U.S. Customs and Border Protection

Attachment A

Requirements Traceability Matrix

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

Version 2.0

July 27, 2009

DOCUMENT CHANGE HISTORY

Version Number	Date	Description
1.0	July 27, 2009	Initial CBP 1400-05D release based solely on DHS 4300A, Version 6.1.1, attachment. There are no substantive differences between this CBP attachment and its source DHS attachment. This attachment is included as part of the CBP 1400-05D handbook suite to enable the CBP user to be able to access all IT security policies (DHS as well as CBP specific) at one location.
2.0	December 21, 2010	No changes.

CONTENTS

1.0 OVERVIEW

Information security policies originate primarily from three sources: the Congress, the President, and Federal agencies, including DHS. The DHS Sensitive Systems Policy Directive 4300A integrates and promulgates applicable information security policies from all sources into policies for the Department of Homeland Security (DHS). The DHS 4300A Sensitive Systems Handbook provides detailed information on techniques and procedures for implementing the policies in the policy directive. Baseline security requirements (BLSRs) generated from the DHS information security policies have been compiled in the Requirements Traceability Matrix (RTM) provided in this attachment to the handbook. The RTM serves two purposes: (1) it converts each DHS information security policy into a Baseline Security Requirement (BLSR) or task and identifies the task leader and (2) it traces each DHS information security policy (and requirement) back to its originating law, regulation, or document.

The RTM follows the paragraph organization of the DHS 4300A Sensitive Systems Handbook. Consequently, natural groupings of BLSRs occur and have been identified as Functional Areas in the table below. An acronym and a sequential number, e.g., ACC-1, identify each BLSR in a Functional Area. As policies are added and deleted, individual BLSR sequential numbers may change from version to version.

Acronym	Functional Area
ACC	Access Control
AUDIT	Audit Records
C&A	Certification and Accreditation
CIRP	Computer Incident Reporting
CM	Configuration Management
CONT	Contractors and Outsourced Operations
COPL	Continuity Planning
CPIC	Capital Planning and Investment Control
CRYPTO	Encryption
DCOM	Data Communications
EQUIP	Equipment
I&A	Identification and Authentication
MEDIA	Media Control
MGMT	Management
MTRX	Performance Measures & Metrics
NWS	Network Security
OCOM	Overseas Communications
PA	Product Assurance
PERS	Personnel Security
PHYS	Physical Security

Acronym	Functional Area
RM	Risk Management
SDLC	System Development Life Cycle
SRAP	Security Review & Assistance Program
TRNG	Security Training
VIRUS	Virus Protection
VOICE	Voice Communications Security
WCOM	Wireless Communications

2.0 RTM CONTENT

The Requirements Traceability Matrix (RTM) contains the following information:

- BLSR #: The unique identifier for the Baseline Security Requirement comprises the acronym for the BLSR's functional area (see table above) and a sequential number.
- Hdbk Ref (Handbook Reference): The section within the DHS 4300A Sensitive Systems Handbook where the policy corresponding to the BLSR is addressed.
- Baseline Security Requirement (BLSR): The actual BLSR text derived from the corresponding policy.
- Office of Primary Responsibility (OPR): In bold type, the person (by role) having primary responsibility for implementing the BLSR. Implementation of a majority of the BLSRs requires the interactions of a variety of personnel involved in the DHS information security effort. In most cases, however, a single individual will be responsible for ensuring that all actions necessary for complying with a BLSR are completed. The role identified as the OPR is the role most commonly responsible for implementing the requirement. However, Components have the latitude to assign implementation responsibility to different roles. See Section 2 of the Handbook for a listing of roles and a description of the responsibilities associated with the roles.
- Collateral Roles: Personnel having a supporting role in implementing the BLSR. These individuals will assist the OPR. Again, the identified positions reflect general practice and are not meant to be mandatory assignments.

The table below lists most of the **role acronyms** (and their meanings) found in the OPR and Collateral Roles column of the RTM.

Role Acronym	Role Title
C&OPD	Compliance & Oversight Program Director
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CO	Certifying Official
COTR	Contracting Officer's Technical Representative
CSIRC	Computer Security Incident Response Center

Role Acronym	Role Title
DAA	Designated Accrediting Authority
FM	Facility Manager
IRB	Investment Review Board
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
ITPM	Information Technology Project Manager
KO	Contracting Officer
PKI OA	Public Key Infrastructure Operational Authority
PKI PA	Public Key Infrastructure Policy Authority
PKI RA	Public Key Infrastructure Registration Authority
Authority	System/Network Administrator
S/NA	
SO	System Owner
SOC	Security Operations Center
SSO	Site Security Officer
TO	Training Officer

- Reference # @ Paragraph #: The source document and the section and/or paragraph within the document from which the BLSR is derived. Its number in the list below identifies each source document.

  1. DHS Sensitive Systems Policy Directive 4300A
  2. Federal Information Security Management Act of 2002 (FISMA)
  3. Office of Management and Budget (OMB) Circular No. A-130, Appendix III, *Security of Federal Automated Information Systems*
  4. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-55, *Security Metrics Guide for Information Technology Systems,* July 2003.
  5. ISSM Guide to the DHS Information Security Program, v2.0, July 19, 2004.
  6. DHS 4300A Sensitive Systems Handbook
  7. NIST Special Publication 800-53 Revision 2, *Recommended Security Controls for Federal Information Systems,* December 2007

3.0 REQUIREMENTS TRACEABILITY MATRIX

Source documents for the DHS baseline security requirements are identified by Reference # in the Requirements Traceability Matrix (RTM) below. Section 2.0 provides a detailed description of the information provided in the RTM.

BLSR-# Hdbk Ref	**Baseline Security Requirement (BLSR)**	**OPR** Collateral Roles	**Reference # @ Paragraph #**
RM-1 3.1	CIOs and Component CISOs/ISSMs shall establish a plan for the security and privacy of their computer systems commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or modification of or unauthorized access to the information contained in each system.	**CIOs, Component CISOs/ISSMs** SOs, ISSOs	8 @Apx F: PL-1 & PL-2, SC-14
MGMT-1 3.1	The DHS CISO and Component CISOs/ISSMs shall establish a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the IT security policies, procedures, and practices of the Department. All significant deficiencies will be addressed by a Plan of Action & Milestones (POA&M).	**CISO, Component CISOs/ISSMs** COs, SOs, DAAs	2 @ §3544(a)(6) 8 @Apx F: PL-1
MGMT-2 3.1.a&b	The CIO and Component Heads shall ensure every DHS computing resource is individually assigned to and accounted for as part of a recognized IT system.	**CIO, Component Heads** Component CISOs/ISSMs, SOs	1 @ 3.1.a
MGMT-3 3.1.b	The Component CIO shall maintain an IT systems equipment inventory.	**CIO** SOs, ITPMs, ISSOs	1 @ 3.1.b
MGMT-4 3.1.c	ITPMs and ISSOs shall jointly prepare and revise annually, as needed, a System Security Plan (SSP) for each DHS IT system that is consistent with NIST guidance.	**ITPMs, ISSOs** Component CISOs/ISSMs, SOs	1 @ 3.1.c, 3 @ 3.a.2) 8 @Apx F: PL-2,
MGMT-5 3.1.d	SOs shall designate an Information Systems Security Officer (ISSO) for their DHS IT systems.	**SOs** CISO, Component CISOs/ISSMs	1 @ 3.1.d

BLSR-# Hdbk Ref	Baseline Security Requirement (BLSR)	OPR Collateral Roles	Reference # @ Paragraph #
MGMT-6 3.1.e	Component CISOs/ISSMs shall structure their Component IT security programs to support DHS and applicable FISMA and OMB requirements.	**Component CISOs/ISSMs** SOs, ISSOs	1 @ 3.1.e
MGMT-7 3.1.f	Component CISOs/ISSMs shall report all pertinent IT security matters to the head of the Component or a designated representative.	**Component CISOs/ISSMs** SOs, ISSOs, S/NAs	1 @ 3.1.f
MGMT-8 3.1.g	The ISSO for each IT system shall serve as the POC for all security matters related to that system.	**ISSOs** SOs, ITPMs, S/NAs	1 @ 3.1.g
MGMT-9 3.1.h	Component CISOs/ISSMs shall ensure that their Component IT systems comply with the DHS Enterprise Architecture (EA) and DHS Security Architecture (SA) or that they possess a signed CIO/CISO waiver for a noncompliant system.	**Component CISOs/ISSMs** CIOs, CISO	1 @ 3.1.h
CPIC-1 3.2	Component Heads and CIOs shall ensure that IT security management processes are integrated with agency strategic and operational planning processes.	**Component Heads, CIOs** Component CISOs/ISSMs, SOs	1 @ 3.2 2 @ §3544(a)(1) 8 @Apx F: SA-1–3
CPIC-2 3.2.a	SOs and Component CISOs/ISSMs shall include security requirements in their capital planning and investment business cases for the current budget year and the Future Years Homeland Security Program.	**SOs, Component CISOs/ISSMs** CIO, IOs	1 @ 3.2.a 8 @Apx F: SA-2
CPIC-3 3.2.b	SOs or DAAs shall ensure IT security requirements are adequately funded and documented in accordance with current OMB budgetary guidance. ISSOs shall provide estimates of costs and funding.	**SOs, DAAs** CIOs, Component CISOs/ISSMs, ISSOs	1 @ 3.2.b 8 @Apx F: SA-2
CPIC-4 3.2.b	Component CISOs/ISSMs shall review and verify priorities of and the funding adequacy of budgets for Component IT program areas, mission support systems, applications, and infrastructure.	**Component CISOs/ISSMs** SOs, ISSOs, S/NAs	6 @ 3.1.5 8 @Apx F: SA-2

BLSR-# Hdbk Ref	Baseline Security Requirement (BLSR)	OPR Collateral Roles	Reference # @ Paragraph #
CPIC-5 3.2.c	Component Investment Review Boards shall approve capital investments only if the security requirements are adequately defined and funded.	**IRBs** SOs, CIO, IOs, Component CISOs/ISSMs	1 @ 3.2.c 8 @Apx F: SA-2
CONT-1 3.3.a & b	ITPMs and KOs shall ensure that outsourced IT services and operations adhere to DHS IT security policies. All statements of work and contract vehicles shall identify and document the specific security requirements for outsourced IT services and operations that are required of the contractor.	**ITPMs, KOs** ISSOs, COTRs, SOs	1 @ 3.3.a, b 8 @Apx F: PS-7, SA-4 & 9
CONT-2 3.3.c	SOs and ITPMs shall ensure statements of work and contract vehicles specify security requirements that include how DHS's 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.	**SOs, ITPMs** ISSOs, KOs, COTRs	1 @ 3.3.c 8 @Apx F: PS-7, SA-4 & 9
CONT-3 3.3.d	SOs and ITPMs shall ensure that at the expiration of the contract, statements of work and contract vehicles require the return of all sensitive DHS information and IT resources provided during the life of the contract.	**SOs, ITPMs** ISSOs, KOs, COTRs	1 @ 3.3.d
CONT-4 3.3.d	SOs and ITPMs shall ensure that at the expiration of the contract, statements of work and contract vehicles require certification that all DHS information has been purged from any contractor-owned system used to process DHS information.	**SOs, ITPMs** ISSOs, KOs, COTRs	1 @ 3.3.d
CONT-5 3.3.e	Components shall conduct reviews to ensure that the IT security requirements in the contract are implemented and enforced.	**ITPMs, KOs** ISSOs, COTRs, SOs	1 @ 3.3.e 8 @Apx F: PS-7, SA-9
MTRX-1 3.4.a	Components shall define performance measures to evaluate the effectiveness of their IT security program.	**CIOs, Component CISOs/ISSMs** SOs, ISSOs, ITPMs	1 @ 3.4.a 5 @ 4.1.5

