TRANSPORTATION SECURITY ADMINISTRATION
INFORMATION TECHNOLOGY
INFORMATION ASSURANCE AND CYBERSECURITY DIVISION

TSA Information Assurance Handbook

Attachment 1 to TSA MD 1400.3 IT Security

Date Signed: 07/27/2018

Paul D. Morris (Executive Director, CISO)

Version 14.0

Records Disposition Schedule (RDS)
Policy Records Code and Item: 2000.4.1
PERMANENT: Cut off at the end of calendar year in which superseded or obsolete. Transfer to NARA 10 years after cut off. [Authority N1-560-04-10, Item 5b]

This Page Intentionally Left Blank

Table of Contents

1. Purpose

This handbook implements the policies and requirements of the Transportation Security Administration (TSA) Management Directive (MD) 1400.3, *Information Technology Security* by establishing guidance applicable to the use, development, and maintenance of TSA Information Technology (IT) assets, networks, and systems. The guidance contained herein is designed to ensure the Confidentiality, Integrity, Availability, and overall assurance of TSA information. This handbook is supplemented by published extension documents, TSA Technical Standards (TSs), and Standard Operating Procedures (SOPs). The IA HB, TSs, SOPs and other relevant documents are published in the IA Policy Outreach page. This document is used to identify responsibilities by educating and increasing awareness of TSA information assurance (IA) policy. An accountability matrix containing roles and responsibilities of key personnel mentioned in this Handbook can be found in an *Information Assurance (IA) Roles and Responsibilities* spreadsheet located in our IA Policy Outreach site. References to the specific areas and authorities to enable successful execution of tasks and job requirements are identified herein. ***Appendix A*** (References) located in the back of this Handbook contains a Figure 1 diagram, which illustrates a top-down approval and alignment order as derived IAW federal policy mandates.

2. Scope

The policies within this handbook apply to all TSA employees, contractors, vendors, detailees, others working on behalf of TSA, and to non-TSA individuals authorized to access TSA information systems, software and/or applications. It also applies to all TSA information systems, software and/or applications that collect, generate, process, store, display, transmit, or receive TSA data, including prototypes and telecommunications systems, in all phases of the Systems Engineering Life Cycle (SELC) unless an approved waiver has been granted using the proper waiver form. The above assets shall be collectively referred to as "IT assets" throughout the document. As required by the Department of Homeland Security (DHS), the Federal Chief Information Officer (CIO) and Office of Management and Budget (OMB) guidance, program and project managers shall be provided with guidance to support the implementation of **Agile Information Technology (IT) Development.** Requirements shall reference the ***DHS "Carwash" User Guide*****,** the **DHS Directive System Instruction Number 102-01-004: *Agile Development and Delivery for Information Technology*** and the **DHS *Agile Center of Excellence - Tools***. These guides enhance understanding as to why Agile is a preferred approach to federal IT development, how it provides a starting point for increasing DHS-wide application of *Agile* methodologies, and helps managers and other key stakeholders identify options for tailoring the SELC for Agile. The private sector uses Agile as an effective and efficient method to deliver software faster, better, and cheaper compared to other methods. **Important note for System Owners (SOs) and Information Systems Security Officers (ISSOs) – In the context of this IA Handbook, the term "*System*" is synonymous with "*Application*" and "*Software*", and the expectation for adherence is the same.**

The structure of this document is based on the controls contained in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations.* Information on privacy controls and related privacy overlays can be found **here**. Furthermore, the controls identified are mapped to Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of*

Federal Information and Information Systems, which establishes the foundation for categorizing systems based on three security objectives: Confidentiality, Integrity, and Availability (C, I, A). These publications, and other relevant NIST guidance, are available online at http://csrc.nist.gov/. Security objectives are assigned a potential impact level, also known as "impact level" throughout this handbook, of Low, Moderate, or High. Within the tables of requirements in this document, the applicability of each control statement is provided in the "Category" column with the following abbreviations: Low (L), Moderate (M), High (H), Privacy System (P), or Chief Financial Officer (CFO) Designated Financial System (F).

Definitions for terms are located in Section 5 *Definitions.* For definitions not identified, the NIST Glossary of Key Information Security Terms shall be used as a baseline for reference.

The DHS Sensitive Systems Policy Directive 4300A, and its supporting Handbook, shall take precedence in instances where there is conflict with TSA MD 1400.3 ITS and this supporting handbook, unless otherwise identified in TSA policy.

With the DHS Trusted Internet Connection (TIC) infrastructure initiative as mandated by OMB M-08-05, this TSA IA Handbook and its extension documents shall address the expansion in scope from a current TSA-only management service function to a DHS entity entrusted in providing a more centrally managed Semi-Trusted/DMZ environment. The overall purpose of the DHS TIC effort is to optimize and standardize the security of individual external network connections (extranet services) currently in use by the TSA and other agencies.

Regarding vulnerabilities, weaknesses and mitigations, POA&Ms shall not exceed the maximum duration for closure based on FIPS 199 impact levels for the system: 45 days (for *high*), 60 days (for *moderate*), and 90 days (for *low*). NOTE: Based on directions from the **DHS USM Memo titled "Strengthening DHS Cyber Defenses" (July 22, 2015)**, a unique type of "*High*" impact level category classified as "*Critical*" may be used under certain circumstances and in response to escalation in cyber related attacks. Weaknesses or vulnerabilities identified as *Critical* by the National Cybersecurity Assessment and Technical Services (NCATS) must be mitigated within **30 days**. This newly created *Critical* impact is also supported by the Binding Operational Directive (BOD) 15-01: "Critical Vulnerability Mitigation Requirement for Federal Civilian Executive Branch Departments' and Agencies' Internet-Accessible Systems". In these special cases, subsequent instructions shall be forthcoming by the TSA Authorizing Official (AO). Those systems not in compliance with this 30-day mitigation requirement risks being shut down or removed from the network at the discretion of the AO.

The CISO has the flexibility and the resources to work with DHS with the presumption that TSA has the full and complete trust in DHS from an architectural perspective to serve as the provider and management of TSA's current Semi-Trusted zone. Additional details may be found in the *TSA TIC Migration Plan of Action and Milestones Agreement and Approval* document, dated August 31, 2011, under *VPN Service* (p. 7) in that, "DHS OneNet network infrastructure is a Department managed service to the DHS Component and should be considered trusted."

In cases where current TSA policy is conflicting, the policy identified in this Handbook shall take precedence. The TSA Chief Information Security Officer (CISO) shall make the final arbitration decision in the case of any conflicting guidance in policy documents. In addition, in cases where this handbook conflicts with SSI Program Office or Privacy Office policy and procedures, the appropriate SSI and Privacy office's guidance shall take precedence.

3. Policy

3.1 Access Control (AC)

The implementation of proper access control is a critical element of the information assurance (IA) solution. TSA and DHS-trusted IT related assets provide an environment that allows active network use by authorized individuals in the performance of their assigned tasks, while also ensuring appropriate measures are in place to maintain the integrity of network information through limited and controlled access. This control supports the logical access control measures of TSA and DHS-trusted IT assets, and is applicable to all TSA IT assets whenever a claim of identity is made. Where applicable, specific detailed guidance of the information security requirements on access control is contained in several TSs including: TS-001 *Passwords/PINs*, TS-002 *Encryption*, TS-003 *Wi-Fi*, TS-008 *End User Assets*, TS-010 *Network Interconnections*, TS-012 *Port Security*, TS-015 *Network Logical Access Control*, TS-016 *Remote Access*, TS-023 *Voice over Internet Protocol (VOIP)*, TS-024 *Radio Frequency Identification (RFID*), TS-025 *Virtual Private Networks (VPNs*), TS-028 *Web Applications*, TS-030 *Internet Site Access*, TS-036 *Infrastructure Asset Security*, TS-037 *Server Security* and TS-049 *Information Systems Logging.*

Other guidance: OMB Memorandum 04-04, 08-05, and 08-27; FIPS Publications 140-2, 199, and 201; NIST Special Publications 800-12, 800-16, 800-46, 800-48, 800-63, 800-73, 800-77, 800-78, 800-98, 800-94, 800-100, 800-113, 800-114, 800-121, and 800-124.

3.1.1 Access Control Policy and Procedures (AC-1)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
1.1.1	The CISO shall develop, disseminate, and annually review/update a formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, and coordination among TSA and DHS trusted entities. The CISO shall also ensure documented procedures are established at the system level and each system needs to develop their own procedures in order to facilitate the implementation of access control policies and associated controls that provide protection from unauthorized alteration, loss, unavailability, or disclosure of information.	5.2.a 5.4.3.a	AC-1	LMH F
1.1.2	The System Owner (SO) shall be responsible for the management of access controls for IT assets for the information system, including oversight and agreements as needed for IT assets outside of direct control by TSA personnel.	5.2.a 5.4.3.a	AC-1 AC-2	LMH F

1.1.3	For the purpose of maintenance, a cleared and authorized vendor/ individual shall sign-in, provide credentials, and be escorted for access to a designated area for the purpose of maintaining TSA or DHS equipment; an authorized federal manager or designee with knowledge of the maintenance task shall be present to escort and monitor the individual at all times.	1.4.25 4.8.3.h 5.2.a 5.4.3.a	AC-1	LMH F
1.1.4	Reserved			
1.1.5	All privileged access control shall be in compliance with the TSA policy.	5.2.a 5.4.3.a	AC-1	LMH F
1.1.6	In the very rare instance where emergency access is needed to an account by an authorized individual other than the account owner, this shall be strictly controlled and approved by the CISO, Deputy CISO, or other designee prior to being granted. This type of access is normally on a temporary basis and whose time frame is determined by the authorized individual or designee.	5.2.a 5.2.d 5.4.3.a	AC-1 AC-2	LMH F
1.1.7	The ISSO shall provide on-going supervision and review of the actions of personnel who enforce access controls and those who are subject to this enforcement.	5.2.a 5.4.3.a	AC-1	LMH F
1.1.8	The ISSO shall ensure the SOC routinely reviews activity logs for signs of inappropriate actions and response action shall be taken as required.	5.2.a 5.4.3.a	AC-1	LMH F
1.1.9	Changes to user access rights shall be regularly reviewed, at least quarterly, by the user's supervisor independent of the information security function.	5.2.a 5.4.3.a	AC-1	LMH F
1.1.10	The user's supervisor shall notify the system ISSO of any abnormal activity and support investigation activities upon request.	5.2.a 5.4.3.a	AC-1	LMH F

3.1.2 Account Management (AC-2)

General user accounts are established by the TSA after the completion of the TSA Form 1403, *Computer and Personal Electronic Device Access Agreement (CAA),* available via the Online Learning Center (OLC). The data and applications available to the specific user are defined by an evaluation of that user's needs to perform his or her duties. A properly completed TSA Form 1403 is used to identify the user and the user's privileges, in order to create a profile. Account management is a critical element in the defense-in-depth approach and provides protection from unauthorized system access. All data, applications, and IT assets of the TSA network are accessed through defined accounts. The establishment of these accounts is rigorously controlled throughout the life cycle.

