transactions signed with their private key. • Verifies that controls are implemented to hold the sponsor of an organization, application, code signing, or device subscriber responsible for the security of and use of the subscriber's private keys. • Verifies that controls are implemented to maintain individual accountability for each use of a shared organizational or code signing private key. • Ensures that DHS CPSs and Operating Procedures require human subscribers and sponsors to read, understand, and sign DHS PKI Subscriber Agreements as a pre-condition for receiving certificates. **DHS Office of Security** • Provides a mechanism, as required by the CPS, to enable PKI registrars to determine the eligibility of each proposed human subscriber to receive one or more certificates from the

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000321

Public Key/Private Key Responsibilities

DHS CA.

- Ensures that registrars under their purview require human subscribers and sponsors to read, understand, and sign DHS PKI Subscriber Agreements as a pre-condition for receiving certificates.

CISO

- Provide a mechanism, as required by the CPS, to enable PKI registrars to determine the eligibility of each proposed human subscriber to receive one or more certificates from the DHS CA.
- Provide a mechanism, as required by the CPS, to enable PKI registrars to determine the authorized human sponsor for each organization, application, code signer, or device.
- Implement controls to hold human subscribers accountable for the security of their private key and for all transactions signed with their private key.
- Implement controls to hold the sponsor of an organization, application, code signing, or device subscriber responsible for the security of and use of the subscriber's private keys.
- Implement controls to maintain individual accountability for each use of a shared organizational or code signing private key.
- Ensure that registrars under their purview require human subscribers and sponsors to read, understand, and sign DHS PKI Subscriber Agreements as a pre-condition for receiving certificates.

ISSOs

- Ensure human subscribers are aware of their responsibilities to protect their private keys.
- Ensure sponsors are aware of their responsibilities to protect the private keys of the subscriber they sponsor.
- Maintain auditable records to ensure individual accountability is maintained for each use of an organization or code-signing private key authorized for use by more than one person.

Human Subscribers

- Assume responsibility for the security of their private keys.
- Abide by the DHS PKI Subscriber Agreement for Human Users that they signed, and review it at least annually.

Sponsors

- Assume responsibility for the security of the private keys of the subscribers they sponsor.
- Abide by the DHS PKI Subscriber Agreement for Sponsors that they signed, and review it at least annually.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000322

CBP employees and contractors should have reasonable assurance that, when initiating a secure transaction:

1. The information sender and recipient both will be identified uniquely so that both parties know not only where the information originated but also its destination.
2. The information was not altered deliberately or inadvertently.
3. The sender's identity is inextricably linked to the transmitted information.
4. The information will be protected from unauthorized use.

5.8 Virus Protection

Computer viruses pose an ever-increasing problem for applications, systems, and networks. All DHS organizations must implement appropriate file, protocol, and content filtering activities to protect their modification by computer viruses. Malicious code includes, but is not limited to, viruses, logic bombs, worms, Trojan horses, and similar software-induced problems.

Policy ID	CBP Policy Statements	Relevant Controls
5.8.a	The CISO shall establish and enforce CBP virus protection control policies.	SI-3, SC-5
5.8.b	Introduction of any recorded media into the CBP information technology environment may be a source of malicious code contamination. Scan such media and verify its source before using it in the CBP environment.	SI-3
5.8.c	Only approved virus scanner-detection programs will be used.	SI-3, SI-4
5.8.d	The LAN or System Administrator (SA) shall update virus signature files as soon as possible after each new release is tested.	SI-3
5.8.e	All virus infections must be immediately reported to the CSIRC and notify your supervisor/manager if it is a significant incident. This is critical to prevent further spread of the infection. (See Attachment F for details on incident reporting procedures and definitions of incidents.)	IR-1, IR-4, IR-5, and IR-6
5.8.f	CBP shall use a defense-in-depth strategy. This strategy includes: • Installation of antivirus software at the desktop that is properly configured to check all files, Internet downloads, and email. • Automatic updates to antivirus software and signature files minimally on a weekly schedule at the desktop without end user	RA-2

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000323

Policy ID	CBP Policy Statements	Relevant Controls
	participation. • Installation of security patches to servers and desktops must follow the guideline set forth within the Information Security Vulnerability Management (ISVM) notice published by DHS SOC.	
5.8.g	CBP may implement appropriate file/protocol/content filtering to protect their data and networks in accordance with their Internet usage policy.	AC-20, PL-4

Virus protection responsibilities are provided below.