BLSR-# Hdbk Ref	Baseline Security Requirement (BLSR)	OPR Collateral Roles	Reference # @ Paragraph #
MTRX-2 3.4.a	ISSOs shall manage the IT security metrics program for their IT systems by collecting and analyzing data during the annual self-assessment and coordinating with their CISO/ISSM on FISMA reporting and POA&M tasks, as appropriate.	**ISSOs** Component CISOs/ISSMs, ITPMs, S/NAs	1 @ 3.4.a
MTRX-3 3.4.b	Components shall provide semiannual data on their progress in implementing IT security performance measures.	**Component CISOs/ISSMs** SOs, ISSOs, COTRs	1 @ 3.4.b
COPL-1 3.5.1.a, 3.5.2.a, 3.5.3.a	The Chief Information Officer shall develop, maintain, and promulgate Continuity of Operations (COOP) and IT Contingency Planning program requirements.	**OCIO** ISSOs	1 @ 3.5.1.a, 3.5.2.a, 3.5.3.a 8 @Apx F, CP-1 & 2
COPL-2 3.5.1.b, 3.5.2.b, 3.5.3.b	The DHS CISO shall ensure compliance with HSPD-7 by developing, documenting, and maintaining a standard DHS-wide process for continuity planning that addresses Contingency Planning, and COOP.	**CISO** CIO	1 @ 3.5.1,b, 3.5.2.b, 3.5.3.b 4 @ (27)
COPL-3 3.5.1.c	Component CISOs/ISSMs and SOs shall develop, test, implement, and maintain comprehensive COOP plans to ensure the continuity and recovery of essential DHS business functionality.	**Component CISOs/ISSMs, SOs** ISSOs, FMs	1 @ 3.5.1.c
COPL-4 3.5.1.d	Component CISOs/ISSMs shall test/exercise COOP plans annually at a minimum.	**Component CISOs/ISSMs,** ISSOs	1 @ 3.5.1.d
COPL-5 3.5.1.e 3.5.3.e	SOs and ITPMs shall identify and train their personnel in the procedures and logistics of COOP planning and implementation and IT contingency planning and implementation.	**SOs, ITPMs** CIOs, Component CISOs/ISSMs, ISSOs	1 @ 3.5.1.e & 3.5.3.e
COPL-6 3.5.3.c	The IT system contingency planning, training, testing and capabilities shall be dependent on the FIPS 199 defined potential impact level. The **availability** security objective alone shall be applied to the NIST SP 800-53 contingency planning (CP) controls defined for the low, moderate, and high potential impact level systems	**SOs, ITPMs** CIOs, Component CISOs/ISSMs, ISSOs	1 @ 3.5.3.c

BLSR-# Hdbk Ref	Baseline Security Requirement (BLSR)	OPR Collateral Roles	Reference # @ Paragraph #
COPL-7 3.5.3.d & e	Comprehensive IT Contingency Plans to continue and recover critical DHS major applications and general support systems shall be developed, tested, exercised, and maintained by all DHS Components in accordance with the requirements for the FIPS 199 potential impact level for the **availability** security objective. At a minimum, when testing is required, IT Contingency Plans shall be tested/exercised annually.	**SOs** CIO, ITPMs	1 @ 3.5.3.d & e & 3.5.1.d
COPL-8 3.5.3	Ensure that adequate contingency plans are included in C&A documentation.	**SOs, Site Managers**	1 @ 3.5.3
COPL-9 3.5.3.f & 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 as required by the **availability** objective for the system. When training is required, all personnel shall receive IT Contingency Plan training or refresher training annually.		1 @ 3.5.3.f & g
SDLC-1 3.6.a	SOs and ITPMs shall manage the information system using a system development life cycle methodology that includes IT security considerations.	**SOs, ITPMs** DAAs, ISSOs, S/NAs	1 @ 3.6.a 8 @Apx F: SA-3
SDLC-2 3.6	Component CISOs/ISSMs shall establish procedures for reviewing compliance with SDLC documentation requirements	**Component CISOs/ISSMs** ISSOs, SOs, ITPMs	1 @ 3.6 8 @Apx F: SA-3 & 5
SDLC-3 3.6	ISSOs shall participate in planning and executing the SDLC process.	**ISSOs** Component CISOs/ISSMs, SOs, ITPMs	1 @ 3.6
SDLC-4 3.6	ISSOs shall review and comment on SDLC security documents for systems they control.	**ISSOs** Component CISOs/ISSMs, SOs, ITPMs	1 @ 3.6

BLSR-# Hdbk Ref	Baseline Security Requirement (BLSR)	OPR Collateral Roles	Reference # @ Paragraph #
SDLC-5 3.6	SOs and ITPMs shall ensure required security documents and reviews are included in the SDLC.	**SOs, ITPMs** ISSOs, Component CISOs/ISSMs, CIOs	1 @ 3.6 8 @Apx F: SA-3
SDLC-6 3.6	SOs and ITPMs shall prepare required security documents.	**SOs, ITPMs** ISSOs	1 @ 3.6
SDLC-7 3.6.1	SOs and ITPMs shall prepare the initial Risk Assessment and Security Plan during the SDLC Planning phase.	**SOs, ITPMs** ISSOs	1 @ 3.6
SDLC-8 3.6.2–3.6.6	SOs and ITPMs shall update the Risk Assessment and Security Plan during the SDLC Requirements Definition, Design, Development, Test, and Implementation phases.	**SOs, ITPMs** ISSOs	1 @ 3.6
SDLC-9 3.6.2	SOs and ITPMs shall prepare the initial security inputs to the IT Training Plan during the SDLC Requirements Definition phase.	**SOs, ITPMs** ISSOs	1 @ 3.6
SDLC-10 3.6.2	SOs and ITPMs shall prepare the initial IT Contingency Plan during the SDLC Requirements Definition phase.	**SOs, ITPMs** ISSOs	1 @ 3.6
SDLC-11 3.6.3	SOs and ITPMs shall update the security information in the IT Training Plan during the SDLC Design phase.	**SOs, ITPMs** ISSOs	1 @ 3.6
SDLC-12 3.6.3	SOs and ITPMs shall update the IT Contingency Plan during the SDLC Design phase.	**SOs, ITPMs** ISSOs, Project Team	1 @ 3.6
SDLC-13 3.6.3	SOs and ITPMs shall initiate the Certification and Accreditation (C&A) package during the SDLC Design phase.	**SOs, ITPMs** Component CISOs/ISSMs, Project Team, S/NAs	1 @ 3.6
SDLC-14 3.6.4	SOs and ITPMs shall conduct the initial Developmental Security Test and Evaluation (ST&E) during the SDLC Development phase.	**SOs, ITPMs** ISSOs, Project Team	1 @ 3.6

BLSR-# Hdbk Ref	Baseline Security Requirement (BLSR)	OPR Collateral Roles	Reference # @ Paragraph #
SDLC-15 3.6.4	SOs and ITPMs shall develop the initial Operational ST&E during the SDLC Development phase.	**SOs, ITPMs** ISSOs, Project Team	1 @ 3.6
SDLC-16 3.6.4	SOs and ITPMs shall update the Certification and Accreditation (C&A) package during the SDLC Development phase.	**SOs, ITPMs** Component CISOs/ISSMs, Project Team, S/NAs	1 @ 3.6
SDLC-17 3.6.5	SOs and ITPMs shall conduct the formal Developmental ST&E during the SDLC Test phase.	**SOs, ITPMs** ISSOs, Project Team	1 @ 3.6
SDLC-18 3.6.5	SOs and ITPMs shall update the Certification and Accreditation (C&A) package during the SDLC Test phase.	**SOs, ITPMs** Component CISOs/ISSMs, Project Team, S/NAs	1 @ 3.6
SDLC-19 3.6.6	SOs and ITPMs shall conduct the Operational ST&E on the upgraded or new system during the SDLC Implementation phase.	**SOs, ITPMs** ISSOs, Project Team	1 @ 3.6
SDLC-20 3.6.6	SOs and ITPMs shall finalize the security inputs to the IT Training Plan during the SDLC Implementation phase.	**SOs, ITPMs** ISSOs, Project Team	1 @ 3.6
SDLC-21 3.6.6	SOs and ITPMs shall finalize the Certification and Accreditation (C&A) package during the SDLC Implementation phase.	**SOs, ITPMs** Component CISOs/ISSMs, Project Team, S/NAs	1 @ 3.6
SDLC-22 3.6.7	SOs and ITPMs shall conduct annual security awareness and role-based training during the SDLC Operations and Maintenance phase.	**SOs, ITPMs** COs	1 @ 3.6
SDLC-23 3.6.7	SOs and ITPMs shall review C&A status during the SDLC Operations and Maintenance phase and shall update C&A documentation as required to maintain C&A currency.	**SOs, ITPMs** Component CISOs/ISSMs, ISSOs	1 @ 3.6

BLSR-# Hdbk Ref	Baseline Security Requirement (BLSR)	OPR Collateral Roles	Reference # @ Paragraph #
SDLC-24 3.6.8	SOs and ITPMs shall terminate system operations during the SDLC Disposition phase.	**SOs, ITPMs** ISSOs, S/NAs, Project Team	1 @ 3.6, 4.3.3, & 4.3.5
SDLC-25 3.6.8 & 4.3.3.a	SOs and ITPMs shall dispose of equipment and media in accordance with security requirements during the SDLC Disposition phase.	**SOs, ITPMs** CIOs, Component CISOs/ISSMs, ISSOs	1 @ 3.6 & 4.3.3.a 8 @Apx F: SA-3
SDLC-26 3.6a	SOs and ITPMs shall ensure that security requirements are integrated into the SDLC through management, operational, and technical control mechanisms from the IT system's inception to its disposal.	**Component CISOs/ISSMs** SOs, ITPMs	1 @ 3.6.a
SDLC-27 3.6	Component CISOs/ISSMs shall participate in capital planning and investment management meetings involving SDLC considerations for IT systems and networks.	**Component CISOs/ISSMs** SOs, ITPMs	1 @ 3.6
SDLC-28 3.6	Component CISOs/ISSMs and ISSOs shall ensure that required IT security documentation is produced and reviewed in accordance with SDLC milestones.	**Component CISOs/ISSMs, ISSOs** SOs, ITPMs	1 @ 3.6
SDLC-29 3.6	Component CISOs/ISSMs shall approve IT security documentation produced as part of the SDLC process (except the C&A package).	**SOs, ITPMs** Component CISOs/ISSMs, CIOs	1 @ 3.6
RM-2 3.7	SOs and ITPMs shall establish and periodically test the capability to continue providing service within a system based upon the needs and priorities of the participants of the system.	**SOs, ITPMs** CISO, COs, ISSOs	3 @ 3a 2) e)
CM-1 3.7.a	Components shall prepare configuration management plans for all IT systems.	**ITPMs** Component CISOs/ISSMs, SOs	1 @ 3.7.a 8 @Apx F: CM-1

BLSR-# Hdbk Ref	Baseline Security Requirement (BLSR)	OPR Collateral Roles	Reference # @ Paragraph #
CM-2 3.7.b	Components shall establish, implement, and enforce configuration management controls on all IT systems and networks. They shall use a POA&M to implement a solution for any significant deficiency.	**ITPMs, ISSOs** SOs, S/NAs	1 @ 3.7.b 8 @Apx F, CM-1, 2
CM-3 3.7.c	Components shall install security patches in accordance with configuration management plans or direction from the DHS Computer Security Incident Response Center (CSIRC).	**ITPMs, S/NAs** ISSOs, CSIRC	1 @ 3.7.c
RM-3 3.8	SOs and Component CISOs/ISSMs shall provide information security for the information and information systems that support the operations and assets under their control by implementing policies and procedures to cost-effectively reduce risks to an acceptable level.	**SOs, Component CISOs/ISSMs** CIOs, ITPMs	2 @ §3544(a)(2)
RM-4 3.8	SOs and Component CISOs/ISSMs shall provide information security for the information and information systems that support the operations and assets under their control by periodically testing and evaluating information security controls and techniques to ensure that they are effectively implemented.	**SOs, Component CISOs/ISSMs** CIOs, ITPMs, ISSOs, S/NAs	2 @ §3544(a)(2) 8 @Apx F, CA-2
RM-5 3.8.a	Components shall establish a risk management program in accordance with NIST SP 800-30, *Risk Management Guide for Information Technology Systems*.	**CIOs, Component CISOs/ISSMs** SOs, ITPMs, ISSOs	1 @ 3.8.a
RM-6 3.8.b	Components shall conduct risk assessments of their IT systems whenever significant changes to the system configuration or to the operational/threat environment have been made, or every 3 years, whichever occurs first.	**ITPMs, ISSOs** Component CISOs/ISSMs, SOs,	1 @ 3.8.b 8 @Apx F, CA-4, RA-3
C&A-1 3.9.a	For each of their sensitive IT systems, Components shall assign an impact level (high, moderate, low) to each security objective (confidentiality, integrity, and availability). Impact levels shall be assigned according to the standards set in FIPS Pub 199, Standards for Security Categorization of Federal Information and Information Systems, and following guidance in NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories.	**DAAs, SOs, ITPMs** Component CISOs/ISSMs, ISSOs	1 @ 3.9.a 8 @ Apx F, RA-2