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
1.2.1	The SO shall be responsible for management and oversight of all accounts used to access the information system.	5.2 4.1.3.a	AC-2	LMH F
1.2.2	The ISSO shall support the SO in account management by: a. Identifying account types (to include individual, group, system, application, service, guest/anonymous, and temporary); see TS-033 *Application/Service Accounts* for additional information and guidance; b. Establishing conditions for group membership; c. Enacting processes to identify authorized users of the information system and specify access privileges; d. Requiring appropriate approvals for requests to establish accounts; e. Enacting processes to establish, activate, modify, disable, and remove accounts; f. Enacting processes to specifically authorize and monitor the use of guest/anonymous or temporary accounts; g. Notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or have their information system usage or need to know/need to share status change; h. Enacting processes to deactivate temporary accounts that are no longer required and the accounts of terminated or transferred users; i. Enacting processes to grant access to the system based on a valid access authorization, intended system usage, and other attributes as required by the TSA or associated missions'/business functions; j. Ensuring/confirming the use of unique group access, which shall be approved by the appropriate AO, is limited to situations dictated by operational necessity or criticality for mission accomplishment. Shared and group accounts are *prohibited* for all systems categorized as High Value Assets (HVAs); and k. Enacting processes to review accounts on an annual basis.	5.2 4.1.6.d	AC-2	LMH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
1.2.3	The ISSO shall ensure that access control implementations follow the principles of least privilege and separation of duties and shall require users to use unique identifiers. Privileged users shall have separate accounts from their general user accounts in order to perform privileged access. Privileged users are authorized and therefore, trusted to perform security-relevant functions that general users are not authorized to perform.	4.1.4.c 5.2.b	AC-2	LMH F
1.2.4	Social Security Numbers (SSN) shall not be used as logon IDs.	5.2.b	AC-2	LMH F
1.2.5	The Authorizing Official (AO) or the CISO shall review, delegate and approve in writing an individual requiring administrator privileges. This individual may be an appropriate SO, IAD SME or Program Manager.	2.1.6.d	AC-2	LMH F
1.2.6	Reserved	5.2.d	AC-2	LMH F
1.2.7	Systems that are part of the Critical DHS Assets Program shall have provisions to allow the CISO to approve new user accounts as part of a Continuity of Operations (COOP) scenario.	3.5	AC-2	LMH F
1.2.8	The SO shall ensure that the duties and responsibilities of critical information system functions are divided among different individuals to minimize the possibility that any one individual would have the necessary authority or system access to be able to engage in fraudulent or criminal activity.	4.1.4.a	AC-2 AC-5	LMH F
1.2.9	Reserved			
1.2.10	The SO shall implement procedures to ensure system access is suspended for personnel on extended absences.	4.1.6.c	AC-2 IA-4	LMH F
1.2.11	General user accounts shall require a TSA Form 1403 *Computer and Personal Electronic Device Access Agreement (CAA)* to be completed by the user prior to granting the user access.	Not Defined	AC-2	LMH F
1.2.12	Data and applications assigned and available to each specific user are defined by an evaluation of that user's needs to perform his or her duties and approved by the SO in accordance with the approved TSA application catalog or repository.	5.1.a	AC-2	LMH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
1.2.13	All data, applications, and IT assets of the TSA network shall be accessed through defined user accounts.	5.2.e	AC-2	LMH F
1.2.14	User assets shall be locked out after fifteen (15) minutes of inactivity.	4.8.1.a	AC-2	LMH F
1.2.15	Users shall lock end user assets when not in use and stepping away from the asset.	4.8.1.c	AC-2	LMH F
1.2.16	Automated mechanisms shall be implemented by the ISSO to support the management of information system accounts.	Not Defined	AC-2 (1)	LMH F
1.2.17	The SO shall ensure the system is programmed to automatically terminate emergency accounts within an approved and specified time frame.	Not Defined	AC-2 (2)	MH F
1.2.18	Reserved			
1.2.19	The SO shall ensure the system automatically audits account creation, modification, disabling, and termination and notify appropriate support and response personnel.	Not Defined	AC-2 (4)	MH F
1.2.20	Users shall log out of any system when no longer in use.	4.8.1.c	AC-2 (5)	LMH F
1.2.21	Reserved			
1.2.22	The ISSO shall monitor for atypical account usage and report such usage to the SO.	5.2	AC-2 (5)	LMH F
1.2.23	Reserved			
1.2.24	Reserved			
1.2.25	All email messages generated or forwarded by a TSA user shall have the user's identity as the originator.	5.1	AC-2	LMH F

3.1.3 Access Enforcement (AC-3)

Access control policies (to include identity-based policies, role-based policies, and attribute-based policies) and access enforcement mechanisms (to include access control lists [ACL], access control matrices, and cryptography) are employed by TSA to control access between users or processes acting on behalf of users and objects (to include devices, files, records, processes, programs, and domains) in the information system. In addition to enforcing authorized access at the information system level, access enforcement mechanisms are employed at the application level, when necessary, to provide increased information security for TSA. Consideration is given to the implementation of an audited, explicit override of automated mechanisms in the event of emergencies or other serious events. Encryption of stored information shall be FIPS 140-2 (as amended) compliant. For

information, the cryptography used is dependent on the Security level of the information. Mechanisms implemented by AC-3 are configured to enforce authorizations determined by other security controls.

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
1.3.1	Access control policies and access enforcement mechanisms shall be employed by TSA systems to control access between users (or processes acting on behalf of users) and objects (to include devices, files, records, processes, programs, and domains) in the system.	5.2.a	AC-3	LMH F P
1.3.2	The SO shall ensure the system enforces approved authorizations for logical access to the system in compliance with applicable policy.	5.2.a 5.4.3.a	AC-3	LMH F P
1.3.3	Reserved.			
1.3.4	The ISSO shall implement controls to ensure that only authorized individuals are able to participate in videoconferences.	4.5.3	AC-3	LMH F P
1.3.5	Physical and logical access to TSA IT assets shall be limited to individuals on the asset's ACL by the ISSO.	Not Defined	AC-3 CM-6	LMH F P
1.3.6	The SO shall ensure that all data-at-rest, particularly in a Federal Risk and Authorization Management Program (FedRAMP)-compliant cloud or other virtual environments, preserves its identification and access requirements; anyone with access to data storage containing more than one type of information must have specific access authorization for every type of data in the storage. See TS-049 *Information System Audit Logging* and **the *IT Cloud Computing Security Handbook*** for additional information. This Handbook provides guidance regarding cloud implementation and services used to host TSA IT systems to process, store, and transmit TSA information. Other related service models, on which cloud environments are based, addresses Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS), and Infrastructure-as-a-Service (IaaS).	5.2.g	AC-3	LMH F P
1.3.7	The SO shall ensure that information systems/applications utilizing cloud computing services are secured in compliance with the **IT Cloud Computing Security Handbook**, TS-072 *Cloud Computing and Virtualization* and TS-049 *Information System Audit Logging.*	3.18	AC-3	LMH F P

1.3.8	TSA data hosted on a shared service environment/cloud service provider shall go through an approved TIC.	5.4.3.b	AC-3	LMH F P
1.3.9	For *non-web facing* systems, TIC inspection is not required but is still recommended. For *web-facing* systems, the connection *must* traverse through the DHS TIC or Managed Trusted Internet Protocol Service (MTIPS+). **See DHS CISO Memo** dated July 22, 2016, Subject: *Policy on TIC Inspection of Cloud Services.*	Not Defined	AC-3	LMH F P
1.3.10	For non-TIC connections, if TSA is already migrating to the Verizon MTIPS, proceed with the same. Once the DHS MTIPS+ is available, TSA shall work with OneNet towards migrating to the DHS MTIPS+. If TSA already migrated to a non-Verizon MTIPS solutions (ex.: AT&T MTIPS) or is in the process of doing so, an approved waiver is needed. **See DHS CISO Memo** dated July 22, 2016, Subject: *MTIPS Policy.*	Not Defined	AC-3	LMH F P

3.1.4 Information Flow Enforcement (AC-4)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
1.4.1	The ISSO shall ensure the information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems, in compliance with TSA and DHS policy and as documented in the Security Plan (SP).	5.4.1.b	AC-4	MH F P
1.4.2	TSA email systems shall provide for security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to (or modification of) information contained in the email system.	5.4.1 5.4.6	AC-4	MH F P
1.4.3	TSA users shall not perform actions to bypass email screening tools (to include renaming file extensions, etc.).	5.4.6	AC-4	MH F P
1.4.4	If SSI or Sensitive Personally Identifiable Information (SPII) is sent by email, users shall encrypt the information in compliance with TS-002 Encryption policy. For additional information on SPII, see TSA MD 3700.4 *Handling Sensitive Personally Identifiable Information (SPII)*, Appendix "TSA Sensitive PII (SPII) Handling Requirements." To send SSI via email, the user shall refer to the *SSI Policies and Procedures Handbook*, Attachment to *TSA MD 2810.1.*	5.4.6.k	AC-4	MH F P

1.4.5	Appropriate transmission protections, commensurate with the highest sensitivity of information to be discussed over the video or teleconference, shall be in compliance with TSA and DHS policies and shall be in place prior to initiating a teleconference.	4.5.3.b	AC-4 SC-8 SC-9	MH F P
1.4.6	In non-operational or non-production environments (to include training laboratories, development environments, and test environments) where non-TSA personnel have physical access, connectivity to TSA production network(s) are prohibited. TSA operational or production data or information cannot reside in any development environments.	Not Defined	AC-4	MH F P
1.4.7	Prior to posting sensitive content on TSA web sites, both internal and external, established data redaction processes shall be followed to include independent review where necessary.	Not Defined	AC-4	MH F P
1.4.8	Content shall be posted to TSA web sites in compliance with the Rules of Behavior (control PL-4) and all policies set forth by the Office of Human Capital (OHC) in TSA MD 1100.73-5 *Employee Responsibilities and Conduct* and DHS MD 4400.1 *DHS Web (Internet, Intranet, and Extranet Information) and Information Systems.*	Not Defined	AC-4	MH F P
1.4.9	SSI, sensitive data, and information protected under the Privacy Act shall be posted to TSA internal web sites only if access controls are in place and approved by IAD and the content has been approved in advance by the SSI Program Office and/or Privacy Office and the Information Owner (IO) for posting.	Not Defined	AC-4	MH F P

1.4.10	Information regarding TSA personnel or their families, (to include names, phone numbers, and addresses) assigned to units that are sensitive, routinely deployable, or stationed in foreign territories shall not be released nor shall such individuals be identified in photographs or articles including: a. Internal program agenda, correspondence, and memos not appropriate for general distribution. b. Information that is procurement or acquisition sensitive. c. Operations Security (OPSEC) and Information Security (INFOSEC) material. d. Other sensitive information, which, by statute, TSA is not required to encrypt, but shall only be posted when authorized by the Information Owner (IO). This includes "Law Enforcement Sensitive (LES)" or "For Official Use Only (FOUO)" information.	Not Defined	AC-4	MH F P
1.4.11	The ISSO shall ensure fax servers are configured so that incoming communications lines cannot be used to access the network or any data on fax servers.	4.5.2.b	AC-4	LMH F P
1.4.12	The ISSO shall ensure data communication connections via modems are limited and are tightly controlled.	5.4.1.a	AC-4 AC-17	LMH F P
1.4.13	Data communication connections via modems are not allowed, unless they have been authorized by the CISO.	5.4.1.a	AC-4 AC-17	LMH F P
1.4.14	Remote access to DHS networks shall be approved and only be accomplished through equipment specifically approved for that purpose.	5.4.1.a	AC-4 AC-17	LMH F P
1.4.15	Tethering through wireless mobile devices is prohibited without the prior written consent of the CISO.	4.6.2.b 5.4.1.a	AC-4 AC-17	LMH F P
1.4.16	Remote access of PII shall comply with all TSA requirements for sensitive systems, including strong authentication. Secure communication shall be accomplished via VPN or equivalent encryption and two-factor authentication. The Security Plan (SP) shall document any remote access of PII, and the remote access shall be approved by the AO prior to implementation.	5.4.1.c	AC-4 AC-17	MH F P
1.4.17	Auto-forwarding of TSA email to addresses outside of the .gov or .mil domain is prohibited and shall not be used. Users may manually forward individual messages after determining that the risks or consequences are minimal.	5.4.6.i	AC-4	LMH F P