Virus Protection Responsibilities
CISO • Establish and enforce virus protection control policy. • Provide technical expertise and evaluate the effectiveness of virus protection approaches. • Ensure that vulnerability to viruses and other malicious code is detailed in the risk analysis section of the C&A documentation and that adequate steps to mitigate that risk are taken for each system. **System Owners** • Assess the impacts associated with system downtime caused by viruses and other malicious code and ensure adequate resources are allocated to address continuity of operations. **System/Network/LAN Administrators/Field Technology Officers** • Ensure that all CBP IT systems employ virus protection software. • Ensure that antivirus software is installed on every workstation, network, laptop, and mobile computing device. • Update virus signature files immediately with each new release. • Ensure that virus protection software employs resident scanning. • Ensure that virus scanning occurs automatically during boot-up and installation of new software. • Ensure that all diskettes are scanned for viruses prior to use (including blank disks). • Follow procedures detailed in this manual in the event that a virus is detected. **ISSOs** • Employ virus prevention measures commensurate with the level of risk identified for virus infections in the risk analysis. • Ensure that procedures are implemented to prevent, detect, eradicate, and report computer virus incidents.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000324

Virus Protection Responsibilities
• Ensure that virus incidents are reported in accordance with CSIRC procedures (see Section 4.9).
Users
• Ensure that no files are downloaded or opened from unknown or untrusted sources. All files should be scanned by antivirus software before opening them. Do not open suspicious email. • Notify the System / Network Administrator if antivirus software is not installed on the user workstation. • Never disable antivirus software functions. • Report virus and other malicious code incidents in accordance with procedures described in Section 4.9.6, Security Incidents and Incident Response and Reporting.

5.8.1 What Is a Virus?

A virus is a self-replicating malicious program segment that attaches itself to legitimate applications programs, operating system commands, or other executable system components and spreads from one system to another. It can also be defined as a program or piece of code that is loaded onto a computer without the user's knowledge and runs against the user's wishes. As it spreads, it is said to be *infecting* the system.

A computer virus may only be a line or two of programming code hidden within a program.
It can be benign and limited to sending a greeting to amuse or annoy, or malicious, written specifically to damage other programs.
It can display a message, erase files, subtly alter stored data, or "crash" a hard drive.

5.8.2 Other Types of Malicious Code

Other types of malicious code can be defined according to the following table:

Table 5.8.2: Types of Malicious Code

Worms: Computer worms are malicious programs that copy themselves from system to system, rather than infiltrating legitimate files. For example, a mass-mailing email worm is a worm that sends copies of itself via email. A network worm makes copies of itself throughout a network or through file shares. Worms often contain Trojan horse or "backdoor" programs.
Logic Bombs: A logic bomb can be defined as dormant code, the activation of which is triggered by a predetermined time or event. For example, a logic bomb might start erasing data files when the system clock reaches a certain date or when the application has been loaded X number of times.
Trojan Horses: A Trojan horse is a computer program that is apparently or actually useful but performs another function. A Trojan horse generally provides remote control access to an unauthorized person. A Trojan horse can be used to modify databases, write checks, send email, or destroy files. It could be imbedded by a programmer or downloaded from the

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000325

Internet.

Web Bugs: A web bug is executable code included in an image (as small as one pixel) that can disrupt the operation of a system or acquire and transmit information from a system without the user's knowledge by merely visiting a malicious or compromised web site.

5.8.3 How Viruses and Other Malicious Code Affect Systems

Regardless of the type of malicious code, viruses and other malicious code can pose a significant threat to CBP systems, which can affect the availability, integrity and confidentiality of information and processing resources. *Therefore, it is essential that all systems employ prevention measures commensurate with the level of risk identified in the risk analysis.* What makes viruses and other malicious code different from other problems is that they can spread —from program to program and from system to system—*without direct human intervention*.

Systems that can be accessed by CBP-approved browser configurations should be categorized (trusted, untrusted, etc.). Users are not allowed to deploy Web browsers "out of the box," since the security policies implemented in such tools tend to reflect the vendor's interests and do not necessarily coincide with those of CBP.

5.8.4 Procedures When a Virus Is Detected on a System

If a virus or other malicious code is detected, the LAN/system administrator is responsible for taking appropriate actions to eradicate the problem. Such actions include:

- Running disinfectors available with antivirus software
- Scanning backup diskettes and tapes for viruses prior to restoring system applications and data files
- Checking for re-infection from overlooked disks or other media during the eradication process
- Notifying the ISSO of the security incident via incident reporting procedures described in Section 4.9.