BLSR-# Hdbk Ref	Baseline Security Requirement (BLSR)	OPR Collateral Roles	Reference # @ Paragraph #
C&A-2 3.9.a	Components shall apply NIST 800-53 controls specific to the security objective at the determined impact level.	**COs, DAAs** Component CISOs/ISSMs, SOs, ITPMs, ISSOs, CIOs	1 @ 3.9.a 8 @Apx F, CA-1
C&A-3 3.9.b	DAAs, SOs, or ITPMs shall implement NIST SP 800-53 security controls based on the impact level established for each security objective (confidentiality, integrity, availability) using the FIPS Pub 200 (*Minimum Security Requirements for Federal Information and Information Systems*) methodology. For systems involving personally identifiable information, the confidentiality security objective shall be assigned an impact level of at least moderate, and 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. Components shall implement the respective controls by the FIPS Pub 200 compliance deadline (March 2007).	**DAAs, SO, ITPMs** Component CISOs/ISSMs, ISSOs	1 @ 3.9.b
C&A-4 3.9.c	Component CISOs/ISSMs and ISSOs should use type certification/accreditation for IT resources that meet the criteria for type certification/accreditation.	**Component CISOs/ISSMs, ISSOs** DAAs, SOs	1 @ 3.9.c
C&A-5 3.9.d	The DAA for a system—normally the system owner or an appropriate program official—should be identified in TrustedAgent FISMA. The Component CIO shall serve as the DAA when the system owner or an appropriate program official has not been named as the DAA.	**DAAs, CIO**	1 @ 3.9.d
C&A-6 3.9.e	Components 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.	**COs** SOs, ISSOs, Component CISOs/ISSMs, ITPMs, DAAs	1 @ 3.9.e 8 @Apx F, CA-4
C&A-7 3.9.f	Components shall document in the certification package the extent to which a particular design and its implementation plan meet a specified set of security safeguards.	**ISSOs, ITPMs** SOs, Component CISOs/ISSMs, COs, DAAs	1 @ 3.9.f

BLSR-# Hdbk Ref	Baseline Security Requirement (BLSR)	OPR Collateral Roles	Reference # @ Paragraph #
C&A-8 3.9.g	Components shall review the impact on the security of the information processed whenever any modification is made to sensitive IT systems or networks or to the physical environment, interfaces, or user community of the system. If the impact is significant, the system shall be re-accredited.	**ITPMs, ISSOs** Component CISOs/ISSMs, SOs	1 @ 3.9.g 8 @Apx F, CA-7
C&A-9 3.9.h	Components shall certify and accredit systems at initial operating capability and every 3 years thereafter or when a major change occurs, whichever occurs first.	**DAAs, COs** Component CISOs/ISSMs, SOs, ISSOs	1 @ 3.9.h 8 @Apx F, CA-4, CA-6
C&A-10 3.9.i	The DAA may grant a system undergoing development testing or in a prototype phase of development an Interim Authorization to Operate (IATO) for a maximum period of 6 months, and may grant a second and final IATO for an additional 6-month period. However, the system must be certified and accredited in an Authorization to Operate (ATO) letter prior to passing Key Decision Point 3 in the development life cycle and becoming operational.	**DAAs** SOs, ISSOs, Component CISOs/ISSMs, ITPMs, COs	1 @ 3.9.i
C&A-11 3.9.j	DAAs shall not allow testing or prototype sensitive systems that are not fully accredited and have not received a full ATO by the end of the second and final IATO to be deployed as an operational system.	**DAAs** SOs, ISSOs, Component CISOs/ISSMs, ITPMs, COs	1 @ 3.9.j
C&A-12 3.9.k	The CIO, CISO, DAAs, and Component CISOs/ISSMs shall honor existing accreditations performed prior to the transfer of a Component's systems to the DHS provided that the accreditation complied fully with policy in effect at time of accreditation, no significant deficiencies have been identified, and the system configuration has not changed since accreditation.	**CIO, CISO, DAAs, Component CISOs/ISSMs** SOs, ISSOs, ITPMs, COs	1 @ 3.9.k
C&A-13 3.9.l	Components, as of April 11, 2005, shall use the automated C&A tool approved by the DHS CISO to accredit all Component IT systems.	**Component CISOs/ISSMs** SOs, DAAs, ISSOs, S/NAs	1 @ 3.9.l

BLSR-# Hdbk Ref	Baseline Security Requirement (BLSR)	OPR Collateral Roles	Reference # @ Paragraph #
C&A-14 3.9	Ensure that the System Security Plan, Security Test & Evaluation, Contingency Plan, and Risk Assessment contain the information required for C&A.	**COs**	1 @ 3.9
SRAP-1 3.10.a	Components shall submit their IT security policies to the DHS CISO for review.	**Component CISOs/ISSMs** CIOs, SOs, ITPMs	1 @ 3.10.a
SRAP-2 3.10.b	Components shall establish an IT security review and assistance program within their respective security organizations.	**Component CISOs/ISSMs** SOs, ISSOs	1 @ 3.10.b
SRAP-3 3.10.c	Components shall conduct their IT security reviews in accordance with NIST Special Publication 800-53 Revision 2, *Recommended Security Controls for Federal Information Systems*, and submit quarterly updates via the TrustedAgent FISMA reporting tool.	**ITPMs, ISSOs** SOs	1 @ 3.10.c
SRAP-4 3.10.c	Component CISOs/ISSMs shall ensure all significant deficiencies identified in the self-assessment are documented.	**Component CISOs/ISSMs** SOs, ISSOs	1 @ 3.10.c 6 @ 3.3.1.b
SRAP-5 3.10.c	Component CISOs/ISSMs shall ensure a Plan of Action and Milestones (POA&M) is developed to address the identified deficiencies.	**Component CISOs/ISSMs** C& OPD, SOs, ISSOs	1 @ 3.10.c 6 @ 3.3.1.c 8 @Apx F, CA-5
SRAP-6 3.10.c	Component CISOs/ISSMs shall monitor the status of POA&M "milestones."	**Component CISOs/ISSMs** SOs, ISSOs	1 @ 3.10.c 6 @ 3.3.1.d
SRAP-7 3.10.c	Component CISOs/ISSMs shall ensure POA&M updates are submitted in TrustedAgent FISMA by the Component data submission deadlines, i.e., March 10, June 10, September 15, and December 10.	**Component CISOs/ISSMs** C&OPD, SOs, ISSOs	1 @ 3.10.c 6 @ 3.3.1.e

BLSR-# Hdbk Ref	Baseline Security Requirement (BLSR)	OPR Collateral Roles	Reference # @ Paragraph #
SRAP-8 3.10.d	The CISO shall conduct review and assistance visits throughout the Department to determine the extent to which the Components and office programs comply with departmental IT security policy, standards, and procedures.	**CISO** CIOs, Component CISOs/ISSMs, SOs, ISSOs, ITPMs	1 @ 3.10.d
SRAP-9 3.11.1.a	Component CISOs/ISSMs shall actively participate in the DHS Information Systems Security Board.	**Component CISOs/ISSMs**	1 @ 3.11.1.a
SRAP-10 3.11.1.b	Component CISOs/ISSMs shall ensure that the Component CIO is kept apprised of all pertinent matters involving the security of IT systems and that IT security-related decisions and information, including updates to the 4300 series of IT security publications, are distributed to the ISSOs and other appropriate persons within their Component.	**Component CISOs/ISSMs** ISSOs	1 @ 3.11.1.b
TRNG-1 3.11.3.a	Components shall appoint a representative to the DHS IT Security Training Working Group. This individual shall be responsible for managing the Component's IT security training program.	**Component CISOs/ISSMs** Training Officers	1 @ 3.11.3.a
TRNG-2 3.11.3.b	Component Training Officers shall actively participate in the DHS IT Security Training Working Group.	**Training Officers** Component CISOs/ISSMs	1 @ 3.11.3.b
PERS-1 3.12.a–c	Component CISOs/ISSMs shall ensure that DHS employees and contractors who fail to comply with DHS IT security policy are held accountable for their actions in accordance with DHS disciplinary policies and applicable laws.	**Component CISOs/ISSMs** Supervisors	1 @ 3.12.a–c 8 @Apx F: PS-8
MGMT-10 3.13	C&A artifacts (e.g., Privacy Impact Assessment, System Security Plan, Security Test & Evaluation Report, Contingency Plan Test Results, Risk Assessment, ATO letter) shall be uploaded into TAF.	**ISSOs, Component CISOs/ISSMs**	1 @ 3.13
MGMT-11 3.13.a	Components shall collect and submit their IT security program status data as required by FISMA	**Component CISOs/ISSMs** SOs, ISSOs	1 @ 3.13.a

BLSR-# Hdbk Ref	Baseline Security Requirement (BLSR)	OPR Collateral Roles	Reference # @ Paragraph #
MGMT-12 3.13.b	Components shall utilize the automated tool approved by the DHS CISO for collecting IT security program data for the periodic FISMA report.	**SOs, ISSOs** Component CISOs/ISSMs	1 @ 3.13.b
MGMT-13 3.14.1.a	Personally identifiable information shall not be physically removed from a DHS facility without written authorization from the system Designated Accrediting Authority (DAA) or person designated in writing by the DAA.		1 @ 3.14.1.a
MGMT-14 3.14.1.b	Personally identifiable information removed from a DHS facility shall be encrypted.		1 @ 3.14.1.b
MGMT-15 3.14.1.c	If personally identifiable information can be physically removed from a DHS facility, the System Security Plan shall document the specific procedures, training, and accountability measures in place to ensure remote use of the encrypted data does not bypass the protections provided by the encryption.		1 @ 3.14.1.c
MGMT-16 3.14.3.a	Components shall determine whether government e-authentication security requirements apply to their systems allowing online transactions.		1 @ 3.14.3.a
MGMT-17 3.14.3.b	For those systems for which e-authentication requirements apply, Components shall determine the appropriate assurance level for e-authentication by following the steps described in OMB M-04-04, E-Authentication Guidance for Federal Agencies		1 @ 3.14.3.b
MGMT-18 3.14.3.c	For those systems for which e-authentication requirements apply, Components shall implement at the appropriate assurance level the technical requirements described in NIST SP 800-63, Electronic Authentication Guideline.		1 @ 3.14.3.c
SDLC-30 3.14.a	ITPMs and SOs shall ensure that a Privacy Impact Assessment is conducted, if required, during the SDLC Planning phase of the development of a new IT system or when an existing system is significantly modified.	**SOs, ITPMs** ISSOs	1 @ 3.14.a 8 @Apx F, PL-5

BLSR-# Hdbk Ref	Baseline Security Requirement (BLSR)	OPR Collateral Roles	Reference # @ Paragraph #
PERS-2 4.1.1.a	Components shall designate the sensitivity or risk level for all government and contractor IT positions.	**SOs** ITPMs, ISSOs, Component CISOs/ISSMs, Office of Security	1 @ 4.1.1.a 8 @Apx F: PS-2
PERS-3 4.1.1.b	Components shall ensure the incumbents of sensitive system positions have favorably adjudicated background investigations.	**SOs** ITPMs, ISSOs, Component CISOs/ISSMs, Office of Security	1 @ 4.1.1.b 8 @Apx F: PS-3
ACC-1 4.1.1.c&d	SOs and S/NAs shall implement controls to ensure that no individual is granted access to DHS systems without having a favorably adjudicated Minimum Background Investigation (MBI).	**SOs, S/NAs** ITPMs, ISSOs, Component CISOs/ISSMs, Office of Security	1 @ 4.1.1.c&d 8 @Apx F: IA-4, PS-3
ACC-2 4.1.1.e	The Component Head or designee shall grant access to DHS systems for non-DHS 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.	**Component Head** CSO, CIO	1 @ 4.1.1.e
PERS-4 4.1.2.a	Components shall establish rules of behavior for the IT systems under their control.	**SOs, ITPMs** SOs, ISSOs, Component CISOs/ISSMs	1 @ 4.1.2.a 8 @Apx F: PL-4