1.4.18	Only Government email accounts shall be used to perform Government business.	5.4.6.l	AC-4	LMH F P
1.4.19	On the use of approved domains, TSA shall only use a **.gov** or **.mil** domain for its official public-facing websites. See ***OMB M-17-06 Policies for Federal Agency Public Websites and Digital Services*** for additional information.	Not Defined	AC-4	LMH F P

3.1.5 Separation of Duties (AC-5)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
1.5.1	The ISSO shall document the separation of duties within the SP and the implementation of separation of duties through assigned information system access authorizations.	4.1.4	AC-5	MH F
1.5.2	Duty requirements for mission critical processing functions shall be clearly documented and distributed to more than one individual.	4.1.4 5.2	AC-5	MH F
1.5.3	The ISSO shall be notified of instances or areas where a single individual is responsible for the performance of an entire mission processing function (to include data input, data processing, log maintenance, application maintenance, and data backup and recovery).	4.1.4	AC-5	MH F
1.5.4	A general user account shall only be issued to an individual identified on the account request form; an account identifier shall be uniquely assigned to an individual user.	5.2.b	AC-5 IA-5	MH F
1.5.5	Separation of duties shall ensure that personnel who control the generation of information security historical data shall not be the same personnel who audit and review that data, in compliance with TS-049 *Information Systems Logging*.	4.1.4	AC-5	LMH F

3.1.6 Least privilege (AC-6)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
1.6.1	The SO shall ensure the information system employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users), which are necessary to accomplish assigned tasks in accordance with (IAW) TSA and DHS missions and business functions.	4.1.4	AC-6	MH F P
1.6.2	Port security on a network appliance within the TSA/DHS network shall be configured by default to deny all and permit by exception. Specific detailed guidance on port security is contained in the TSA TS-012 *Port Security*.	4.1.4	AC-6	MH F P
1.6.3	Personnel using or supporting TSA systems, shall not attempt to use service accounts or any other account to circumvent resource or security restrictions. See also TS-033 *Application/Service Accounts* for service account information and guidance.	4.1.4	AC-6	MH F P
1.6.4	Each system shall be configured to restrict a user or process to the least privileges or access required to perform authorized tasks.	4.1.4	AC-6	MH F P
1.6.5	Remote access privileges shall only be granted to authorized TSA employees, contractors, and agents with valid business requirements for remote access.	4.1.4	AC-6	MH F P
1.6.6	Each remote access account request shall be formally reviewed and approved by the SO.	4.1.4	AC-6	MH F P
1.6.7	Each system's ISSO shall submit an up-to-date list to the TSA Security Operations Center (SOC) each month, containing the names of individuals allowed remote access.	4.1.4	AC-6	MH F P
1.6.8	ISSOs shall limit network communications to specific protocols to reduce network and firewall rule complexity. Additional information can be found in TS-019 *Network Communication Protocol*.	4.1.4 4.5.2 4.5.4. 5.4.5.b	AC-6	MH F P
1.6.9	Least privilege is applicable to all infrastructure and end user assets on all TSA networks, regardless of SELC status.	4.1.4	AC-6	MH F P

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
1.6.10	Privileged accounts shall only be used with the specific functions for which the accounts were assigned. All other system functions (to include email, web browsing, and document preparation) shall use accounts with the lowest necessary privileges.	4.1.4	AC-6	MH F P
1.6.11	The SO shall ensure data stored on RFID tags is limited 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.	4.6.4.b	AC-6 PL-5	MH F P
1.6.12	Reserved			
1.6.13	All downloads of PII via remote access shall follow the concept of least privilege and shall be documented in the SP.	5.4.1.d	AC-6	MH F P
1.6.14	The AO, or delegated authority, shall provide final approval of privileged access accounts to TSA systems.	4.1.4.b	AC-6 (1)	LMH F P
1.6.15	A privileged user shall employ a: a. Dedicated and locked down workstation in order to specifically access their privileged account; and b. General user account using a separate, standard configuration workstation when accessing functions such as email, web-browsing, or document creation.	4.1.4.c 4.1.4.d	AC-6 (2)	LMH F P
1.6.16	The SO shall review and monitor privileged users to include: a. Minimizing the number of privileged users, b. Limiting functions that can be performed when using privileged accounts, c. Limiting the duration that privileged users can be logged in, d. Limiting the privileged functions that can be performed using remote access, and e. Ensuring that privileged user activities are logged and that such logs are reviewed regularly.	4.1.4.	AC-6 (9)	LMH F
1.6.17	The SO shall assess any use of privileged accounts, or roles, for general use functions.	Not Defined	AC-6	MH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
1.6.18	The SO and AO shall only authorize network access to sensitive or mission-critical data for compelling operational needs, and the ISSO shall document the rationale for such access in the SP.	Not Defined	AC-6 (3)	LMH F P
1.6.19	Following account removal instructions by the COR (for contractors) or the Supervisor (for Federal employees), the SO shall ensure, as well as provide proof that a *privileged access account* was disabled/removed within one (1) hour of notification by the SO. *General user accounts* shall be disabled within twenty-four (24) hours. Termination of privileged access shall also apply to employees whose job functions have changed such that they no longer have access to the level to which they were previously granted.	Not Defined	AC-6 (3)	LMH F P
1.6.20	The ISSO shall limit privileged user accounts to designated system administration personnel.	Not Defined	AC-6 (5)	LMH F P
1.6.21	The ISSO shall ensure that systems employ access controls to prevent users from altering malicious code protection software or prevent such software from operating as intended by the SP.	5.2.b	AC-6 (10)	MH F
1.6.22	The ISSO shall ensure the information system is configured to prevent general users from circumventing intrusion detection and prevention capabilities.	5.2.b	AC-6 (10)	MH F
1.6.23	Users shall only have access to sensitive information to which they have an established need to know and for which they are assigned duties requiring access.	4.1.3.a	AC-6	MH F

3.1.7 Unsuccessful Logon Attempts (AC-7)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
1.7.1	All user accounts shall be automatically locked after three (3) consecutive failed logon attempts.	5.2.1.a	AC-7	LMH F
1.7.2	The automatic lockout period for accounts locked due to failed logon attempts shall be set for twenty (20) minutes.	5.2.1.b	AC-7	LMH F
1.7.3	The SPOC shall have procedures in place for unlocking a user account *prior* to the 20 minute lockout period after sufficient user identification is provided.	5.2.1.c	AC-7	LMH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
1.7.4	Workstation, laptop, wireless mobile device, and tablet logon, logoff, and locking procedures shall be consistent with DHS 4300A PD and supporting configuration guidance.	3.7.e 5.2.1	AC-3 CM-2	LMH F
1.7.5	The VPN logon shall lock following *three* (3) unsuccessful attempts; and the Personal Identity Verification (PIV) card chip disables itself (www.gemalto.com) following *ten* (10) incorrect attempts. (The PIV card includes mechanisms to block activation of the card after a number of consecutive failed attempts. The number of consecutive failed activation attempts varies by the activation mechanism.)	5.2.1	AC-7 FIPS PUB 201-2, 4.3.1, 6.2.2	LMH F

3.1.8 System Use Notification (AC-8)

To effectively meet access control requirements, TSA implements the requirements of DHS MD 4400.1, *DHS Web (Internet, Intranet, and Extranet Information) and Information Systems*, regarding the allocation of safeguards for TSA Internet, Intranet, and Extranet web sites and the proper notification to individuals of privacy safeguards.

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
1.8.1	A TSA-approved logon *Acceptable Use Policy* warning banner message shall be displayed on the logon screens of TSA IT assets that have a viewing screen (to include workstations, laptops, tablets, and mobile devices) to the extent technologically feasible.	5.2.3	AC-8	LMH F
1.8.2	The DHS approved warning banner, as stated in DHS 4300A, paragraph 5.2.3, shall be utilized as the TSA approved logon warning banner.	5.2.3.a	AC-8	LMH F
1.8.3	The SO shall ensure clear privacy policies are posted on TSA web sites, as well as at any other known, major entry points to sites, and at any web page where personal information is posted or collected.	4.8.4 4.9 5.2.3	AC-8	LMH F
1.8.4	Security and privacy policies shall be clearly labeled and easily viewed at the entry point to every TSA facing web site.	4.8.4, 4.9 5.2.3.b	AC-8	LMH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
1.8.5	TSA information system users shall have no expectations of privacy associated with the use of the system. By completing the authentication process, the user acknowledges his or her consent to monitoring. The use of TSA office equipment and TSA systems/computers constitutes consent to monitoring and auditing of the equipment/systems. Monitoring includes the tracking of internal transactions and external transactions such as Internet access. It also includes auditing of stored data on local and network storage devices as well as removable media. Consent to monitoring shall be noted within the signed rules of behavior.	4.8.4.c 4.8.4.d 4.8.4.e	AC-8 PL-4	LMH F

3.1.9 Previous Logon (Access) Notification (AC-9)

Currently, this control does not apply to any control baselines, nor does it apply to Privacy or Financial systems.

3.1.10 Concurrent Session Control (AC-10)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
1.10.1	Concurrent sessions to the same system or application using the same authentication credentials are not allowed without strong authentication, unless a specific business or operational need is documented and approved by the AO.	5.2.f	AC-10	H

3.1.11 Device Lock (AC-11)

Information concerning this control may be found in TSA TS-015 *Network Logical Access Control.*

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
1.11.1	Network applications or systems shall automatically lock user sessions when the session is inactive for twenty (20) minutes. The user shall be required to re-authenticate to re-establish network access.	5.2.2.a 5.2.2.b	AC-11	MH F

3.1.12 Session Termination (AC-12)

The term *session* refers to a connection between a terminal device (workstation, laptop, mobile device) and a networked application or system. The term *session* also refers to accessing an

application or system such as a database or networked application through the DHS network. When a session is locked, the user shall resume activity by re-authenticating.

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
1.12.1	Sessions shall automatically terminate after sixty (60) minutes of inactivity.	5.2.2.c	AC-12	MH F

3.1.13 Supervision and Review—Access Control (AC-13) (Withdrawn)

This control has been withdrawn by NIST and is no longer in force.

3.1.14 Permitted Actions without Identification or Authentication (AC-14)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
1.14.1	The CISO shall approve any actions on an information system to be performed by a user without proper identification and authentication in order to accomplish mission/business objectives.	Not Defined	AC-14 (1)	LMH
1.14.2	The SO shall document and provide supporting rationale in the SP for all user actions not requiring identification and authentication.	Not Defined	AC-14	LMH

3.1.15 Automated Marking (AC-15) (Withdrawn)

This control has been withdrawn by NIST and is no longer in force.

3.1.16 Security and Privacy Attributes (AC-16)

Currently, this control does not apply to any control baselines, nor does it apply to Privacy or Financial systems.

3.1.17 Remote Access (AC-17)

This control provides direction for minimizing the threats associated with remote access and applies to all authorized TSA employees, contractors, vendors, and agents with remote access to TSA IT assets. Remote access implementations that are covered by this policy include, but are not limited to, VPNs, dial-in modems, frame relay, Integrated Services Digital Network (ISDN), Secure Shell (SSH) connections, and connections made through asynchronous transfer mode (ATM), Wireless, or Digital Subscriber Line (DSL). Remote access controls are applicable to information systems/applications other than public web servers or systems specifically designed for public access.