Once the malicious code has been eradicated, the system administrator shall determine the extent of the damage and restore all damaged files or programs to uninfected files and programs. Back-up media should be scanned *prior to restoring* system applications and data files.

Note that occurrences of malicious code constitute a *security incident* that must be reported; reporting procedures are described in Section 4.9.6, Security Incidents and Incident Response and Reporting.

5.9 Product Assurance

Information assurance (IA) involves protecting and defending information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. Information assurance is achieved through the use of IA and IA-enabled products.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000326

Policy ID	CBP Policy Statements	Relevant Controls
5.9.a	Information Assurance (IA) shall be considered a requirement for all systems used to input, process, store, display, or transmit sensitive or national security information. IA shall be achieved through the acquisition and appropriate implementation of evaluated or validated commercial off-the-shelf (COTS) IA and IA-enabled IT products. These products shall provide for the availability of systems. The products also shall ensure the integrity and confidentiality of information and the authentication and nonrepudiation of parties in electronic transactions.	---
5.9.b	*Strong preference* shall be given to the acquisition of COTS IA and IA-enabled IT products (to be used on systems entering, processing, storing, displaying, or transmitting sensitive information) that have been evaluated and validated, as appropriate, in accordance with the following: • The NIST FIPS validation program. • The National Security Agency (NSA)/NIST National Information Assurance Partnership (NIAP) Evaluation and Validation Program • The International Common Criteria for Information Security Technology Evaluation Mutual Recognition Agreement	---
5.9.c	The evaluation and validation of COTS IA and IA-enabled IT products shall be conducted by accredited commercial laboratories or by NIST.	---
5.9.d	CBP shall use only cryptographic modules that have been validated in accordance with FIPS 140-2.	---
5.9.e	Transaction-based systems (e.g. database management systems, transaction processing systems) shall implement transaction rollback and transaction journaling, or technical equivalents.	---

Product assurance responsibilities are provided below.

Product Assurance Responsibilities
CISO • Provide guidance in the use of COTS information assurance products. • Validate the proper use of information assurance products. **System/Network Administrators/Field Technology Officers/ISSOs** • Ensure selected information assurance products are properly deployed and configured. **IT Project Managers** • Comply with product assurance policy during system development.

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000327

The National Information Assurance Partnership (NIAP), a collaboration between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA), is a U.S. Government initiative designed to meet the security testing, evaluation, and assessment needs of both IT producers and consumers. NIAP combines the extensive security experience of both agencies to promote the development of technically sound security requirements for IT products and systems and appropriate metrics for evaluating those products and systems.

The NIAP Common Criteria Evaluation and Validation Scheme for IT Security (CCEVS) is a partnership between the public and private sectors, to evaluate IT product conformance to international standards. This program is being implemented to help consumers select commercial off-the-shelf IT products that meet their security requirements and to help manufacturers of those products gain acceptance in the global marketplace.

CBP will be kept apprised of the above ongoing initiatives and strongly consider the recommendations and findings of the NIAP in the selection of COTS products. This guidance applies to both stand-alone COTS products as well as those incorporated in other IT systems. Compliance with this policy, coupled with the restriction that the products have been appropriately validated by the designated Federal authorities and the Common Criteria, will reduce costs and remove the burden of maintaining and providing interoperability between numerous custom written software systems by a variety of contractors.

5.10 Malware Protection

Policy ID	CBP Policy Statements	Relevant Controls
5.10.a	Component CISOs/ISSMs shall establish and enforce Component-level malware protection control policies.	SI-3
5.10.b	Components shall implement a defense-in-depth strategy that: Installs antivirus software on desktops and servers Configures antivirus software on desktops and servers to check all files, downloads, and email Installs updates to antivirus software and signature files on desktops and servers in a timely and expeditious manner without requiring the end user to specifically request the update Installs security patches to desktops and servers in a timely and expeditious manner.	SI-3
5.10.c	System Owners shall develop and enforce procedures to ensure proper malware scanning of media prior to installation of primary hard drives, software with associated files, and other purchased products.	AC-20, SI-3

epic.org EPIC-18-07-31-CBP-FOIA-20190517-1stInterim-Production-pt3 000328