BLSR-# Hdbk Ref	Baseline Security Requirement (BLSR)	OPR Collateral Roles	Reference # @ Paragraph #
PERS-5 4.1.2.b	Components shall train users regarding the Rules of Behavior for the IT systems to which they have been granted access. Training shall describe potential disciplinary actions that may be taken for violating the system rules of behavior. ISSOs shall obtain and maintain signed Rules of Behavior from new users.	**ISSOs** SOs, ITPMs, Component CISOs/ISSMs	1 @ 4.1.2.b 8 @Apx F: PL-4, PS-6 & 8
PERS-6 4.1.2	SOs shall enforce Rules of Behavior for IT systems under their authority.	**SOs** ISSOs, Component CISOs/ISSMs, Supervisors	1 @ 4.1.2
PERS-7 4.1.3.a	SOs shall ensure that users of the systems supporting their programs have a validated requirement to access these systems.	**SOs** ISSOs, ITPMs, Supervisors	1 @ 4.1.3.a 8 @Apx F: PS-3
PERS-8 4.1.4.a	Components shall, where possible, divide and separate duties and responsibilities of critical functions among different individuals to ensure that no individual has total control of the system's security mechanisms.	**SOs** ISSOs, S/NAs	1 @ 4.1.4.a
TRNG-3 4.1.5.a	Components shall establish an IT Security Training Program that complies with all applicable DHS IT Security Training policies. The training program shall encompass initial awareness training, refresher training for all users, and specialized training for security professionals.	**Component CISOs/ISSMs** SOs, ISSOs, Supervisors	1 @ 4.1.5.a 8 @Apx F: AT-1
TRNG-4 4.1.5.b	DHS personnel and contractors accessing DHS IT systems shall receive initial training in security awareness and accepted security practices as part of their orientation and shall sign rules of behavior prior to being given access to DHS IT systems; they shall receive refresher training by May 31st of each year..	**Component CISOs/ISSMs, ISSOs** SOs, Supervisors	1 @ 4.1.5.b 8 @Apx F: AT-2 & 3
TRNG-5 4.1.5.c	DHS personnel and contractors with significant security responsibilities (e.g., ISSOs, system administrators) shall receive specialized training specific to their security responsibilities prior to being given access to DHS IT systems.	**COTRs** KOs, Component CISOs/ISSMs, ISSOs, SOs	1 @ 4.1.5.c

BLSR-# Hdbk Ref	Baseline Security Requirement (BLSR)	OPR Collateral Roles	Reference # @ Paragraph #
TRNG-6 4.1.5.c	Component CISOs/ISSMs and SOs shall ensure that security professionals receive annual specialized training specific to their security responsibilities.	**Component CISOs/ISSMs, SOs** CIOs, ISSOs	1 @ 4.1.5.c 8 @Apx F, AT-3
TRNG-7 4.1.5.d	Component CISOs/ISSMs, ISSOs, and COTRs shall maintain accurate records of completed IT security training. Records shall include signed Rules of Behavior and shall contain names and positions of individuals receiving training, the type of training provided, and training costs.	**Component CISOs/ISSMs, ISSOs, COTRs** SOs, Supervisors	1 @ 4.1.5.d 8 @Apx F, AT-4
TRNG-8 4.1.5.e	Unless the CISO/ISSM grants a waiver, Components shall disable user accounts and access privileges, including access to e-mail, of those DHS users who have failed to complete annual security awareness training.	**S/NAs, ISSOs** Component CISOs/ISSMs, SOs, ITPMs	1 @ 4.1.5.e
TRNG-9 4.1.5.f	Component CISOs/ISSMs shall prepare and submit to the DHS IT Security Training Program Director, by September 1 each year, a Security Awareness Training Plan and an IT Security Professional Training Plan. The awareness plan shall include the following: Total number of employees and contractors with DHS network accounts Awareness programs/training provided in addition to the DHS Official Information Systems Security Training How Component personnel are made aware of the awareness programs Dates awareness training will occur. The professional training plan shall contain: Number of information systems security personnel Training venue (e.g., DHS Virtual Campus, Component-sponsored classroom training, seminars, conferences) Training dates	**Component CISOs/ISSMs** ISSOs, COTRs, ITPMs, SOs	1 @ 4.1.5.f 8 @Apx F, AT-1

BLSR-# Hdbk Ref	Baseline Security Requirement (BLSR)	OPR Collateral Roles	Reference # @ Paragraph #
TRNG-10 4.1.5.g	Components shall prepare and submit training statistics semiannually to the DHS IT Security Training Program Director as follows: (1) total number of personnel and number of personnel who have received annual awareness training and (2) total number of IT security personnel and total number who have been trained.	**Component CISOs/ISSMs** ISSOs, COTRs, ITPMs, SOs	1 @ 4.1.5.g
TRNG-11 4.1.5.g	Components shall ensure that IT security awareness and training statistics are provided to the CISO/ISSM as required to meet DHS reporting deadlines.	**ISSOs, COTRs** ITPMs, SOs	1 @ 4.1.5.g
TRNG-12 4.1.5.h	Components shall provide evidence of training provided to their personnel 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.		1 @ 4.1.5.h
PERS-9 4.1.6.a	Components shall implement procedures to ensure system accesses are revoked for employees or contractors who leave the Component or are reassigned to other duties.	**SOs, Supervisors** ISSOs, S/NAs	1 @ 4.1.6.a 8 @Apx F: IA-4, PS-4 & 5
PERS-10 4.1.6.b	Components shall establish procedures to ensure sensitive information stored on any media is transferred to an authorized individual upon the termination or reassignment of an employee or contractor.	**SOs, Component CISOs/ISSMs** ITPMs, ISSOs	1 @ 4.1.6.b
PHYS-1 4.2.1.a	FMs shall grant access only to authorized personnel for entry into DHS buildings, rooms, work areas, spaces, and structures housing IT systems, equipment, and data, including any non-DHS or contractor facilities that house DHS IT systems.	**FMs** SOs, SSOs, ISSOs, Office of Security	1 @ 4.2.1.a 8 @Apx F: PE-2 & 3.
PHYS-2 4.2.1.a	FMs shall implement access controls that safeguard DHS assets against loss, theft, destruction, accidental damage, hazardous conditions, fire, malicious actions, and natural disasters.	**FMs** SOs, SSOs, ISSOs, Office of Security	1 @ 4.2.1.a 8 @Apx F: PE-1, 3, 6, 12 – 16, SI-3
PHYS-3 4.2.1.b	FMs shall establish and implement procedures to require visitors to log in and out and to be escorted while in the facility. Visitor logs shall be maintained for one year.	**FMs** SOs, SSOs, ISSOs, Office of Security	1 @ 4.2.1.b 8 @Apx F: PE-7 & 8

BLSR-# Hdbk Ref	Baseline Security Requirement (BLSR)	OPR Collateral Roles	Reference # @ Paragraph #
PHYS-4 4.2.1.b	FMs shall establish and implement procedures to restrict contractor access to those work areas requiring their presence. Separate contractor visitor logs shall be maintained for one year.	**FMs** SOs, SSOs, ISSOs, Office of Security	1 @ 4.2.1.b 8 @Apx F: PE-8
PHYS-5 4.2.2.a	SOs and FMs shall incorporate physical protection measures based on the criticality of the operations and missions supported by the information processed by IT systems within the facility.	**SOs, FMs** SSOs, ISSOs, Office of Security	1 @ 4.2.2.a 8 @Apx F: PE-1, 6 & 12
PHYS-6 4.2.2.b	FMs shall implement controls to ensure that sensitive information or data not suitable for public release is secured in a locked area, such as an office, room, desk, bookcase, or file cabinet.	**FMs** SSOs, ISSOs, Supervisors	1 @ 4.2.2.b
MEDIA-1 4.3.1.a	FMs shall implement controls to ensure that all media containing sensitive information, including hard copy media, backup media and 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.	**FMs** ISSOs, Supervisors	1 @ 4.3.1.a
MEDIA-2 4.3.1.b	FMs shall ensure that backup media are stored off site in accordance with their business continuity and IT contingency plans.	**FMs** SSOs, ISSOs, Office of Security	1 @ 4.3.1.b
MEDIA-3 4.3.2.a	Media determined by the information owner to contain sensitive information should be appropriately marked in accordance with DHS MD 11042.1: *Safeguarding Sensitive but Unclassified (For Official Use Only) Information*.	**ISSOs** SOs, Users	1 @ 4.3.2.a
MEDIA-4 4.3.3.a & b	Components shall implement controls to ensure that any information systems storage medium containing sensitive information is sanitized using approved methods before it is disposed of, reused, recycled, or returned to the owner or manufacturer and that records are maintained of the sanitization and disposition of information systems storage medium.	**FMs** ISSOs, S/NAs, SSOs, Users	1 @ 4.3.3.a & b
MEDIA-5 4.3.3.c	Components shall periodically test degaussing equipment to verify the equipment is functioning properly.	**SSOs, ISSOs** SOs, S/NAs	1 @ 4.3.3.c

BLSR-# Hdbk Ref	Baseline Security Requirement (BLSR)	OPR Collateral Roles	Reference # @ Paragraph #
MEDIA-6 4.3.4.a & b	Components shall establish and implement procedures to ensure sensitive information cannot be accessed or stolen by unauthorized individuals, with the procedures covering sensitive information in electronic or paper form and including the protection of this information during transport and mailing.	**FMs** ISSM, SOs, ISSOs, SSOs, S/NAs, Users	1 @ 4.3.4.a, .b 8 @Apx F, MP-2
VOICE-1 4.4.1.a	Components shall provide adequate physical and IT security for all DHS-owned private branch exchanges (PBXs).	**FMs** SSOs, S/NAs	1 @ 4.4.1.a
VOICE-2 4.4.2.a	Components shall develop guidance for discussing sensitive information on the telephone.	**Component CISOs/ISSMs** SOs, CIOs	1 @ 4.4.2.a
VOICE-3 4.4.2.a	Classified national security information shall under no circumstances be discussed on unsecured telephones.	**Component CISOs/ISSMs, ISSOs, COTRs** SSOs	1 @ 4.4.2.a
VOICE-4 4.4.3.a	Components shall establish and enforce procedures to ensure that sensitive information is not stored in voice mail.	**FMs** ISSOs, SSOs, S/NAs, Supervisors	1 @ 4.4.3.a
DCOM-1 4.5.1.a	Components shall develop guidance for the selection and implementation of cost-effective telecommunications protection techniques.	**Component CISOs/ISSMs** CISO, SOs, S/NAs, ISSOs, FMs, SSOs	1 @ 4.5.1.a
DCOM-2 4.5.2.a	Components shall develop guidance for the selection, implementation, and enforcement of technical controls for fax technology and systems (including fax machines, servers, gateways, software, and protocols) that transmit and receive sensitive information.	**Component CISOs/ISSMs** ISSOs, S/NAs	1 @ 4.5.2.a
DCOM-3 4.5.2.b	Components shall configure fax servers to ensure that incoming lines cannot be used to access the network or any data on the fax server.	**S/NAs** ISSOs	1 @ 4.5.2.b

BLSR-# Hdbk Ref	Baseline Security Requirement (BLSR)	OPR Collateral Roles	Reference # @ Paragraph #
ACC-3 4.5.3.a	Components shall implement controls to ensure that only individuals with the appropriate clearance and need to know are allowed to participate in video teleconferences.	**ISSOs, SSOs** SOs, Supervisors	1 @ 4.5.3.a
DCOM-4 4.5.3.b	Components shall ensure appropriate transmission protections are in place commensurate with the highest classification of information to be discussed during a video teleconference.	**ISSOs, S/NAs** SOs, SSOs	1 @ 4.5.3.b
DCOM-5 4.5.3.c	S/NAs shall ensure that video teleconferencing equipment and software are disabled when not in use.	**S/NAs** ISSOs	1 @ 4.5.3.c
DCOM-6 4.5.4a	Components shall approve the use of voice over data network technology only when the inherent risks are clearly identified in the Accreditation package and a strong business justification for the use of this technology has been documented.	**DAAs** COs, SOs, ITPMs, ISSOs	1 @ 4.5.4.a
DCOM-7 4.5.4.b	When approved for use, ITPMs shall design voice over data network implementations with sufficient redundancy to ensure network outages do not result in the loss of both voice and data communications.	**ITPMs** DAAs, Component CISOs/ISSMs, SOs, CIOs, ISSOs, S/NAs	1 @ 4.5.4.b
DCOM-8 4.5.4.c	Components shall ensure appropriate identification and authentication controls, audit logging, and integrity controls are implemented on every component of any voice over data network approved for use.	**ITPMs** DAAs, Component CISOs/ISSMs, ISSOs, SOs, S/NAs	1 @ 4.5.4.c
PHYS-7 4.5.4.d	SSOs shall ensure physical access to voice over data network components is restricted to authorized personnel.	**SSOs** ISSOs	1 @ 4.5.4.d
WCOM-1 4.6.a	The DAA shall specifically approve the technology and application of every wireless communication method to be employed within DHS.	**DAA** CIO, Component CISOs/ISSMs, ISSOs	1 @ 4.6.a
WCOM-2 4.6.b	Components 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.	**DAAss** SOs, Component CISOs/ISSMs, ITPMs	1 @ 4.6.b