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
1.17.1	The SO shall document allowed methods of remote access to the information system, establish usage restrictions and implementation guidance for each allowed remote access method.	5.4.1	AC-17	LMH F P
1.17.2	The CISO shall establish usage restrictions and implementation guidance for each allowed remote access method.	5.4.1	AC-17	LMH F P
1.17.3	The SO shall ensure the information system and/ or SOC monitors for unauthorized remote access to the information system.	5.4.1	AC-17	LMH F P
1.17.4	The AO, or delegated authority, shall authorize remote access to the information system prior to connection.	5.4.1	AC-17	LMH F P
1.17.5	The SO shall enforce requirements for remote connections to the information system.	5.4.1	AC-17	LMH F P
1.17.6	The ISSO shall ensure that the inbound dial-in capabilities are disabled on any multifunction device connected to a TSA information system containing sensitive data.	4.12.j	AC-17	LMH F P
1.17.7	Reserved			
1.17.8	Remote access of PII shall not permit the download and remote storage of information, unless the requirements for the use of removable media with sensitive information have been addressed.	5.4.1.d	AC-17	LMH F P
1.17.9	The CISO shall ensure TSA systems employ automated mechanisms to facilitate monitoring and control of remote access methods.	Not Defined	AC-17 (1)	LMH F P
1.17.10	The SO shall ensure the system uses cryptography to protect the Confidentiality and Integrity of remote access sessions in compliance with TS-002 *Encryption*.	Not Defined	AC-17 (2)	LMH F P
1.17.11	The SO shall ensure the system routes remote access through a limited number of managed access control points.	Not Defined	AC-17 (3)	LMH F P
1.17.12	The CISO shall authorize remote access for the execution of privileged commands and security-relevant information only for compelling operational needs; the ISSO shall document the rationale for such access in the security plan for the information system.	Not Defined	AC-17 (4)	LMH F P

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
1.17.13	The CISO shall ensure operational systems continuously monitor for unauthorized remote connections and take appropriate action if an unauthorized connection is discovered.	Not Defined	AC-17 (5)	LMH F P
1.17.14	The SO shall ensure that users protect information about remote access mechanisms from unauthorized use and disclosure.	Not Defined	AC-17 (6)	MH F P
1.17.15	The CISO shall ensure that remote sessions for accessing sensitive systems are logged and monitored in compliance with TS-049 *Information Systems Logging.*	5.4.1.c	AC-17 (7)	LMH F P
1.17.16	The SO shall ensure that systems disable unauthorized protocols, except for explicitly identified components in support of specific operational requirements with a signed and approved waiver from the CISO using the proper waiver process.	1.5	AC-17 (8)	LMH F P

3.1.18 Wireless Access (AC-18)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
1.18.1	The CISO shall ensure the establishment of usage restrictions and implementation guidance for wireless access. See TS-003 *Wi-Fi* (802.11) and DHS 4300A Attachment Q1, Wireless Systems	4.6.1.g	AC-18 PM-5	LMH
1.18.2	The CISO shall ensure prevention of unauthorized wireless access to TSA information systems and ensure that systems are being monitored in the event of any violations.	5.1 4.6.1.g	AC-18	LMH
1.18.3	The CISO shall authorize wireless access to information systems prior to implementation.	4.6.1.g	AC-18	LMH
1.18.4	The CISO shall enforce requirements for wireless connections to the information system.	4.6.1.g	AC-18	LMH
1.18.5	Wireless mobile devices shall not be tethered or otherwise physically or wirelessly connected to TSA or non-TSA information systems without ***prior*** written AO authorization.	4.6.2.b	AC-18	LMH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
1.18.6	The CISO shall ensure Wi-Fi, Bluetooth, and RFID are implemented in compliance with TS-003 *Wi-Fi*, TS-004 *Bluetooth*, and TS-024 *RFID*, respectively. See NIST SP 800-121 Rev 1 *Guide to Bluetooth Security;* DHS 4300A Sensitive Systems Policy Directive, Attachment Q6 *Bluetooth Security;* DHS 4300A Attachment Q1 *Wireless System* and TS-026 *Patch Management* for additional guidance.	4.6.2.4 Attch Q1 & Q6	AC-18	LMH
1.18.7	The SO shall ensure the system protects wireless access to the system using authentication and encryption.	4.6.1.d, Q1, Q6	AC-18 (1)	MH
1.18.8	The SO shall enforce and perform continuous monitoring of systems looking for unauthorized wireless access point connections to information systems; appropriate action shall be taken when an unauthorized connection is discovered.	2.1.2, 2.1.10, 3.7, Q6	AC-18 (2)	H
1.18.9	The CISO shall approve requirements for the implementation of Bluetooth technology when connecting with TSA assets and accessories. *Assets* shall include any device which is capable of storing TSA data, and *accessories* generally include devices which pair with assets to facilitate input and output, such as: keyboards, earpieces, headsets, personal identity verification (PIV) card readers, microphones, speakers, projectors, mice, and printers. See TS-004 *Bluetooth* for additional information.	4.6.2.4 Attch Q6	AC-18	LMH
1.18.10	The SO shall not allow users to independently configure wireless networking capabilities.	Attch Q6	AC-18 (4)	LMH

3.1.19 Access Control for Mobile Devices (AC-19)

This control provides general security direction for mobile TSA IT assets allocated to end users in the performance of their assigned duties. TSA IT assets include, but are not limited to: workstations, laptop computers, mobile devices (such as tablets), infrastructure devices (switches, routers, firewalls, etc.), software (individual and enterprise), firmware, peripheral devices (Universal Serial Bus [USB] drives, USB microphones, keyboards, etc.), and Mobile Electronic Media (MEM). These requirements shall extend to TSA IT assets located at non-TSA facilities. The user shall review supporting sections of the TSA TS-008 *End User Assets*, for specific asset policies. The DHS 4300A Sensitive System Handbook *Attachment Q1 "Wireless Systems,"* DHS 4300A Handbook Attachment *Q2 "Mobile Devices,"* as well as the NIST SP 800-124, Rev 1 *"Guidelines for Managing the Security of Mobile Devices in the Enterprise,"* have guidance on wireless and mobile devices, mobile applications, and mobile management in the enterprise. DHS Enterprise Secure Architecture (ESA) *Secure Mobile Computing* also provides security principles and guidelines regarding appropriate

safeguards. Lastly, the NIST SP 800-164 *Guidelines on Hardware-Rooted Security in Mobile Devices*, as well as the NIST SP 800-163 *Guidelines for Testing and Vetting Mobile Applications* both provide general references for safeguarding mobile components.

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
1.19.1	The AO shall authorize connection of mobile devices to TSA information systems.	4.6.2	AC-19	LMH
1.19.2	The CISO shall ensure prevention and monitoring of unauthorized connections of mobile devices to TSA information systems.	4.6.2	AC-19	LMH
1.19.3	The SO shall: a. Enforce requirements for the connection of mobile devices to TSA information systems, and b. Disable information system functionality that provides the capability for automatic execution of code on mobile devices without user direction.	4.6.2	AC-19	LMH
1.19.4	The SO of mobile devices shall: a. Issue specially configured mobile devices to individuals traveling to locations that the TSA deems to be of significant risk, and b. Upon the individual's return from travel, apply preventative security measures to mobile devices returning from these locations.	4.6.2.v	AC-19	LMH
1.19.5	Information stored on laptop computers, tablets, or other mobile computing devices that may be used in a residence or on travel shall use encryption in compliance with TS-002 Encryption policy.	4.6.2.t	AC-19 PL-4	LMH
1.19.6	When unattended outside a Controlled Access Area (CAA), laptop computers and other mobile computing devices shall be secured using one of the following methods: • a locked office, • a locking cable, • a locked cabinet, or • a locked desk. CAA would be considered a physical area (e.g., building, room, etc.) to which only authorized personnel are granted unrestricted access. All other personnel are either escorted by authorized personnel or are under continuous surveillance.	4.3.1 4.6.2.u	AC-19 PL-4	LMH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
1.19.7	Users on official non-routine travel outside the U.S. or its territories shall inform their Branch Managers and subsequently their Director (or delegated official) in writing and obtain written approval ***prior*** to taking their TSA-issued laptop or other mobile computing device overseas. Management strongly discourages users on non-official travel outside of the U.S. or its territories from taking their GFE devices due to major security concerns.	4.6.2.v	AC-19 PL-4	LMH
1.19.8	Unclassified mobile devices and other wireless enabled devices or any recording device shall not be used within areas where classified information is discussed, processed, or stored.	4.6.2.a 4.6.2.k	AC-19 PL-4	LMH
1.19.9	The CISO shall approve the use of writable, removable media in TSA information systems.	4.3.1.a	AC-19 MP-2 PM-9	LMH
1.19.10	Non-GFE removable media shall not be used on TSA systems.	4.3.1.c	AC-19 (2) MP-1	LMH
1.19.11	Only TSA owned and approved removable media may be used with TSA information systems.	Not Defined	AC-19 (3)	LMH
1.19.12	Users who telework may connect their TSA-issued laptop to their home peripheral equipment such as a: monitor, keyboard, and mouse. None of these three peripheral devices shall have residual memory and all must be cabled or hardwired (no wireless connection).	Not Defined	AC-19 (5)	LMH
1.19.13	Mobile device users shall have available to them: preauthorized, reusable, secured, and compliant mobile applications (or apps) and services. This shall be done via an authorized and dedicated TSA enterprise applications catalog, code repository, and library or apps store.	4.6.1.f 4.6.2.d	AC-19 SC-18	LMH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
1.19.14	For secure mobile applications, the IT Operations and Engineering Division (OED), who manages and maintains the smartphone Mobile Device Management (MDM) infrastructure, shall ensure to: a. Restrict which app stores, library, repository or catalog may be used and which applications may be installed through whitelisting or blacklisting; b. Restrict the amount and types of commercial pre-loaded mobile applications; c. Restrict permissions assigned to each mobile application; d. Ensure proper build, configuration, internal testing, independent third party penetration testing or application vulnerability scanning, deployment, installation, update, tracking and removal of applications; e. Maintain an accurate and detailed inventory of all mobile applications; f. Restrict the use of application synchronization (example: local device synch services, remote synch services and websites); g. Verify digital signatures on mobile applications to ensure that only apps from trusted entities are installed on the device and that the code has not been modified; h. Limit mobile device deployment to TSA-sanctioned devices, technologies, and applications by using MDM systems, which allows centralization of mobile devices and enforcement of security policies on the devices; i. Incorporate mobile devices and applications into the TSA SELC process (as complemented by the **Agile Development and Delivery for IT Manual**) and consider phases such as product: initiation, design, development, testing, independent third party testing or application vulnerability scanning, implementation, deployment, O&M, and disposition; j. Coordinate and let the Customer Engagement and Development Division (CEDD) lead efforts in the central management of mobile applications by an enterprise Mobile Application Management (MAM), which functions to evaluate and select mobile applications, as well as acts as an authorized enterprise application store for users. MAM also provides for the ability to monitor installed applications and remotely upgrade or uninstall applications, as necessary; k. Allow for Over-the-Air (OTA) software distribution, configuration change detection, remote data-wipe, remote configuration, and asset/property management; and l. Regarding TSA-issued iPhones, SSI or PII shall not be entered, processed, stored, or transmitted outside of the smartphone Mobile Messaging Client; no data shall be transferred from the smartphone Mobile Messaging Client to personally owned devices. Government data must reside exclusively inside the secured container's Mobile Messaging Client.	4.6.2	AC-19 SC-18	LMH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
1.19.15	A mobile device shall allow for remote purging/wiping of information in order to address the threat of theft, loss of the device, or failed logon.	4.6.2	AC-7 MP-6(8)	LMH F
1.19.16	Federal employees shall not engage in text messaging when (a) driving a Government-Owned-Vehicle (GOV) or driving a Privately-Owned-Vehicle (POV) while on official Government business, or (b) when using electronic equipment supplied by the Government while driving.	4.1.2, 4.1.5	AT-1 PL-4 PS-6	LMH
1.19.17	Non-GFE devices such as Bringing Your Own Device (BYOD) are prohibited without prior approval of the DHS CISO since these devices tend to be untrustworthy. For example, there are frequent “jailbreaking” and “rooting” of these devices where built-in restrictions on security and OS use have been bypassed.	4.8.2	MP-7	LMH
1.19.18	The AO shall evaluate and determine whether to accept any risk associated with authorizing the use of non-GFE: hardware, equipment, software, or email to collect, generate, process, store, display, transmit, or receive TSA SSI related information. A Risk Assessment Memo or Waiver Request shall be processed and approved by the AO to allow personal cellular use for transmitting SSI.	1.5	MP-7	MH
1.19.19	Short Message Service (SMS) and Multimedia Messaging Service (MMS) shall not be used to process, store, or transmit sensitive information, and shall be disabled whenever possible.	4.6.2.3.c	AC-19	LMH
1.19.20	Where required and authorized, all communications outside of the United States and its territories shall be in compliance with the Department of State Foreign Affairs Manual (FAM), 12 FAM 600 *Information Security Technology*.	4.7.a	AC-19	LMH