BLSR-# Hdbk Ref	Baseline Security Requirement (BLSR)	OPR Collateral Roles	Reference # @ Paragraph #
WCOM-3 4.6.c	The DHS Wireless Management Office shall be notified within 30 days of all wireless communications systems acquisitions.	**DAAs**	1 @ 4.6.c
WCOM-4 4.6.1.a	Component CISOs/ISSMs shall ensure annual security assessments are conducted on all approved wireless systems and enumerate vulnerabilities, risk statements, risk levels, and corrective actions.	**Component CISOs/ISSMs** SOs, ITPMs, ISSOs, S/NAs	1 @ 4.6.1.a
WCOM-5 4.6.1.b	SOs and ITPMs shall develop and maintain risk mitigation plans that address wireless security vulnerabilities, prioritize corrective actions, and implement milestones in accordance with defined risk levels.	**SOs, ITPMs** Component CISOs/ISSMs, ISSOs, S/NAs	1 @ 4.6.1.b
WCOM-6 4.6.1.c	SOs and ITPMs shall identify and establish cost-effective countermeasures to denial-of-service attacks before a wireless system is approved for use.	**SOs, ITPMs** CISO, Component CISOs/ISSMs,	1 @ 4.6.1.c
WCOM-7 4.6.1.d	SOs and ITPMs shall ensure that the System Security Plan adopts a defense-in-depth strategy in order to ensure security solutions and secure connections to external interfaces are consistently enforced.	**SOs, ITPMs** Component CISOs/ISSMs, ISSOs	1 @ 4.6.1.d
WCOM-8 4.6.1.e	SOs, Component CISOs/ISSMs, and ITPMs who direct the operation of legacy DHS wireless systems that are not compliant with DHS IT security policy shall obtain a CISO-approved waiver or exception, as appropriate, to continue operations, shall prepare a migration plan to a DHS-compliant security architecture, and shall implement the migration plan.	**SOs, Component CISOs/ISSMs, ITPMs** CISO, DAAs, ISSOs	1 @ 4.6.1.e
WCOM-9 4.6.2.a	Wireless PED users are prohibited, except by DAA written consent, from using their wireless PEDs and accessory devices in areas where DHS sensitive or classified information is discussed. Also prohibited are PED functions that can record or transmit data via video, IR, or RF.	**DAAs, Users** ISSOs, S/NAs, Supervisors	1 @ 4.6.2.a

BLSR-# Hdbk Ref	Baseline Security Requirement (BLSR)	OPR Collateral Roles	Reference # @ Paragraph #
WCOM-10 4.6.2.b	S/NAs shall implement controls to ensure that wireless PEDs are not connected either physically or wirelessly to the wired core DHS network without written DAA consent.	**S/NAs, DAAs** Component CISOs/ISSMs, SOs, ITPMs	1 @ 4.6.2.b
WCOM-11 4.6.2.c	SOs and ITPMs shall ensure encryption of all sensitive information [e.g., combinations, personal identification numbers (PINs)] that is or will be stored, processed, or transmitted by wireless PEDs.	**SOs, ITPMs** Users, DAAs	1 @ 4.6.2.c
WCOM-12 4.6.2.d	SOs and ITPMs shall ensure that wireless PEDs such as BlackBerry devices and smartphones employ strong identification, authentication, and encryption (data and transmission) technologies. They shall ensure that PEDs such as BlackBerry devices and smartphones are password-protected, with a security timeout period established. For BlackBerry devices, the security timeout shall be set to 10 minutes.	**SOs, ITPMs** Component CISOs/ISSMs, DAAs, SOs, ISSOs	1 @ 4.6.2.d
WCOM-13 4.6.2.e	SOs and ITPMs shall develop and implement provisions, procedures, and restrictions, documented in the System Security Plan, for using a wireless PED to download mobile code.	**SOs, ITPMs** DAAs, Component CISOs/ISSMs, ISSOs	1 @ 4.6.2.e
WCOM-14 4.6.2.f	S/NAs shall ensure that DHS Technical Reference Model (TRM)-approved versions of antivirus software and software patches are installed on wireless PEDs.	**S/NAs** SOs, ITPMs, Component CISOs/ISSMs, ISSOs	1 @ 4.6.2.f
WCOM-15 4.6.2.g	SOs and ITPMs shall ensure that cost-effective countermeasures to denial-of-service attacks are identified and established before a wireless PED is approved for use.	**SOs, ITPMs** Component CISOs/ISSMs, ISSOs, S/NAs	1 @ 4.6.2.g
WCOM-16 4.6.2.h	SO and ITPMs shall maintain an up-to-date inventory of all wireless PEDs approved for use.	**SOs, ITPMs** SOs, ITPMs, Component CISOs/ISSMs, CIOs	1 @ 4.6.2.h

BLSR-# Hdbk Ref	Baseline Security Requirement (BLSR)	OPR Collateral Roles	Reference # @ Paragraph #
WCOM-17 4.6.2.i	ISSOs and S/NAs shall clear a wireless PED of all information before it is surplused or reused by another DHS individual, office, or Component. ISSOs and S/NAs shall follow approved procedures for sanitizing a wireless PED before it is disposed of, recycled, or returned to the owner or manufacturer.	**ISSOs, S/NAs** SOs, ITPMs, Component CISOs/ISSMs, DAAs	1 @ 4.6.2.i
WCOM-18 4.6.2.j	SOs shall obtain an approved waiver or exception from the CISO, as needed, for legacy wireless PED systems that are not compliant with DHS IT security policy.	**SOs** Component CISOs/ISSMs, ISSOs, S/NAs	1 @ 4.6.2.j
WCOM-19 4.6.2.j	SOs shall implement a migration plan that describes the provisions, procedures, and restrictions for transitioning noncompliant legacy wireless PEDs to DHS-compliant security architectures.	**SOs** Component CISOs/ISSMs, ISSOs, S/NAs	1 @ 4.6.2.j
WCOM-20 4.6.2.k	ISSOs shall implement controls to prevent the use of personally owned portable electronic devices (PEDs) for the processing, storage, or transmission of sensitive DHS information.	**ISSOs** SOs, S/NAs, Supervisors	1 @ 4.6.2.k 8 @Apx F, AC-20
WCOM-21 4.6.2.l	The DAA must approve the use of Government-owned PEDs before the PEDs can be used to process, store, or transmit sensitive DHS information.	**DAAs** Component CISOs/ISSMs, SOs, ISSOs, SSOs, Users	1 @ 4.6.2.l
WCOM-22 4.6.2.m	The DAA must approve the use of PED data-capture devices, such as cameras and recorders, before such devices can be used.	**DAAs** Component CISOs/ISSMs, ISSOs,	1 @ 4.6.2.m
WCOM-23 4.6.2.m	S/NAs and ISSOs shall implement controls to ensure that PED functions that can record or transmit information via video, IR, or RF are disabled in areas where sensitive information is discussed or located.	**S/NAs, ISSOs** SOs, Component CISOs/ISSMs, Users	1 @ 4.6.2.m

BLSR-# Hdbk Ref	Baseline Security Requirement (BLSR)	OPR Collateral Roles	Reference # @ Paragraph #
WCOM-24 4.6.2.1.a	Component CISOs/ISSMs shall develop guidance for discussing sensitive information on cellular phones.	**Component CISOs/ISSMs** SOs, CIOs	1 @ 4.6.2.1.a
WCOM-25 4.6.2.2.a	Component CISOs/ISSMs and ISSOs shall ensure that users are trained on proper use of pagers to ensure that pagers are not used to transmit sensitive information.	**Component CISOs/ISSMs, ISSOs** Supervisors, SSOs	1 @ 4.6.2.2.a
WCOM-26 4.6.2.3.a	S/NAs and ISSOs shall implement controls to ensure that all enabled functions on multifunctional wireless devices are encrypted using approved cryptographic modules.	**S/NAs, ISSOs** Supervisors, SSOs, Users	1 @ 4.6.2.3.a
WCOM-27 4.6.2.3.b	S/NAs and ISSOs shall implement controls to ensure that functions on multifunctional wireless devices that transmit or receive video, infrared (IR), or radio frequency (RF) signals are disabled in areas where sensitive information is discussed.	**S/NAs, ISSOs** SOs, Component CISOs/ISSMs, Users	1 @ 4.6.2.3.b
WCOM-28 4.6.2.3.c	Short Message Service (SMS) and Multimedia Messaging Service (MMS) shall not be used and shall be disabled when possible.		1 @ 4.6.2.3.c
WCOM-29 4.6.3.a	ISSOs, S/NAs, or users shall notify DAAs immediately when any security feature of a wireless tactical system is disabled due to time-sensitive, mission-critical incidents.	**ISSOs, S/NAs, Users** DAAs, Component CISOs/ISSMs, SOs	1 @ 4.6.3.a
WCOM-30 4.6.3.b	SOs and ITPMs shall ensure that wireless tactical systems implement strong identification, authentication, and encryption.	**SOs, ITPMs** Component CISOs/ISSMs, DAAs, ISSOs, S/NAs	1 @ 4.6.3.b
WCOM-31 4.6.3.c	SOs and ITPMs shall identify and establish cost-effective countermeasures to denial-of-service attacks prior to requesting approval of a wireless tactical system.	**SOs, ITPMs** Component CISOs/ISSMs, ISSOs, S/NAs	1 @ 4.6.3.c

BLSR-# Hdbk Ref	Baseline Security Requirement (BLSR)	OPR Collateral Roles	Reference # @ Paragraph #
WCOM-32 4.6.3.d	SOs and ITPMs shall maintain an up-to-date inventory of all approved wireless tactical systems.	**SOs, ITPMs** Component CISOs/ISSMs, ISSOs	1 @ 4.6.3.d
WCOM-33 4.6.3.e	SOs and Component CISOs/ISSMs shall implement a migration plan for noncompliant legacy wireless tactical systems that transitions these systems to a DHS-compliant security architecture. SOs and Component CISOs/ISSMs shall also obtain the necessary approved waiver or exception from the CISO, as appropriate. The plan shall describe the provisions, procedures, and restrictions for obtaining system compliance with DHS IT security policies.	**SOs, Component CISOs/ISSMs** ISSOs	1 @ 4.6.3.e
WCOM-34 4.6.3.f	ISSOs and S/NAs shall validate the security configuration of Land Mobile Radio (LMR) subscriber units via over-the-air-rekeying (OTAR) or hard rekey using a crypto-period no longer than 180 days.	**ISSOs, S/NAs** SOs, Component CISOs/ISSMs, DAAs	1 @ 4.6.3.f
WCOM-35 4.6.3.g	SOs and ITPMs shall ensure that all LMR systems comply with Project 25 (P25, EIA/TIA-102) security standards where applicable.	**SOs, ITPMs** DAAs, Component CISOs/ISSMs, ISSOs, S/NAs	1 @ 4.6.3.g
WCOM-36 4.6.4.a	Components implementing RFID systems shall assess hazards of electromagnetic radiation to fuel, ordinance, and personnel before deployment of the RFID technology.		1 @ 4.6.4.a
WCOM-37 4.6.4.b	Components shall 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.		1 @ 4.6.4.b
WCOM-38 4.6.4.c	Components 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.		1 @ 4.6.4.c
WCOM-39 4.6.4.d	Components 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 the Component's physical perimeter.		1 @ 4.6.4.d

BLSR-# Hdbk Ref	Baseline Security Requirement (BLSR)	OPR Collateral Roles	Reference # @ Paragraph #
WCOM-40 4.6.4.e	When the RFID system is connected to a DHS data network, Components shall implement network security controls to appropriately segregate RFID network components such as RFID readers, middleware, and databases from other non-RFID network hosts.		1 @ 4.6.4.e
WCOM-41 4.6.4.f	Components implementing RFID technology 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.		1 @ 4.6.4.f
OCOM-1 4.7.a	SOs shall implement controls to ensure that all overseas communications comply with the applicable provisions of Department of State Foreign Affairs Manual (FAM), 12 FAM 600, *Information Security Technology*.	**SOs** ISSOs, S/NAs, Users	1 @ 4.7.a
EQUIP-1 4.8.1.a	Components shall implement controls to ensure that all unattended workstations are either logged off, locked, or use a password-protected screensaver.	**ISSOs** SSOs, Users	1 @ 4.8.1.a
EQUIP-2 4.8.1.b	Components shall implement controls to ensure that all workstations are protected from theft.	**FMs** ISSOs, SSOs, Users	1 @ 4.8.1.b
EQUIP-3 4.8.2.a	Information stored on any laptop computer or other mobile computing device that may be used in a residence or on travel shall be encrypted using FIPS 140-2-approved encryption.	**S/NAs, ISSOs** Component CISOs/ISSMs	1 @ 4.8.2.a
EQUIP-4 4.8.2.a	ISSOs shall implement controls, including computer security awareness training, to ensure that users do not store passwords and smart cards on or with their laptop computers and other mobile computing devices.	**ISSOs** Component CISOs/ISSMs, SSOs, Users	1 @ 4.8.2.a
EQUIP-5 4.8.2.b	ISSOs shall implement controls, including computer security awareness training, to ensure that users secure unattended laptop computers and other mobile computing devices via a locking cable, a locked office, or a locked cabinet or desk.	**ISSOs** SSOs, Users	1 @ 4.8.2.b

BLSR-# Hdbk Ref	Baseline Security Requirement (BLSR)	OPR Collateral Roles	Reference # @ Paragraph #
EQUIP-6 4.8.2.c	ISSOs shall implement controls to ensure that employees obtain the written approval of the appropriate program official(s) before taking a laptop computers or other mobile computing device overseas.	**ISSOs** SOs, SSOs, Users	1 @ 4.8.2.c
EQUIP-7 4.8.3.a	ISSOs shall implement controls, including computer security awareness training, to ensure that personally owned equipment and software are not used to process, access, or store sensitive information unless the equipment has been explicitly approved by the appropriate DAA(s) for such use.	**ISSOs** DAAs	1 @ 4.8.3.a 8 @Apx F, AC-20
EQUIP-8 4.8.3.b	S/NAs and ISSOs shall implement controls to ensure that personally owned equipment and software are not connected to DHS equipment or networks without written approval from the Component ISSM.	**S/NAs, ISSOs** Component CISOs/ISSMs, Users	1 @ 4.8.3.b 8 @Apx F, AC-20
RM-7 4.8.4	ISSOs and S/NAs shall implement routine normal and preventive maintenance on their information system components as specified by manufacturer, vendor, and/or organizational requirements.	**ISSOs, S/NAs** SOs, ITPMs	1 @ 4.8.4 8 @Apx F: MA-2
RM-8 4.8.4	SOs and ITPMs shall approve, control, and monitor the use of information system maintenance tools and ensure the tools are maintained.	**SOs, ITPMs** ISSOs, S/NAs	1 @ 4.8.4 8 @Apx F: MA-3
CM-4 4.8.4.a	Components shall ensure that the installation of hardware and software meets requirements in the applicable DHS Hardening Guides.	**ISSOs, S/NA** SOs, ITPMs, Component CISOs/ISSMs	1 @ 4.8.4.a
ACC-4 4.8.4.b	Components shall implement controls to ensure that access to system and network software and hardware is restricted to authorized personnel.	**ITPMs, S/NAs** ISSOs, SSOs	1 @ 4.8.4.b 8 @Apx F: IA-2 & 4, MA-4 & 5, PE-2, PS-6

BLSR-# Hdbk Ref	Baseline Security Requirement (BLSR)	OPR Collateral Roles	Reference # @ Paragraph #
CM-5 4.8.4.c	Components shall test, authorize, and approve all new and revised software and hardware prior to implementation in accordance with the system's Configuration Management Plan.	**ITPMs** SOs, CIOs, ISSOs	1 @ 4.8.4.c 8 @Apx F: CM-3 & 4
RM-9 4.8.4.d	Components shall mitigate security risks through vulnerability testing, promptly installing patches, and eliminating or disabling unnecessary services.	**ITPMs, S/NAs** Component CISOs/ISSMs, ISSOs	1 @ 4.8.4.d
RM-10 4.8.4.e	ISSOs and S/NAs shall ensure that maintenance ports are enabled only during maintenance.	**ISSOs, S/NAs** COTRs	1 @ 4.8.4.e 8 @Apx F: MA-4
RM-11 4.8.5.a	SOs and ITPMs shall advise DHS users that they are permitted to use Government office equipment and/or DHS information systems/computers, including Internet and e-mail services, for authorized purposes only.	**SOs, ITPMs** ISSOs, SSOs, S/NAs	1 @ 4.8.5.a
RM-12 4.8.5.b	ISSOs shall, via Rules of Behavior and annual awareness training, advise users of their responsibilities when employing the e-mail and Internet limited-personal-use provisions found in DHS MD 4400.1 and 4500.1.	**ISSOs** SO, ITPMs, Component CISOs/ISSMs	1 @ 4.8.5.b
RM-13 4.8.5.c	ISSOs shall, via Rules of Behavior and annual awareness training, advise DHS users that they do not have any right to or expectation of privacy while using Government office equipment and/or DHS IT systems/computers, including Internet and e-mail services.	**ISSOs** DHS Employees & Contractors	1 @ 4.8.5.c
EQUIP-9 4.8.5.d	SOs and ITPMs shall ensure users know that the use of Government office equipment and DHS information systems/computers constitutes consent to monitoring and auditing of the equipment/systems at all times.	**SOs, ITPMs** SSOs, ISSOs, S/NAs	1 @ 4.8.5.d
ACC-5 4.8.5.e	SOs and S/NAs shall implement controls to ensure that DHS users sign Rules of Behavior prior to being granted access to DHS IT systems.	**SOs, S/NAs** ISSOs	1 @ 4.8.5.e 8 @Apx F, PL-4, PS-6

BLSR-# Hdbk Ref	Baseline Security Requirement (BLSR)	OPR Collateral Roles	Reference # @ Paragraph #
PERS-11 4.8.5.e	SOs shall create and employ a User Agreement that contains a "Consent to Monitor" provision and an acknowledgement that the user has no expectation of privacy.	**SOs** ISSOs, Supervisors	1 @ 4.8.5.e
CONT-6 4.8.5.f	ITPMs and Contracting Officers shall enforce limited-personal-use provisions for contractors authorized to use Government office equipment or information systems/computers if limited personal use is authorized by the contract or memorandum of agreement.	**ITPMs, KOs** SOs, ISSOs, S/NAs	1 @ 4.8.5.f
DCOM-9 4.12.a	ISSOs shall ensure that DHS security personnel, SOs, and users are made aware that the policies in the 4300A handbook, including certification and accreditation requirements, apply to any devices that contain information technology, including copiers, fax machines, and HVAC systems.	**ISSOs** SOs, S/NAs, FMs, SSOs, Users	1 @ 4.12.a
CIRP-1 4.9.a & Attachment F	Components shall establish and maintain a computer incident response capability for their Components.	**Component CISOs/ISSMs** CIOs, ISSOs, S/NAs	1 @ 4.9.a & Attachment F 2 @ §3544(a)(7) 3 @ 3a 2) d) 8 @Apx F: IR-4 & 7
CIRP-2 4.9.b & Attachment F	S/NAs, ISSOs, and Users shall report significant computer security incidents to the DHS Computer Security Incident Response Center (CSIRC) immediately upon identification and validation of incident occurrence in accordance with the procedures established in Attachment F, *Incident Response and Reporting*, to the DHS 4300A Sensitive Systems Handbook. Reportable incidents include incidents involving personally identifiable information in electronic or physical form and suspected as well as confirmed incidents.	**S/NAs, ISSOs, Users** Component CISOs/ISSMs, CIOs, SOs	1 @ 4.9.b & Attachment F 8 @Apx F: IR-6
CIRP-3 4.9.b & Attachment F	Component CSIRCs shall report significant computer security incidents to the DHS Computer Security Incident Response Center (CSIRC) immediately upon identification and validation of incident occurrence in accordance with the procedures established in Attachment F, *Incident Response and Reporting*, to the DHS 4300A Sensitive Systems Handbook.	**Component CSIRCs** Component CISOs/ISSMs, CIOs, SOs	1 @ 4.9.b & Attachment F

BLSR-# Hdbk Ref	Baseline Security Requirement (BLSR)	OPR Collateral Roles	Reference # @ Paragraph #
CIRP-4 4.9.c & Attachment F	DHS CSIRC shall report all incidents involving personally identifiable information to US-CERT within one hour of notification by a Component CSIRC. Reportable incidents include incidents involving personally identifiable information in electronic or physical form and suspected as well as confirmed incidents.		1 @ 4.9.c & Attachment F
CIRP-5 4.9.d & Attachment F	Component CSIRCs shall report both significant and minor incidents to the DHS CSIRC in a weekly incident report in accordance with the procedures established in Attachment F, *Incident Response and Reporting*, to the DHS 4300A Sensitive Systems Handbook.	**Component CSIRCs** Component CISOs/ISSMs, ISSOs, S/NAs, Users	1 @ 4.9.d & Attachment F
SDLC-31 4.10.a	Components shall ensure that security requirements for their sensitive systems are incorporated in the life-cycle documentation and that changes are documented throughout the life cycle of the system.	**SOs, ITPMs** Component CISOs/ISSMs, S/NAs, ISSOs	1 @ 4.10.a 8 @Apx F, SA-3
SDLC-32 4.11.a	Components shall 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.	**S/NAs** Component CISOs/ISSMs, ITPMs, SOs, ISSOs	1 @ 4.11.a 8 @Apx F, CP-9
I&A-1 5.1	SOs and ITPMs shall implement a system authentication mechanism that provides feedback to the user after a failed authentication but does not compromise the mechanism.	**SOs, ITPMs** ISSOs, S/NAs	1 @ 5.1 8 @Apx F: IA-6
I&A-2 5.1.a	Components shall control and limit user access based on positive user identification and authentication mechanisms that support the minimum requirements of access control, least privilege, and system integrity.	**S/NAs** SOs, ISSOs, Supervisors	1 @ 5.1.a 8 @Apx F, AC-3, IA-2 & 5
I&A-3 5.1.b	S/NAs shall ensure that each user is authenticated before IT system access occurs.	**S/NAs** ISSOs	1 @ 5.1.b 8 @Apx F, IA-2

BLSR-# Hdbk Ref	Baseline Security Requirement (BLSR)	OPR Collateral Roles	Reference # @ Paragraph #
I&A-4 5.1.c	For systems with low impact for the confidentiality security objective, Components shall disable user identifiers after 90 days of inactivity; for systems with moderate and high impacts for the confidentiality security objective, Components shall disable user identifiers after 30 days of inactivity.		1 @ 5.1.c
I&A-5 5.1.d	DHS users shall not share passwords or other authentication materials and shall not allow other persons to use their passwords or other authentication materials.	**Users** Supervisors, S/NAs, ISSOs	1 @ 5.1.d & 5.1.1.c 8 @Apx F: IA-5
I&A-6 5.1.e	ISSOs and S/NAs shall treat all user authentication materials as sensitive material.	**ISSOs, S/NAs** Component CISOs/ISSMs, SOs	1 @ 5.1.e
I&A-7 5.1.1.a	ISSOs shall determine and enforce measures to ensure strong passwords are used.	**ISSOs** S/NAs	1 @ 5.1.1.a
I&A-8 5.1.1.b	ISSOs shall establish and implement procedures to ensure that user passwords are changed at least every 180 days.	**ISSOs** Component CISOs/ISSMs, S/NAs, Users	1 @ 5.1.1.b
I&A-9 5.1.1.c	ISSOs and S/NAs shall enforce the policy that DHS users shall not share personal passwords.	**ISSOs, S/NAs** SOs, ITPMs, SSOs	1 @ 5.1.1.c
I&A-10 5.1.1.d	ITPMs and S/NAs shall implement controls to ensure that the use of group passwords is limited to situations dictated by operational necessity or critical for mission accomplishment and that approval for the use of group passwords has been granted by the appropriate DAA.	**ITPMs, S/NAs** Component CISOs/ISSMs, CIOs, COs, DAAs, SOs, ISSOs	1 @ 5.1.1.d
I&A-11 5.1.1.a	ISSOs and S/NAs shall implement controls to ensure that users employ passwords that meet the criteria outlined in Section 5.1.1.1 of the DHS 4300A Sensitive Systems Handbook.	**ISSOs, S/NAs** Users, Supervisors	7 @ 5.1.1.a

BLSR-# Hdbk Ref	Baseline Security Requirement (BLSR)	OPR Collateral Roles	Reference # @ Paragraph #
I&A-12 5.1.1.3	S/NAs shall ensure that system and network settings are configured to adhere to the password guidelines cited in Section 5.1.1.3 of the DHS 4300A Sensitive Systems Handbook.	**S/NAs** ISSOs, ITPMs, Component CISOs/ISSMs	7 @ 5.1.1
ACC-6 5.2	SOs and ITPMs shall implement and maintain system access control measures that prevent users from opening more than one personal active session on a DHS system unless explicitly authorized by the DAA.	**SOs, ITPMs** ISSOs, S/NAs	1 @ 5.2 8 @Apx F: AC-10
ACC-7 5.2.a	Components shall implement access control measures that provide protection from unauthorized alteration, loss, unavailability, or disclosure of information. This includes the requirement that no transactions may be performed on active DHS systems or those under development without an audit record leading to an authenticated user or administrator logon.	**SOs, ISSOs, ITPMs** S/NAs	1 @ 5.2.a 8 @Apx F, AC-1 & 3, AU-2, PE-2,
ACC-8 5.2.b	Components shall ensure that access privileges are granted based on the principles of least privilege and separation of duty.	**SOs, Supervisors** ISSOs, S/NAs, Users	1 @ 5.2.b 8 @Apx F, AC-3, 5, 6, & 13, PS-5 & 6
ACC-9 5.2.b	ISSOs and S/NAs shall implement controls to ensure that users adhere to access control requirements that specify the form and content of system identifiers, i.e., users' IDs and passwords.	**ISSOs, S/NAs** Users, Supervisors	1 @ 5.2.b 8 @Apx F, IA-2
ACC-10 5.2.c	Users shall not provide their password to anyone, including system administrators.		1 @ 5.2.c
ACC-11 5.2.1.a & b	Components shall implement and enforce an account lockout policy that limits the number of consecutive failed logon attempts to 3 and shall configure systems to lock a user's account for 20 minutes after 3 consecutive failed attempts.	**S/NAs** ISSOs	1 @ 5.2.1.a & b 8 @Apx F, AC-7
ACC-12 5.2.2.a	Components shall ensure that sessions on workstations, laptops, and PEDs are terminated after 20 minutes of inactivity.	**S/NAs** ISSOs	1 @ 5.2.2.a 8 @Apx F, AC-11 & 12, SC-10