3.1.20 Use of External Information Systems (AC-20)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
1.20.1	The SO shall establish terms and conditions with other external organizations owning, operating, and/or maintaining external information systems that allow authorized individuals to: a. Access the TSA information system from the external information systems and process, store, and/or b. Transmit TSA-controlled information using the external information systems.	2.1.3 2.1.11	AC-20	LMH
1.20.2	TSA owned removable media shall not be connected to any non-TSA IT asset, unless authorized by the AO.	4.3.1.e	AC-20 PM-9	LMH
1.20.3	Any device or hardware that has been obtained through civil or criminal asset forfeiture shall not be used as part of a TSA information system, nor used to process TSA information.	4.8.2.c	AC-20	LMH
1.20.4	The SO shall develop and enforce procedures to ensure proper malware scanning of media prior to installation of primary hard drives, software with associated files, and other purchased products.	5.6.c	AC-20	LMH
1.20.5	The use of Internet webmail (to include Gmail, Yahoo, AOL, Hotmail, etc.) or other personal email accounts is not authorized over TSA furnished equipment or network connections except as provided in section 4.6.45 of this Handbook.	5.4.7.a 1.5.1.i	AC-20 SA-7	LMH
1.20.6	The AO shall approve the use of an external information system to access TSA systems or to process, store, or transmit TSA-controlled information.	2.1.3 2.1.11	AC-20 (1)	LMH
1.20.7	The AO shall approve the use of a TSA portable storage media on external systems.	Not Defined	AC-20 (2)	LMH
1.20.8	The AO shall ensure that a properly configured, secured, tested, and authorized web browser is integrated as part of a locked-down TSA image for laptops and/or smartphones for web browsing purposes. For additional information and guidance, see TS-028 Web Applications Security	Not Defined	AC-20 AC-1	LMH

3.1.21 Information Sharing (AC-21)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
1.21.1	TSA employees and contractors shall limit the dissemination of sensitive information for authorized purposes. Sensitive information is information, not otherwise categorized by statute or regulation that, if disclosed, could have an adverse impact on the welfare or privacy of individuals or on the welfare or conduct of Federal programs. TSA shall share information with DHS and other appropriate Federal agencies, State and local government officials, or industry stakeholders who have a need to know: a. Facilitate information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions of the information; and b. Provide a centralized information system for access and retrieval of information by users (example: email, SharePoint, and databases) to assist in obtaining and making information sharing/collaboration decisions. See ***Homeland Security Act of 2002*** for additional information.	1.7	AC-21	MH
1.21.2	Each information system through which information is shared shall: a. Have the capability to transmit unclassified, SBU or classified information (as appropriate), though the procedures and recipients for each capability may differ; b. Have the capability to restrict delivery of information to specified subgroups by geographic location, type of organization, position of a recipient within an organization, or a recipient's need to know of such information; c. Be configured to allow the efficient and effective sharing of information to authorized personnel; d. Be accessible to State and local government officials and industry stakeholders (as appropriate); and e. Provide data integrity through the timely removal and destruction of obsolete or erroneous names and information. See ***Homeland Security Act of 2002*** for additional information.	1.7	AC-21	MH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
1.21.3	Sharing PII outside the Department shall be restricted to a purpose compatible with the purpose for which the PII was collected. TSA shall use PII only for legally authorized purposes and in a manner compatible with uses identified in the Privacy Act or in other public notices. See *TSA MD 3700.4 Handling Sensitive Personally Identifiable Information*, as well as the DHS Handbook for Safeguarding SPII for additional information.	3.14.8	AC-21	MH

3.1.22 Publicly Accessible Content (AC-22)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
1.22.1	The IO shall designate individuals authorized to clear TSA information for public release and recommend posting of information onto a TSA information system that is publicly accessible.	Not Defined	AC-22	LMH
1.22.2	The IO shall ensure that individuals authorized to clear TSA information for public release are properly trained to ensure that publicly accessible information does not contain non-public information.	Not Defined	AC-22	LMH
1.22.3	The proposed content of publicly accessible information for non-public information shall be reviewed for public clearance prior to posting onto information systems.	Not Defined	AC-22	LMH
1.22.4	The IO shall review and report the content on publicly accessible TSA information systems for non-public information quarterly.	Not Defined	AC-22	LMH
1.22.5	The IO shall remove and report non-public information from the publicly accessible TSA information system, when discovered.	Not Defined	AC-22	LMH
1.22.6	The TSA Office of Strategic Communications and Public Affairs shall designate “content managers” to post official TSA content to social media sites.	3.16.a	AC-22 SA-6	LMH
1.22.7	Content managers shall ensure posted content to TSA web sites is in keeping with the TSA Terms of Service (TOS) and guidelines for a given social media host (to include YouTube, Twitter, etc.). Under no circumstances shall sensitive information be posted to social media sites.	3.16.b	AC-22 SC-4	LMH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
1.22.8	Content managers shall ensure information is not posted to any social media site for which the Department has not approved.	3.16.c	AC-22 SA-6 SC-4	LMH
1.22.9	Content managers shall review and understand the appropriate Department-level TOS for the appropriate social media host.	3.16.d	AC-22 SC-4 AT-3	LMH
1.22.10	Content managers shall make a risk decision prior to posting any information and shall recognize that social medial hosts are not TSA information systems and, therefore, subject only to the TSA TOS and not to TSA policy. Once released, information is no longer under TSA control.	3.16.e	AC-22 AT-2 SC-4 SI-9	LMH

3.1.23 Data Mining Protection (AC-23)

Currently, this control does not apply to any control baselines, nor does it apply to Privacy or Financial systems.

3.1.24 Access Control Decisions (AC-24)

Currently, this control does not apply to any control baselines, nor does it apply to Privacy or Financial systems.

3.1.25 Reference Monitor (AC-25)

Currently, this control does not apply to any control baselines, nor does it apply to Privacy or Financial systems.

3.2 Awareness and Training (AT)

All TSA users to include *Privileged Users* and *General Users* are required to conduct mandatory annual IT security awareness training using the Online Learning Center (OLC) commensurate with their system responsibilities. Prior to gaining access to TSA information systems/applications, all TSA users are required to sign TSA Form 1403 *Computer and Personal Electronic Device Access Agreement (CAA)* and annually thereafter. In addition, all users are required to have a level of awareness to support their responsibilities in protecting the security of the TSA information systems/applications. These goals are accomplished through initial and refresher training in compliance with the TSA IT Security Awareness, Training, and Education policy and DHS 4300A. This control applies to all TSA personnel and contractors.

3.2.1 Awareness and Training Policy and Procedures (AT-1)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
2.1.1	The CISO shall develop, disseminate, and annually review/update a formal, documented security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among TSA entities, and compliance; and formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.	2.1.3 4.1.5.a	AT-1	LMH
2.1.2	The CISO shall ensure the maintenance of an ongoing IT Security/information assurance awareness program comprised of trainings, posters, newsletters, and other promotional materials.	Not Defined	AT-1	LMH
2.1.3	The CIO and CISO shall provide resources to develop or acquire, refine, and deliver IT Security/IA Cybersecurity Awareness Training and Significant Security Responsibility position security training.	4.1.5	AT-1	LMH
2.1.4	The SO shall factor training impacts into proposed or planned technology or operational changes.	4.1.5	AT-1	LMH
2.1.5	The CISO shall prepare and submit IT Security/IA Awareness, Training, and Education statistics monthly and training reports to the DHS IT Security Training Program Director, as required by DHS 4300A.	4.1.5.g 4.1.5.h	AT-1	LMH
2.1.6	The CISO shall ensure that general users are trained regarding rules of behavior and that each user signs a copy prior to being granted user accounts or access to information systems, applications or data, as required by DHS 4300A.	4.1.5.b	AT-1	LMH
2.1.7	Education and training shall meet standards established by NIST and DHS.	4.1.5.a	AT-1	LMH
2.1.8	Information system users shall abide by TSA security training requirements.	3.11.2.c	AT-1	LMH

3.2.2 Awareness Training (AT-2)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
2.2.1	All contractor employees requiring system access shall receive initial Organizational Security Fundamentals (OSF) Training within 60 days of assignment to the contract via the **Online Learning Center (OLC).** Refresher training shall be completed annually thereafter.	4.1.5	AT-2	LMH
2.2.2	New users of TSA IT assets, including TSA personnel, contractors, or others working on behalf of TSA with significant security responsibilities (e.g., Information Systems Security Officers (ISSO), system administrators) shall receive specialized training prior to obtaining access to the system(s) containing sensitive information. Those individuals will need to complete refresher training each fiscal year.	4.1.5.c	AT-2	LMH
2.2.3	Individual role based security training plans shall be automatically designed and assigned by the Online Learning Center (OLC) depending upon each individual's job/responsibility. Individual training plans shall be refreshed annually or immediately after a change in the individual's position or related position description requirements.	4.1.5.d	AT-2	LMH
2.2.4	IT security awareness training shall include information on recognizing and reporting potential indicators of insider threat. The OLC-provided *OSF* training shall be taken by all TSA federal employees, to include refresher training on an annual basis.	4.1.5 1.8	AT-2 (2)	LMH

3.2.3 Role-Based Training (AT-3)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
2.3.1	All users with access to TSA IT, assets including TSA personnel, contractors, or others working on behalf of TSA (for example, employees, detailees, military personnel, interns, etc.) shall receive annual IT Security/IA awareness refresher training. User accounts and access privileges, including access to email, shall be disabled for those employees who have not completed annual refresher training in a timely manner.	4.1.5.b	AT-3	LMH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
2.3.2	Reserved			
2.3.3	The TSA IAD shall annually review the DHS master training plan that defines the curriculum required for each Significant Security Responsibility (SSR) position description, along with related courseware requirements.	4.1.5.d	AT-3	LMH
2.3.4	Individuals, including TSA personnel, contractors, or others, working on behalf of TSA (for example, employees, detailees, military personnel, interns, etc.) with SSRs shall receive annual specialized training commensurate with the responsibilities required of the position, or role.	4.1.5	AT-3	LMH
2.3.5	Reserved			
2.3.6	Reserved			
2.3.7	All TSA personnel are responsible for proper handling of TSA sensitive information (e.g. classified, sensitive, PII, and SSI) and shall complete awareness training specific to the appropriate handling of the information they can be expected to encounter.	4.3.1	AT-3	MH F

3.2.4 Training Records (AT-4)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
2.4.1	All users of TSA information systems/applications shall complete TSA Form 1403 *Computer and Personal Electronic Device Access Agreement (CAA)* upon initial employment. Records of these forms shall be maintained including name, position, and date.	4.1.5	AT-4	LMH
2.4.2	OLC shall maintain evidence of security awareness reports and provide to the DHS CISO, via the TSA CISO.	4.1.5.h	AT-4	LMH
2.4.3	Security awareness training records shall be retained by the TSA in the OLC System for a period of five (5) years. These records shall include training name and position, security role of trainee, training course title, type of training received, completion date of training, and costs of training.	4.1.5.d	AT-4	LMH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
2.4.4	The CISO shall submit a roster during the first month and during the seventh month of each fiscal year identifying all significant information security personnel, including full name, security role, employment status (federal employee, military, contractor, etc.), and work location (state) to the DHS Information Security Training Program Office. At a minimum, the roster shall include all standard information security roles: Chief Information Officer, Chief Information Security Officer, Authorizing Official, Program Manager, System Owner, Information System Security Officer, Security Operations Center Manager, System Administrator (Windows-based), and Contracting Officer/Contracting Officer Representative (COR).	2.2.9 4.1.5.k	AT-3 AT-4	LMH

3.2.5 Contacts with Security Groups and Associations (AT-5) (Withdrawn)

Withdrawn and incorporated into PM-15.