BLSR-# Hdbk Ref	Baseline Security Requirement (BLSR)	OPR Collateral Roles	Reference # @ Paragraph #
ACC-13 5.2.3.a	S/NAs shall ensure that IT systems internal to a DHS network display the DHS sign-on warning banner or one approved by the CISO.	**S/NAs** CISO, ISSOs	1 @ 5.2.3.a 8 @Apx F, AC-8
ACC-14 5.2.3.b	ITPMs and S/NAs shall ensure that IT systems accessible to the public provide both a security and privacy statement at every entry point.	**ITPMs, S/NAs** ISSOs	1 @ 5.2.3.b 8 @Apx F, AC-8
AUDIT-1 5.3	Component CISOs/ISSMs and SOs shall ensure that audit collection and review procedures contain adequate separation of duties provisions and that auditing is performed independently from system/network administration.	**Component CISOs/ISSMs, SOs** ITPMs, S/NAs, ISSOs, Supervisors	1 @ 5.3
AUDIT-2 5.3	Component CISOs/ISSMs will work with SOs and ITPMs to establish, maintain, and enforce a baseline set of transactions that must be audited within, by, or from each DHS system.	**Component CISOs/ISSMs, SOs, ITPMs** ISSOs, S/NAs	1 @ 5.3 8 @Apx F: AU-2
AUDIT-3 5.3.a	S/NAs shall ensure that audit records contain the information needed to reconstruct security-relevant events.	**S/NAs** ISSOs	1 @ 5.3.a 8 @Apx F, AU-3
AUDIT-4 5.3.a	ISSOs shall review audit records as specified in the IT System Security Plan and report security-relevant events to the Component CSIRC.	**ISSOs** Component CISOs/ISSMs, SOs, S/NAs	1 @ 5.3.a 8 @Apx F, AU-6
AUDIT-5 5.3.a	S/NAs shall ensure that audit records contain the identity of each user and device accessing or attempting to access an IT system.	**S/NAs** ISSOs	1 @ 5.3.a 8 @Apx F, AU-3
AUDIT-6 5.3.a	S/NAs shall ensure that audit records contain the time and date of the access and the logoff.	**S/NAs** ISSOs	1 @ 5.3.a 8 @Apx F, AU-3
AUDIT-7 5.3.a	S/NAs shall ensure that audit records contain the activities that might modify, bypass, or negate IT security safeguards, including all activities performed using an administrator's identity.	**S/NAs** ISSOs	1 @ 5.3.a 8 @Apx F, AU-2 & 3

BLSR-# Hdbk Ref	Baseline Security Requirement (BLSR)	OPR Collateral Roles	Reference # @ Paragraph #
AUDIT-8 5.3.a	S/NAs shall ensure that audit records contain security-relevant actions associated with processing.	**S/NAs** ISSOs	1 @ 5.3.a 8 @Apx F, AU-2 & 3
AUDIT-9 5.3.b	Components shall ensure that their audit records and audit logs are protected from unauthorized modification, access, or destruction.	**S/NAs** ISSOs	1 @ 5.3.b 8 @Apx F, AU-9
AUDIT-10 5.3.c	Components shall ensure that audit logs are recorded and retained in accordance with the Component's Record Schedule or the DHS Records Schedule. At a minimum audit trail records shall be maintained online for at least 90 days.	**S/NAs** ISSOs	1 @ 5.3.c 8 @Apx F, AU-4 & 11
AUDIT-11 5.3.b & c	S/NAs shall ensure that audit records are adequately backed up in accordance with the system's contingency plan.	**S/NAs** ISSOs	1 @ 5.3.b & c 8 @Apx F, AU-9 & 11, CP-6
AUDIT-12 5.3.d	Components shall evaluate the system risks associated with extracts of personally identifiable information from databases and, if the risk is determined to be sufficiently high, a procedure shall be developed for logging computer-readable data extracts. If it is determined that logging these extracts is not possible, this determination shall be documented, and compensating controls shall be identified.		1 @ 5.3.d
AUDIT-13 5.3.e	Computer-readable data extracts involving personally identifiable information shall be erased within 90 days unless the information included in the extracts is required beyond the 90 days; erasure of the extracts or the need for continued use of the data shall be documented.		1 @ 5.3.e
NWS-1 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 DHS networks; data communication connections are not allowed unless they have been authorized by the Component ISSM.		1 @ 5.4.1.a

BLSR-# Hdbk Ref	Baseline Security Requirement (BLSR)	OPR Collateral Roles	Reference # @ Paragraph #
NWS-2 5.4.1.b	Components shall ensure 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. Strong authentication for remote access should consider two-factor authentication, where one of the factors is provided by a device separate from the device gaining access.	**ISSOs, S/NAs** Component CISOs/ISSMs, CIOs, SOs, Supervisors	1 @ 5.4.1.b 8 @Apx F, AC-17
NWS-3 5.4.1.c	The Risk Assessment and System Security Plan shall document any remote access of personally identifiable information, and the remote access shall be approved by the DAA prior to implementation.		1 @ 5.4.1.c
NWS-4 5.4.1.d	Remote access of personally identifiable information shall comply with all DHS requirements for sensitive systems, including strong authentication. Strong authentication shall be accomplished via virtual private network (VPN) or equivalent encryption (e.g., https) and two-factor authentication. Any two-factor authentication shall be based on agency-controlled certificates or hardware tokens issued directly to each authorized user		1 @ 5.4.1.d
NWS-5 5.4.1.e	Remote access of personally identifiable information 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 System Security Plan		1 @ 5.4.1.e
VIRUS-1 5.4.1.b	Components shall implement controls to ensure that equipment employed by users to gain remote access is protected from malicious code and that protection software is kept current.	**ISSOs, S/NAs** Supervisors, Users	1 @ 5.4.1.b 8 @Apx F, AC-17, SI-3
NWS-6 5.4.2.a	Components shall establish and implement a security operations capability to monitor their networks for security events.	**Component CISOs/ISSMs, Component Security Operations** CISO, CIOs, S/NAs, ISSOs	1 @ 5.4.2.a 8 @Apx F: SC-7

BLSR-# Hdbk Ref	Baseline Security Requirement (BLSR)	OPR Collateral Roles	Reference # @ Paragraph #
NWS-7 5.4.2.b	Component CISOs/ISSMs, ISSOs, and S/NAs shall respond to intrusion alerts, participate in CSIRC-led incident response investigations, evaluate the impact of the event on the system, and implement necessary corrections in accordance with Attachment F of the DHS 4300A Sensitive Systems Handbook.	**Component CISOs/ISSMs, ISSOs, S/NAs** CISO (Security Operations), CIOs	1 @ 5.4.2.b 7 @ 5.4.2.5, Attachment F 8 @Apx F: IR-1, 4, & 6
NWS-8 5.4.3.a	Components shall implement identification and authentication controls, audit logging, and integrity controls on every network component.	**Component CISOs/ISSMs, ISSOs, S/NAs** ITPMs	1 @ 5.4.3.a 8 @Apx F, AU-2, SC-7
NWS-9 5.4.3.b	DAAs shall ensure that interconnections between sensitive IT systems and IT systems not controlled by DHS are established through controlled interfaces.	**DAAs** COs, Component CISOs/ISSMs, ISSOs, SOs, S/NAs	1 @ 5.4.3.b 8 @Apx F, CA-3, SC-7
NWS-10 5.4.3.b	DAAs shall ensure that system interconnections are accredited at the highest security level of information on the network.	**DAAs** COs, Component CISOs/ISSMs, ISSOs, SOs, S/NAs	1 @ 5.4.3.b
NWS-11 5.4.3.c	Components shall document interconnections with other external networks with an Interconnection Security Agreement (ISA). Interconnections between DHS Components shall require an ISA when there is a difference in the security categorizations for confidentiality, integrity, and availability for the two networks. ISAs shall be signed by both DAAs or by the official designated by the DAA to have signatory authority.	**DAAs** COs, Component CISOs/ISSMs, ISSOs, SOs, S/NAs	1 @ 5.4.3.c 8 @Apx F: CA-3
NWS-12 5.4.3.c	DAAs shall ensure the format and content of the ISA comply with Section 5.4.3.1 and Attachment N of the DHS 4300A Sensitive Systems Handbook.	**DAAs** COs, Component CISOs/ISSMs, ISSOs, SOs, S/NAs	7 @ 5.4.3.2 8 @Apx F, CA-3

BLSR-# Hdbk Ref	Baseline Security Requirement (BLSR)	OPR Collateral Roles	Reference # @ Paragraph #
NWS-13 5.4.3.d	DAAS shall ensure that ISAs are reissued every three years or whenever any significant changes have been made to any of the interconnected systems.	**DAAs** SOs, Component CISOs/ISSMs, ISSOs	1 @ 5.4.3.d
NWS-14 5.4.3.e	ISSOs shall review their systems' ISAs and recommend changes, if needed, to the DAA as part of the annual FISMA self-assessment	**ISSOs** DAAs, SOs, Component CISOs/ISSMs	1 @ 5.4.3.e
NWS-15 5.4.4.a	Components shall restrict physical access to firewalls to authorized personnel.	**S/NAs** SOs, SSOs, ISSOs	1 @ 5.4.4.a
NWS-16 5.4.4.b	Components shall implement strong identification and authentication for personnel authorized to administer firewalls.	**ISSOs, S/NAs** ITPMs, Component CISOs/ISSMs	1 @ 5.4.4.b
NWS-17 5.4.4.c	Components shall ensure that remote maintenance paths to firewalls are encrypted.	**ISSOs, S/NAs** ITPMs, Component CISOs/ISSMs	1 @ 5.4.4.c 8 @Apx F: MA-4
NWS-18 5.4.4.d	Components shall conduct testing at least quarterly to ensure that firewall configurations are correct.	**ISSOs, S/NAs** ITPMs, Component CISOs/ISSMs	1 @ 5.4.4.d
NWS-19 5.4.4.e	Component SOCs/CSIRCs shall submit reports, as required, on security operations status and incident reporting to the CISO Security Operations Program Director.	**SOCs, CSIRCs** CIO, CISO, Component CISOs/ISSMs	1 @ 5.4.4.e
NWS-20 5.4.5.a	DAAs shall ensure that any direct connection of DHS networks to the Internet or to extranets occurs through firewalls that have been certified and accredited.	**DAAs** COs, ISSOs, S/NAs	1 @ 5.4.5.a 8 @Apx F: SC-7

BLSR-# Hdbk Ref	Baseline Security Requirement (BLSR)	OPR Collateral Roles	Reference # @ Paragraph #
NWS-21 5.4.5.b	S/NAs shall ensure that firewalls are configured to prohibit any protocol or service that is not explicitly permitted.	**S/NAs** ISSOs, ITPMs	1 @ 5.4.5
NWS-22 5.4.5.c	Component CISOs/ISSMs shall centrally manage dial-up connections.	**Component CISOs/ISSMs** ISSOs, S/NAs, SOs	1 @ 5.4.5.c
NWS-23 5.4.5.d	ISSOs and S/NAs 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 DHS environment. [Note: When the technology becomes available and code can be vetted for security, the requirement will be "Ensure that all approved code, including mobile code (e.g., ActiveX, JavaScript), is digitally signed by the designated DHS authority and that only signed code is allowed to execute on DHS IT systems.]	**ISSOs, S/NAs** DAAs, Component CISOs/ISSMs, SOs	1 @ 5.4.5
NWS-24 5.4.5.e & f	ISSOs and S/NAs shall ensure that telnet and the File Transfer Protocol (FTP) are not used to connect to or from any DHS computer.	**ISSOs, S/NAs** Component CISOs/ISSMs, SOs, ITPMs	1 @ 5.4.5.e & f
NWS-25 5.4.6.a	Components shall provide security for their e-mail systems and e-mail clients by correctly securing, installing, and configuring the underlying operating system.	**S/NAs** ISSOs, ITPMs	1 @ 5.4.6.a
NWS-26 5.4.6.b	Components shall provide security for their e-mail systems and e-mail clients by correctly securing, installing, and configuring mail server software.	**S/NAs** ISSOs, ITPMs	1 @ 5.4.6.b
NWS-27 5.4.6.c	Components shall provide security for their e-mail systems and e-mail clients by securing and filtering e-mail content.	**S/NAs** ISSOs, ITPMs	1 @ 5.4.6.c
NWS-28 5.4.6.d	Components shall provide security for their e-mail systems and e-mail clients by deploying network protection mechanisms such as firewalls, routers, switches, and intrusion detection systems.	**S/NAs** ISSOs, ITPMs	1 @ 5.4.6.d

BLSR-# Hdbk Ref	Baseline Security Requirement (BLSR)	OPR Collateral Roles	Reference # @ Paragraph #
NWS-29 5.4.6.e, f	Components shall provide security for their e-mail systems and e-mail clients by (1) securing e-mail clients and (2) administering the mail server in a secure manner, to include performing regular backups and updating software.	**S/NAs** ISSOs, ITPMs	1 @ 5.4.6.e & f
NWS-30 5.4.6.f	Components shall perform periodic security testing of e-mail servers and review audit logs at least weekly.	**ISSOs** S/NAs, Component CISOs/ISSMs, ITPMs	1 @ 5.4.6.f
NWS-31 5.4.7.a	S/NAs and Supervisors shall ensure technical and operational controls are in place and properly functioning to prohibit and/or deter the transmission of sensitive DHS information to personal e-mail accounts.	**S/NAs, Supervisors** ISSOs, Component CISOs/ISSMs, ITPMs, Users	1 @ 5.4.7.a
NWS-32 5.4.8.a	Component CISOs/ISSMs shall conduct vulnerability assessments and/or testing on IT systems containing sensitive information on a yearly basis or when significant changes are made to the IT systems; this should include scanning for unauthorized wireless devices. These tasks shall include the use of POA&Ms, if needed.	**Component CISOs/ISSMs** SOC, S/NAs, ITPMs, ISSOs	1 @ 5.4.8.a 8 @Apx F, CA-2 & 5
NWS-33 5.4.8.b	Component CISOs/ISSMs shall 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 SDLC support.	**Component CISOs/ISSMs** ISSOs, CSIRCs	1 @ 5.4.8.b
NWS-34 5.4.8.c	Component CISOs/ISSMs shall ensure coordination among the DHS CSIRC, the Component CSIRC, and the Information Security Vulnerability Management (ISVM) Program when vulnerability assessments encompass more than one Component.	**Component CISOs/ISSMs** ISSOs, CSIRCs	1 @ 5.4.8.c
NWS-35 5.4.9.a	S/NAs and Supervisors shall ensure technical and operational controls are in place and properly functioning to prohibit and/or deter the use of peer-to-peer software on DHS computers.	**S/NAs, Supervisors** ISSOs, Component CISOs/ISSMs, ITPMs, Users	1 @ 5.4.9.a

BLSR-# Hdbk Ref	Baseline Security Requirement (BLSR)	OPR Collateral Roles	Reference # @ Paragraph #
CRYPTO-1 5.5.1.a	SOs and ITPMs shall determine the level of protection required and the need for encryption of sensitive information processed by IT systems based on a risk assessment.	**SOs, ITPMs** Component CISOs/ISSMs, ISSOs	1 @ 5.5.1.a
CRYPTO-2 5.5.1.a & b	ITPMs and SOs shall develop implement, and maintain encryption plans and, if authorized, provide the capability to encrypt sensitive information using DHS-approved encryption methods.	**ITPMs, SOs** Component CISOs/ISSMs, ISSOs, S/NAs, SOs	1 @ 5.5.1.a & b 8 @Apx F: SC-13
CRYPTO-3 5.5.2.a	The CISO shall serve as the PKI Policy Authority (PKI PA) to perform DHS-level PKI oversight.	**CISO** Component CISOs/ISSMs, ISSOs, S/NAs	1 @ 5.5.2.a
CRYPTO-4 5.5.2.b	The PKI PA shall appoint a PKI Operational Authority (PKI OA).	**PKI PA** Component CISOs/ISSMs, SOs	1 @ 5.5.2.b
CRYPTO-5 5.5.2.c	The CISO and Component CISOs/ISSMs shall ensure that the DHS PKI operates under an X.509 Certificate Policy (CP) that is approved by the PKI PA.	**CISO, Component CISOs/ISSMs** PKI PA, SOs	1 @ 5.5.2.c
CRYPTO-6 5.5.2.d	The CISO shall ensure that the DHS CP complies with the U.S. Federal PKI CP for the Federal Bridge Certificate Authority (CA) at all assurance levels: basic, medium, and high.	**CISO** PKI PA, Component CISOs/ISSMs, SOs	1 @ 5.5.2.d
CRYPTO-7 5.5.2.e	The CISO shall establish and maintain a single DHS high-assurance root CA. Additional DHS CAs shall be subordinate to the DHS root CA.	**CISO** PKI OA, Component CISOs/ISSMs, SOs	1 @ 5.5.2.e
CRYPTO-8 5.5.2.f	The CISO shall ensure that the DHS root CA is cross-certified with the Federal Bridge at the basic, medium, and high assurance levels.	**CISO** PKI OA, Component CISOs/ISSMs, SOs	1 @ 5.5.2.f

BLSR-# Hdbk Ref	Baseline Security Requirement (BLSR)	OPR Collateral Roles	Reference # @ Paragraph #
CRYPTO-9 5.5.2.g	The CISO and Component CISOs/ISSMs shall ensure that every DHS CA operates under an X.509 Certificate Practices Statement (CPS) that complies with the DHS CP and is approved by the PKI PA.	**CISO, Component CISOs/ISSMs** PKI PA, SOs	1 @ 5.5.2.g
CRYPTO-10 5.5.2.h	The CISO shall appoint PKI auditors to ensure that all CAs undergo an annual compliance audit.	**CISO** PKI OA, SOs, Component CISOs/ISSMs	1 @ 5.5.2.h
CRYPTO-11 5.5.2.i	The CISO shall ensure the creation and maintenance of secure, dedicated primary and backup CA sites to ensure continuity of PKI operations.	**CISO** PKI OA, Component CISOs/ISSMs, SOs	1 @ 5.5.2.i
CRYPTO-12 5.5.2.j	The CISO shall ensure the establishment and use of a DHS archive facility for PKI records.	**CISO** PKI OA, Component CISOs/ISSMs, SOs	1 @ 5.5.2.j
CRYPTO-13 5.5.2.k	ITPMs, ISSOs, and S/NAs shall not use a PKI certificate from any test, pilot, third party, or other CA to protect sensitive DHS data or to authenticate to DHS operational systems containing sensitive data.	**ITPMs, ISSOs, S/NAs** PKI OA, Component CISOs/ISSMs, SOs	1 @ 5.5.2.k
CRYPTO-14 5.5.3.a	The CISO and Component CISOs/ISSMs shall ensure that separate public/private key pairs are used for encryption and digital signature by human, organization, application, and code-signing subscribers.	**CISO, Component CISOs/ISSMs** PKI OA, SOs	1 @ 5.5.3.a
CRYPTO-15 5.5.3.b	ISSOs and S/NAs shall ensure that device (e.g., server) subscribers use separate public/private key pairs for encryption whenever native device protocols support separate public/private key pairs.	**ISSOs, S/NAs** Component CISOs/ISSMs, SOs, ITPMs	1 @ 5.5.3.b

BLSR-# Hdbk Ref	Baseline Security Requirement (BLSR)	OPR Collateral Roles	Reference # @ Paragraph #
CRYPTO-16 5.5.3.c	PKI Registration Authorities shall ensure that a human sponsor represents an organization, application, code-signing, or device subscriber when it applies for one or more certificates from a DHS CA.	**PKI Registration Authorities** ISSOs, S/NAs	1 @ 5.5.3.c
CRYPTO-17 5.5.3.d	The PKI PA and OA will ensure implementation of a DHS CA process that enables PKI registrars to determine the eligibility of each proposed human, organization, application, code signer, or device to receive one or more certificates.	**PKI PA, PKI OA** PKI Registration Authorities	1 @ 5.5.3.d
CRYPTO-18 5.5.3.e	The PKI PA and OA will implement a process that enables PKI Registration Authorities to determine the authorized human sponsor for each nonhuman subscriber for which a PKI certificate is issued.	**PKI PA, PKI OA** PKI Registration Authorities	1 @ 5.5.3.e
CRYPTO-19 5.5.3.f	The CISO and Component CISOs/ISSMs shall implement controls that hold each human PKI subscriber accountable for all transactions signed with the subscriber's private keys.	**CISO, Component CISOs/ISSMs** ISSOs, Users	1 @ 5.5.3.f
CRYPTO-20 5.5.3.g	The CISO and Component CISOs/ISSMs shall implement controls that hold the sponsor of each nonhuman PKI subscriber responsible for the security and use of the subscriber's private keys.	**CISO, Component CISOs/ISSMs** PKI Sponsor	1 @ 5.5.3.g
CRYPTO-21 5.5.3.h	PKI Registration Authorities shall implement controls to ensure that only authorized persons use the private key of a nonhuman subscriber, and auditable records show each person's use.	**PKI Registration Authorities**	1 @ 5.5.3.h
CRYPTO-22 5.5.3.i	PKI Registration Authorities shall obtain a signed DHS PKI Subscriber Agreement for Human Users from every human subscriber as a pre-condition for providing DHS CA PKI certificates.	**PKI Registration Authorities** Users	1 @ 5.5.3.i
CRYPTO-23 5.5.3.j	PKI Registration Authorities shall obtain a signed DHS PKI Subscriber Agreement for Sponsors from the authorized human sponsor of every nonhuman subscriber as a pre-condition for providing DHS CA PKI certificates.	**PKI Registration Authorities** PKI Sponsors	1 @ 5.5.3.j

BLSR-# Hdbk Ref	Baseline Security Requirement (BLSR)	OPR Collateral Roles	Reference # @ Paragraph #
VIRUS-2 5.6.a	Component CISOs/ISSMs shall establish and enforce virus protection control policy.	**Component CISOs/ISSMs** SOs, ISSOs, Users	1 @ 5.6.a
VIRUS-3 5.6.b	S/NAs shall ensure that antivirus software is installed on desktops and servers and is configured to check all files, downloads, and e-mail.	**S/NAs** ISSOs, Supervisors, Users	1 @ 5.6.b
VIRUS-4 5.6.b	S/NAs shall ensure that updates to antivirus software and signature files are installed on desktops and servers in a timely and expeditious manner without requiring the end user to request the update.	**S/NAs** ISSOs, Supervisors, Users	1 @ 5.6.b
VIRUS-5 5.6.b	S/NAs shall ensure security patches to desktops and servers are tested and installed in a timely and expeditious manner.	**S/NAs** ISSOs, Supervisors, Users	1 @ 5.6.b
VIRUS-6 5.6.c	S/NAs shall implement appropriate file/protocol/content filtering to protect their data and networks.	**S/NAs** ISSOs, SOs	1 @ 5.6.c
PA-1 5.7.a	SOs and ITPMs shall ensure that Information Assurance (IA) is a requirement for all systems that enter, process, store, display, or transmit sensitive or National Security information.	**SOs, ITPMs** CIOs, Component CISOs/ISSMs, DAAs, COs, S/NAs, ISSOs, Supervisors, Users	1 @ 5.7.a
PA-2 5.7.a&b	Information Assurance (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.	**SOs, ITPMs** IOs, Component CISOs/ISSMs, KOs, S/NAs, ISSOs	1 @ 5.7.a&b

BLSR-# **Hdbk Ref**	**Baseline Security Requirement (BLSR)**	**OPR** Collateral Roles	**Reference # @** **Paragraph #**
PA-3 5.7.c	SOs and ITPMs shall ensure that the evaluation and validation of COTS IA and IA-enabled IT products are conducted by accredited commercial laboratories or by NIST.	**SOs, ITPMs** CIOs, Component CISOs/ISSMs, KOs, S/NAs, ISSOs	1 @ 5.7.c
CRYPTO-24 5.7.d	ITPMs and S/NAs shall ensure that only cryptographic modules that have been validated in accordance with FIPS 140-2 are used.	**ITPMs, S/NAs** Component CISOs/ISSMs, ISSOs	1 @ 5.7.d 8 @Apx F: IA-7