3.3 Audit and Accountability (AU)

The configurations of IT assets are audited on a regular basis in compliance with the TSA TS-049 *Information Systems Logging*. The TSA IAD has the primary responsibility to conduct internal security audits for operational information systems (to include General Support Systems [GSS] and Major Applications [MA]), as well as for systems and applications under development. (Every GSS and MA shall have an ISSO assigned.) IAD shall provide TSA senior management with reports on the effectiveness of IT security by identifying weaknesses and recommending improvements. The CISO shall determine what events shall be audited and set requirements for audit data retention. Formal audits of the TSA IT environment are conducted by the IAD Audit Team on a recurring basis. The plan for each audit element is formulated once per year and defines the number of sites or assets to be sampled, the order in which the assets and sites are visited, and the samples to be collected from each.

3.3.1 Audit and Accountability Policy and Procedures (AU-1)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
3.1.1	The CISO shall develop, disseminate, and annually review/update a formal, documented audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among TSA entities, and compliance; and formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated controls.	5.3	AU-1	LMH F
3.1.2	The SO shall ensure that information systems/applications perform audit and accountability actions in compliance with TS-049 *Information Systems Logging.*	5.3	AU-1	LMH F
3.1.3	The SO shall ensure that information systems provide visibility into system actions that may lead to security events or incidents in compliance with TS-049 *Information Systems Logging*.	5.3	AU-1 AU-2	LMH F
3.1.4	The SO shall ensure that information systems provide visibility into all privileged system actions in compliance with TS-049 *Information Systems Logging*.	5.3	AU-1	LMH F
3.1.5	The SO shall ensure that the data contained in system logs is maintained and controlled in a manner that prohibits tampering, loss, or destruction. This control also applies to the management and oversight responsibilities regarding Information Systems Logging in compliance with TS-049 *Information Systems Logging.*	5.3.c	AU-1 AU-11 PE-2	LMH F
3.1.6	The SO shall ensure that all devices capable of auditing (to include event, security, application, etc.) have logging enabled in compliance with TS-049 *Information Systems Logging.*	5.3	AU-1	LMH F
3.1.7	The CISO shall ensure that IA system scans are conducted, validate that the configuration of the IT assets in the system are correct, and ensure that the policy associated with those assets is enforced. The performance of IA system scans shall be consistent with and in satisfaction of DHS 4300A PD Attachment O *Vulnerability Management.* See also TS-026 *Patch Management* for ISVM related information and guidance on patching.	5.3	AU-1	LMH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
3.1.8	The CISO shall ensure that IA conformance/ performance audits validate that the operational requirements of the system are enforced.	5.3	AU-1	LMH F
3.1.9	The respective ISSO for each information system shall perform an annual audit (self-assessment) IAW NIST SP 800-53A and forward the results and associated Plan of Action and Milestones (POA&Ms) to the IAD.	5.3	AU-1	LMH F
3.1.10	The TSA SOC shall implement both general and threat-specific event logging.	5.3.f	AU-1	LMH F

3.3.2 Audit Events (AU-2)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
3.2.1	The CISO shall determine the list of general auditable events for TSA information systems and set forth general requirements in TS-049 *Information Systems Logging*, which shall be reviewed annually.	5.3.a	AU-2	LMH F P
3.2.2	The ISSO shall determine the specific list of auditable events for the information system on behalf of the SO, based on a risk assessment, and mission/business needs, and in compliance with TS-049 *Information Systems Logging*. In addition, the ISSO shall document the rationale for the selection of auditable events with regards to a potential incident investigation and why the list of events is deemed adequate.	5.3.a	AU-2	LMH F P
3.2.3	The ISSO shall coordinate the security audit functionality for the information system with other TSA entities requiring audit-related information.	5.3	AU-2	LMH F P
3.2.4	The ISSO shall ensure that appropriate audit logging controls are implemented on every network element.	5.4.3.a	AU-1 AU-2	LMH F P
3.2.5	The ISSO shall ensure that appropriate audit logging controls are implemented for all remote access capabilities provided by the information system.	4.8.4.c 5.4.1.b	AC-4 AC-8 AC-17 AU-2	LMH F P

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
3.2.6	Use of Government Furnished Equipment (GFE) shall constitute the consent to monitoring and auditing. This monitoring includes transactions within and transactions that transverse government networks (to include access to the Internet). It also includes auditing of stored data on local and network storage devices, as well as removable media.	4.8.4.c 5.3	AC-8 AU-2	LMH F P
3.2.7	TSA personnel and contractors shall not have an expectation of privacy in the use of government computers or computer systems.	4.8.4.d	AC-8	LMH F P
3.2.8	TSA shall access system transactions, email messages, or other electronic data on government computer systems whenever there is a legitimate governmental purpose for doing so, to include random security reviews.	4.8.4.c 5.3	AC-8 AU-2	LMH F P
3.2.9	The CISO shall ensure that reviews, analysis, and updates are conducted on audited events in a timely manner.	2.1.9.d 2.1.10 2.1.11 5.3 5.4.2	AU-2 (3)	MH F P
3.2.10	Reserved			
3.2.11	The ISSO shall review and update the list of auditable events annually. These auditable events shall be documented and maintained within the SP.	5.3	AU-2 (4)	MH F
3.2.12	Reserved			

3.3.3 Content of Audit Records (AU-3)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
3.3.1	TSA information systems shall produce audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event.	5.3.a	AU-3	LMH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
3.3.2	TSA information systems shall produce audit records to monitor any activities that might modify, bypass, or negate information security safeguards, all security-relevant actions associated with processing, and all activities performed using an administrator's identity.	5.3.a	AU-3	LMH F
3.3.3	The CISO shall determine what minimum events shall be audited and set requirements for audit data retention. A sample list of auditable events may be found in TS-049 *Information Systems Logging.*	5.3	AU-3	LMH F
3.3.4	Auditable events related to servers, applications, and routers, firewalls, or other major network devices shall be identified and audited.	5.3	AU-3	LMH F
3.3.5	The ISSO shall review and update the list of auditable events annually and shall be documented and maintained within the SP.	5.3	AU-2 AU-3	MH F P
3.3.6	Audit records shall include additional audit events identified by type, location, or subject in compliance with TS-049 *Information Systems Logging.*	5.3	AU-3 (1)	MH F
3.3.7	The SO shall centrally manage the content of audit records for applicable information systems in compliance with TS-049 *Information Systems Logging*	5.3	AU-3 (2)	H F

3.3.4 Audit Storage Capacity (AU-4)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
3.4.1	The SO shall allocate audit record storage capacity and configure auditing to reduce the likelihood of such capacity being exceeded.	5.3.d	AU-4	LMH

3.3.5 Response to Audit Processing Failures (AU-5)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
3.5.1	TSA information systems shall issue alerts in the event of an audit processing failure. Audit failures shall include software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.	5.3.g	AU-5	LMH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
3.5.2	The ISSO shall document the procedural steps to be taken when audit failure occurs for an information system within the SP, including the plan to shut down the information system, overwrite the oldest audit records, or stop generating audit records completely.	5.3.g	AU-5	LMH
3.5.3	TSA information systems shall provide a warning when allocated audit record storage volume reaches 80% of maximum audit record storage capacity.	Not Defined	AU-5 (1)	H
3.5.4	TSA information systems shall provide real-time alerting when failure events occur.	5.3	AU-5 (2)	H

3.3.6 Audit Review, Analysis, and Reporting (AU-6)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
3.6.1	Reserved			
3.6.2	The ISSO shall report findings and indications of inappropriate or unusual activity to the SO and CISO.	5.3.b	AU-6	LMH F P
3.6.3	The ISSO shall adjust the level of audit review, analysis, and reporting within the information system when there is a change in risk to TSA operations, assets, or individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.	5.3	AU-6	LMH F P
3.6.4	Audit logs shall be made available immediately to authorized TSA personnel without prior notice or request.	5.3	AU-6	LMH F P
3.6.5	The CISO shall have exclusive approval authority for requests for release of audit and/or logging information outside the TSA IT security environment. Any request for release of audit findings or information shall be submitted to the CISO.	5.3	AU-6	LMH F P
3.6.6	The respective SO shall evaluate system risk related to PII extracts from databases. The SO shall log computer-readable data extracts when the risk is high.	5.3.e	AU-1 AU-2 AU-3 AU-6 PM-9	LMH F P
3.6.7	The SO shall ensure data protection methods are available and for audit upon request from IAD personnel.	5.3	AU-6	LMH F P

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
3.6.8	CISO shall ensure that periodic audits are conducted and laptop log files are reviewed for compliance with DHS and TSA information security requirements.	5.3	AU-6	LMH F P
3.6.9	Reserved			
3.6.10	The ISSO shall review audit records for financial systems or for systems hosting or processing PII on a monthly basis.	5.3.b	AU-6	MH F P
3.6.11	Sponsoring organizations and contractor facilities with TSA IT assets shall conduct an audit of their respective connections on an annual basis to ensure that all existing connections are still needed, and that the access provided meets the Interconnection Security Agreement (ISA).	5.3	AU-6	LMH F P
3.6.12	IAD has the primary responsibility to conduct internal security audits for operational information systems (GSS and MA), as well as for systems and applications under development. IAD shall provide TSA senior management with reports on the effectiveness of IT security by identifying weaknesses and recommending improvements.	5.3	AU-6	LMH F P
3.6.13	The SO shall develop integrated audit review, analysis, and reporting processes for each information system in order to support TSA processes for investigation and response to suspicious activities.	5.3	AU-6 (1)	H F P
3.6.14	The SOC shall ensure that analysis and correlation of audit records are conducted across different repositories to gain organization-wide situational awareness.	5.3	AU-6 (3)	MH F P
3.6.15	The SOC shall ensure that it integrates analysis of audit records with analysis of information system monitoring to further enhance the ability to identify inappropriate or unusual activity.	5.3	AU-6 (5)	H F P
3.6.16	The SOC shall ensure that it correlates information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malicious activity.	5.3	AU-6 (6)	H F P
3.6.17	The SOC shall review and analyze information system audit records for indications of inappropriate or unusual activity: at least weekly for mail servers, monthly for financial systems or systems containing PII, and as required in the SP for all other systems.	5.3	AU-6	H F P

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
3.6.18	The SOC shall ensure inappropriate/unusual activities are reported in information system audit records, to include: a. Activities that might modify, bypass, or negate information security safeguards; b. Security-relevant actions associated with processing; and c. All activities performed using an administrator's identity.	5.3	AU-6	H F P

3.3.7 Audit Reduction and Report Generation (AU-7)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
3.7.1	TSA information systems shall provide an audit reduction and report generation capability.	5.3.h	AU-7	MH
3.7.2	Audit reduction and report generation capabilities shall provide support for near real-time audit review, analysis, and audit reporting as described in this document, and after-the-fact investigations of security incidents.	5.3.h	AU-7	MH
3.7.3	Audit Reduction and reporting tools shall not alter the original audit records.	5.3.h	AU-7	MH
3.7.4	TSA information systems shall provide capability to automatically process audit records for events of interest based on selectable event criteria.	5.3.h	AU-7 (1)	MH
3.7.5	Audit record fields shall require search and/or sort capabilities for: a. Activities that might modify, bypass, or negate information security safeguards; b. Security-relevant actions associated with processing; and c. All activities performed using an administrator's identity.	5.3.h	AU-7 (2)	LMH

3.3.8 Time Stamps (AU-8)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
3.8.1	TSA information systems shall utilize an internal TSA-approved authenticated Network Time Protocol (NTP) server to generate time stamps for audit records. Audit log time stamps are necessary to determine when logged events occurred in the event of in incident.	5.3.i	AU-8	LMH
3.8.2	Time stamps generated by the information system shall include both date and time. The time shall be expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC.	5.3.i	AU-8	LMH
3.8.3	The information system shall compare the internal information system clock with a designated TSA time server source and shall synchronize the system clock to this time server.	5.3.i	AU-8 (1)	MH

3.3.9 Protection of Audit Information (AU-9)

Protection of Audit Information is necessary to preserve the "pristine" state of the logged data for future litigation or other use. The following controls are related to the protection of audit information.

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
3.9.1	TSA Information Systems shall protect audit information and audit tools from unauthorized access, modification, and deletion. Audit information includes all information (to include audit records, audit settings, and audit reports) needed to successfully audit information system activity.	5.3.c	AU-9	LMH F
3.9.2	The SO shall determine privileged access to device audit trail data logs for TSA IT assets under their control.	5.3.c	AU-9	LMH F
3.9.3	The ISSO shall ensure that audit trails and audit logs are protected against unauthorized alteration, loss, unavailability, disclosure, or destruction.	5.3.c	AU-9	LMH F
3.9.4	The SO shall restrict access to audit records to users with privileged accounts.	5.3	AU-9	LMH F
3.9.5	Information systems shall back up audit records, to include incremental and full backups and backup storage onto a physically different system or system component than the system or component being audited.	3.5.2 4.3.1 5.3.c	AU-9 (2)	H F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
3.9.6	The information system shall implement cryptographic mechanisms to protect the integrity of audit information and audit tools.	5.3.c	AU-9 (3)	H F
3.9.7	The AO shall authorize access to management of audit functionality to selected privileged network users with administrator access.	4.1.b	AU-9 (4)	MH F

3.3.10 Non-repudiation (AU-10)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
3.10.1	TSA shall implement mechanisms that shall prevent individuals from successfully challenging the validity of a statement or action produced by an information system.	1.1 5.7.a	AU-10	H

3.3.11 Audit Record Retention (AU-11)

Audit record retention must be in line with retention timelines for the information contained within the logs.

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
3.11.1	ISSO shall ensure audit logs are recorded and retained in compliance with the TSA Records Management Program, Handbook, TSA Records Disposition Schedule, or the DHS Records Schedule. At a minimum, audit trail records shall be maintained online for at least ninety (90) days and preserved for a period of three (3) years as part of managing records for each system to allow audit information to be placed online for analysis with reasonable ease.	5.3.d	AU-11	LMH F
3.11.2	IAD shall retain a copy of all scan results, any corresponding action plans, and action plan completion reports until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes, in compliance with TSA's IT Records Retention guidance.	5.3	AU-11	LMH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
3.11.3	The SO and ISSO shall retain a copy of all audit results, any corresponding action plans, and action plan completion reports until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes, in compliance with TSA's IT Records Retention guidance.	5.3	AU-11	LMH F
3.11.4	Where IR related security incidents have been documented, as defined in IR controls, associated audit records shall be kept in hard copy or digital media for a period of three (3) years after completion of closure activities associated with the incident as required by the National Archive and Records Administration (NARA). This would be IAW RDS 1400.9 "*Computer Security Incident Handling, Reporting, and Follow-up Records.*" Audit records shall then be disposed of in compliance with TSA records management procedures and records disposition schedules (RDS).	5.3	AU-11	LMH F

3.3.12 Audit Generation (AU-12)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
3.12.1	TSA information systems shall provide audit record generation capability for the list of auditable events defined in AU-2.	5.3	AU-12	LMH F
3.12.2	TSA information systems shall allow designated TSA personnel to select which auditable events are to be audited by specific components of the system.	5.3	AU-12	LMH F
3.12.3	Reserved			
3.12.4	TSA information systems shall compile audit records from all active devices into a system-wide logical audit trail that is time correlated to within three milliseconds (0.003 seconds).	5.3	AU-12 (1)	LMH F
3.12.5	TSA information systems shall provide the capability for designated personnel to change the auditing to be performed on a system based on findings within a security event.	5.3	AU-12 (3)	H F

3.3.13 Monitoring for Information Disclosure (AU-13)

Currently, this control does not apply to any control baselines, nor does it apply to Privacy or Financial systems.

3.3.14 Session Audit (AU-14)

Currently, this control does not apply to any control baselines, nor does it apply to Privacy or Financial systems.

3.3.15 Alternate Audit Capability (AU-15)

Currently, this control does not apply to any control baselines, nor does it apply to Privacy or Financial systems.

3.3.16 Cross-Organizational Auditing (AU-16)

Currently, this control does not apply to any control baselines, nor does it apply to Privacy or Financial systems.

3.4 Assessment, Authorization and Monitoring (CA)

TSA periodically assesses security controls to determine their effectiveness in providing an appropriate level of protection. Security controls in an information system are assessed as part of: (1) security authorization or reauthorization; (2) meeting the Federal Information Security Modernization Act of 2014 (FISMA of 2014) requirement for annual assessments; (3) ongoing authorization (OA) per the OA Manager; (4) continuous diagnostics and mitigation (CDM) - when deployed; and (4) testing/evaluation or penetration testing (internal or independent external testing) of the information system as part of the SELC/Agile process. A security control assessment report documents the assessment results in sufficient detail to determine whether the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements of the information system. TSA IT infrastructure and systems undergo security control assessments in compliance with NIST SP 800-37 *Guide for Applying the Risk Management Framework (RMF) to Federal Information Systems* prior to receiving an Authorization to Operate (ATO) by the AO. The Certifying Official (CO) role has been renamed Security Control Assessor (SCA).

Specific detailed guidance of the information security requirements regarding this control family are contained in the *Plan of Action and Milestone (POA&M) Process*, *Security Authorization*, *Ongoing Authorization*, the DHS *Performance Plan*, DHS 4300A PD Attachment B *Waiver Request Form*, DHS 4300A PD Attachment D *Type Accreditation*, DHS 4300A PD Attachment E *FISMA Reporting*, and DHS 4300A PD Attachment H *Plan of Action and Milestones (POA&M) Process Guide*.

Other Guidance: The DHS *Security Authorization Process Guide* describes detailed processes governing the Security Authorization Process.

3.4.1 Assessment, Authorization and Monitoring Policies and Procedures (CA-1)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
4.1.1	The CISO shall develop, disseminate, and annually review/update a formal, documented security assessment and authorization policy. This effort shall address purpose, scope, roles, responsibilities, management commitment, and coordination among TSA entities, and compliance; along with formal, documented procedures to ensure that all information systems are formally assessed through a comprehensive evaluation of applicable security controls.	2.1.3 3.9.e 3.9.n 3.9.1	CA-1 PM-10	LMH F
4.1.2	The AO shall ensure all TSA information systems undergo security assessment and authorization and obtain an ATO prior to operation and deployment. This includes all systems (including pilots) that connect to the TSA network or process TSA sensitive data.	3.9. 3.9. 3.9.	CA-1 PM-4 PM-10	LMH F
4.1.3	The SO shall ensure that FedRAMP-approved cloud service providers (CSPs) are used when acquiring cloud services from external providers and when hosting applications in public cloud services (see NIST SP 800-37 RMF). See TS-072 *Cloud Computing and Virtualization* and TS-049 *Information System Audit Logging* for additional information.	3.18	AC-16 AC-20	LM
4.1.4	The CISO, or designated official, shall perform the security control assessment of all TSA information systems, as directed by the DHS 4300A.	2.1.7.a 3.9	CA-1 PM-10	LMH F
4.1.5	The CISO shall ensure that information security program status data is submitted quarterly and annually to DHS, or as required by the DHS Performance Plan.	3.13.a	CA-2	LMH F
4.1.6	The CFO shall assign the financial systems, which must comply with additional internal controls. The list of additional internal controls must be reviewed and published annually by the TSA Office of the CFO.	3.15.b	CA-1 CA-2	MH F
4.1.7	The CISO shall specify tools, techniques, and methodologies to: assess and authorize information systems, report and manage FISMA data, and document and maintain POA&Ms.	1.4.15 3.9.l	CA-1 PM-4 PM-10	LMH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
4.1.8	The SO shall ensure that information systems that control physical access shall be authorized to operate by the AO and approved by the DHS CSO IAW this policy document, whether they connect to other TSA information systems or not.	2.2.5.a	CA-1 PM-10	LMH F
4.1.9	TSA shall be accepted into the DHS OA Program with the concurrence of the DHS CISO and TSA's CIO and/or AO.	3.9.1.a	CA-1	LMH F
4.1.10	The TSA CFO shall work with the CISO to approve any major system changes to CFO designated systems identified in the TSA inventory and shall be a signature authority on the authorizations to operate.	3.15.m	CA-1 CM-8	MH F
4.1.11	The SO shall implement NIST SP 800-53 security controls, using the FIPS Pub 200, Minimum Security Requirements for Federal Information and Information Systems methodology, based on the FIPS 199 impact level established for each separate security objective (Confidentiality, Integrity, Availability) for the information system.	3.9.a 3.9.b	CA-1 PM-1 PL-1	LMH F
4.1.12	The SO shall utilize Type Security Authorization for information resources that are under the same direct management control; have the same function or mission objective, operating characteristics, security needs, and that reside in the same general operating environment, or in the case of a distributed system, reside in various locations with similar operating environments. Type Security Authorizations shall consist of a master Security Authorization package describing the common controls implemented across sites and site-specific controls and unique requirements that have been implemented at the individual sites. **See *DHS Common Controls Implementation Guide, v2.2 Feb 10, 2015* for additional information and *CIO Memo on Cybersecurity Reciprocity, dated December 20, 2017*.**	3.9.c	CA-1 SC-1	LMH F
4.1.13	TSA enterprise services shall be required to use a DHS-provided catalog of common controls that have been assessed and authorized by the AO of that service.	3.9.w	CA-1	LMH F

3.4.2 Assessments (CA-2)

TSA assesses the security controls in an information system as part of ongoing security authorization or reauthorization, meeting the FISMA requirement for annual assessments, continuous monitoring, and testing/evaluation of the information systems as part of the SELC/Agile process.

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
4.2.1	The CISO, as the SCA, shall ensure that all information systems are formally assessed through a comprehensive evaluation of their security controls.	3.9.e	CA-2 PM-10	LMH F
4.2.2	The SCA shall ensure a security control assessment plan is developed for each security control assessment performed on an information system which includes: a. The security controls and enhancements under assessment; b. Security control assessment procedures and test methodologies used to determine security control effectiveness; and c. A description of the assessment environment, assessment team, and assessment roles and responsibilities.	2.2.9.b 3.9.e 2.1.7.d	CA-2 PM-10 PL-1	LMH F
4.2.3	The Security Authorization Package shall contain the following security documentation: a. Security Plan (SP) and System Design Document (SDD) - if security architecture, information flow and network topology information in the SP requires augmentation; b. Contingency Plan (CP) and results; c. Self-Assessment results; d. FIPS 199 Assessment; e. Security Assessment Report (SAR); f. Privacy Threshold Analysis (PTA); g. Privacy Impact Assessment (PIA); and h. E-Authentication as required. The Security Authorization Package is transmitted from the SO to the SCA.	Glossary Authorization Package 3.14 3.5.2.e 3.9.b 3.14.7	CA-2 PL-5	LMH F P
4.2.4	The SCA shall ensure security control assessments are performed on all TSA information systems that process, store, or transmit sensitive information. The security control assessments shall thoroughly test the implementation of all applicable security controls IAW the security control assessment plan.	2.1.7.d	CA-2 CA-6	LMH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
4.2.5	The SCA shall document the results of the security control assessment in the Security Assessment Report, to reflect the information system's compliance with the security requirements, outstanding POA&Ms, and residual risk.	5.4.8.a	CA-2	LMH F
4.2.6	The SCA shall submit an authorization recommendation to the AO, stating whether or not the system should be authorized to operate based on the results of the security control assessment for each assessed information system.	2.1.7.d	CA-2	LMH F
4.2.7	The AO shall approve the information system's authority to operate based on an evaluation of the security control assessment results and the risk determination.	Not Defined	CA-2	LMH F
4.2.8	The SCA shall ensure that the SO takes action for all remedial actions needed to address security vulnerabilities found during the security control assessment or notify the AO accordingly.	2.1.7.c	PM-4 CA-5	LMH F
4.2.9	A subset of security controls, including any security controls deemed critical, shall be tested through a continuous monitoring process. This testing may be conducted by the ISSO.	3.9.a	CA-2 CA-7	LMH F
4.2.10	The SO shall request a waiver for information systems that are temporarily unable to comply with security authorization assessments, authorizations, or policy.	1.5.1.c	CA-1 CA-2 CA-6	LMH F
4.2.11	A waiver shall be issued per instructions by DHS 4300A, Attachment B *Waiver Request Form*.	1.5.1	CA-2	LMH F
4.2.12	The ISSO shall ensure that each waiver request includes the system name, and system Information Assurance Compliance System (IACS) Inventory ID, operational justification, and risk mitigation.	1.5.1	CA-2 CM-3	LMH F
4.2.13	Reserved			
4.2.14	Reserved			
4.2.15	Security control assessment and authorization documents shall be uploaded and maintained in the DHS IACS tool by the ISSO and IAD.	3.9.m	CA-1 CA-2	LMH F
4.2.16	The AO for a system shall be identified in IACS.	3.9.d	CA-2 CA-6	LMH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
4.2.17	The SO shall ensure that information systems are authorized at initial operating capability (IOC), when a major change occurs to the system, an existing ATO expires, and every three years thereafter.	3.9.h	CA-2	LMH F
4.2.18	For each information system, the SO shall ensure: a. Information security compliance, b. Development and maintenance of security plans, c. Completion of user security training for their systems, d. Notification of officials of the need for security authorization, and e. Officials are alerted when the need for additional resources arises.	2.2.9.d	CA-2	LMH F
4.2.19	The SO is responsible for ensuring that security control assessments of key security controls for CFO Designated Systems are completed annually in IACS and that the security control assessment and SAR are updated annually.	3.15.a	CA-2	MH F
4.2.20	The CISO shall ensure that annual information security control assessments are conducted on all approved wireless systems. Wireless information security control assessments shall enumerate vulnerabilities, risk statements, risk levels, and corrective actions.	4.6.1.a	CA-2 PM-9	LMH F
4.2.21	The CISO and the IAD staff shall continuously monitor the effectiveness of the TSA information security program.	3.10.d	CA-2	LMH F
4.2.22	The ISSO shall utilize the DHS CISO approved automated tool for FISMA reporting.	3.4.d	CA-2	LMH F
4.2.23	The information system's Security Authorization Package shall document the specific procedures, training, and accountability measures in place for systems in compliance with Security Authorization and the DHS Performance Plan.	3.9.n	CA-1	LMH F
4.2.24	The SO shall ensure the Security Authorization Package is completed and maintained for the information system as directed in the DHS Performance Plan and DHS 4300A PD.	3.9.h	CA-6	LMH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
4.2.25	The Security Authorization Package for each information system shall contain a Privacy Threshold Analysis and, as deemed required, a Systems of Records Notice (SORN) and Privacy Impact Assessment.	3.14.2.b	CA-2	LMH F
4.2.26	The Security Authorization Package shall contain a SSI Threshold Analysis (SSI TA), and, as deemed required, a SSI Impact Assessment (SSI IA).	Not Defined	CA-2	LMH F
4.2.27	Type security authorizations consistent with DHS 4300A PD Attachment D *Type Certification* shall be obtained for information systems that: a. Are under the same direct management control; b. Have the same function or mission objective, operating characteristics, security needs; and c. Reside in the same general operating environment, or, in the case of a distributed system, reside in various locations with similar operating environments.	3.9.c	CA-2	LMH F
4.2.28	Type Security Authorization Packages shall consist of a master package describing the common controls implemented across sites and site-specific controls and unique requirements that have been implemented at the individual sites.	3.9	CA-2	LMH F
4.2.29	The CISO shall employ an independent assessment team to conduct an assessment of the security controls for each TSA information system.	3.8.c	CA-2 (1) RA-1	MH F
4.2.30	Penetration testing exercises for both physical and technical controls shall be coordinated by the SO and may be performed as part of the security control assessment.	Not Defined	CA-2 (2)	H
4.2.31	The AO shall approve penetration testing methods.	Not Defined	CA-2 (2)	H F
4.2.32	The AO shall ensure the assessment of at least one third (1/3) of security controls annually **or** IAW the information system's Ongoing Authorization security controls in the IS. This is performed to determine the extent the controls: are implemented, are operating as intended, and are producing the desired outcome.	3.9.1 3.9.f	CA-2	LMH F

3.4.3 Systems Interconnections (CA-3)

The TSA network interconnects with networks external to TSA such as DHS, DHS components, other Government agencies, and commercial entities working with TSA. TSA carefully considers the risk that may be introduced when information systems are connected to other systems with different security levels and controls, both within the organization and external to TSA.

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
4.3.1	The CISO shall ensure that interconnections between TSA systems and non-DHS systems (including systems and networks owned by other Federal agencies) are documented based on interagency agreements, Memoranda of Understanding (MOU), Service Level Agreements (SLA), or interconnection Security Agreements (ISA) prior to activation. See DHS 4300A 5.4.3.f for additional details.	5.4.3.g 5.4.3.f	CA-3	LMH F
4.3.2	The CISO shall ensure that interconnections between TSA systems and DHS OneNet are documented with an ISA signed by the OneNet AO and the TSA AO.	5.4.3.c 5.4.3.g	CA-3	LMH F
4.3.3	The CISO shall ensure that interconnections between TSA systems and systems owned by other DHS Components are documented with a signed ISA.	5.4.3.f	CA-3	LMH F
4.3.4	The CISO shall ensure that interconnections between TSA and non-TSA systems shall be established through the Trusted Internet Connection (TIC) and by approved service providers.	5.4.3.b	CA-3	LMH F
4.3.5	The CISO shall ensure ISAs are established for information systems connecting to TSA networks consistent with DHS 4300A PD Attachment N *Interconnection Security Agreements.*	5.4.3.c	CA-3	LMH F
4.3.6	Interconnections between two authorized DHS systems do not require an ISA if the interface characteristics, security requirements, nature of information communicated and monitoring procedures for verifying enforcement of security requirements are accounted for in the SPs or are described in another formal document, such as an SLA or contract, and the risks have been assessed and accepted by all involved AOs.	5.4.3.m	CA-3	LMH F
4.3.7	The CISO shall ensure that the information system connections are monitored on an ongoing basis verifying enforcement of security requirements.	2.1.9	SI-4	LMH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
4.3.8	ISSOs shall review ISAs annually, update and, if still required, reissue and sign them every three (3) years (or whenever any significant changes have been made to any of the interconnected systems) as a part of the annual FISMA self-assessment.	5.4.3.d 5.4.3.e	CA-3	LMH F
4.3.9	The AO shall grant a maximum of two Interim Authorizations to Operate (IATOs) for pilot systems. Pilot systems shall not be connected to, or deployed as, an operational system until an ATO is authorized.	3.9.i 3.9.j	CM-2 CM-4 PL-1	LMH F
4.3.10	The AO shall ensure to test, authorize, and approve all new and revised software and hardware prior to implementation in accordance with their CM Plan.	4.8.3.c	CM-2	LMH F
4.3.11	ATOs for Pilot systems shall not exceed ninety (90) days and these systems shall be removed from the operational network unless an extension is approved by the AO.	Not Defined	CA-3	LMH F
4.3.12	In the event there is a requirement to interconnect systems where one or more of the systems do not have an ATO, the AO may grant an Interim Authority to Operate (IATO) for an initial period not to exceed six (6) months. The intent of an IATO is to provide a limited authorization to operate development, testing, or prototype systems under specified terms and conditions. Under special circumstances, the AO may grant an additional six (6) month extension at their discretion. There are certain circumstances where an Interconnection Security Agreement (ISA) would be required to support the connection of a system with an IATO. ISA's are particularly relevant when connecting systems with two or more different AO's. See Section 3.4.6 Authorization (CA-6) for additional requirements concerning IATOs.			
4.3.13	The CISO shall permit the use of a single ISA for multiple connections provided that the security Authorization is the same for all connections covered by that ISA.	5.4.3.h	CA-3	LMH F
4.3.14	Reserved			
4.3.15	Granting the ability to log into one TSA system through another TSA system does not require an ISA.	5.4.3.n	CA-3	LMH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
4.3.16	TSA shall document all interconnections to the DHS OneNet with an Interconnection Security Agreement (ISA) signed by the OneNet AO and by each appropriate AO. Additional information on ISAs is published in the, *Preparation of Interconnection Security Agreements,* Attachment N to the DHS 4300A Sensitive Systems Handbook. Interconnections between DHS and non-DHS systems shall be established only through the TIC and by approved service providers. The controlled interfaces shall be authorized at the highest security level of information on the network.	5.4.3	CA-3 (5)	MH F

3.4.4 Security Certification (CA-4) (Withdrawn: Incorporated into CA-2)

This control has been withdrawn by NIST and is no longer in force.

3.4.5 Plan of Action and Milestones (CA-5)

FISMA legislation mandates that all federal departments and agencies develop and implement a corrective action plan, known as a POA&M, to identify and resolve information security weaknesses and periodically report progress to OMB and Congress.

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
4.5.1	The CISO shall ensure that the POA&M process is used by the SO to document and manage the planned remedial actions to mitigate vulnerabilities, correct deficiencies in security controls, and remediate weaknesses for the TSA enterprise.	3.9.o	CA-5 PM-4	LMH F
4.5.2	The SO shall ensure that the POA&M process is used to document and manage the planned remedial actions to mitigate vulnerabilities, correct deficiencies in security controls, and remediate weaknesses for specific information systems. The scheduled completion date for system POA&Ms is within one year of POA&M creation and within 6 months for CFO designated systems and high value assets (HVAs).	3.9.o	CA-5 PM-4	LMH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
4.5.3	The CISO shall be responsible for ensuring the development and maintenance of *enterprise-level* POA&Ms when vulnerabilities, deficiencies, or weaknesses impact multiple information systems across different program offices. CISO shall also establish, implement, and enforce CM controls on all information systems and networks, and address significant deficiencies as part of a POA&M.	3.7.b	CA-5 PM-4	LMH F
4.5.4	The Program Manager shall be responsible for ensuring the development and maintenance of *program-level* POA&Ms when vulnerabilities, deficiencies, or weaknesses impact multiple information systems across the respective program office.	2.2.8.a 3.7.b	CA-5 PM-4	LMH F
4.5.5	The CISO shall ensure copies of enterprise-level POA&Ms are provided to the SO and ISSO of impacted information systems as needed.	2.1.3	CA-5 PM-2	LMH F
4.5.6	The Program Manager shall ensure copies of program-level POA&Ms are provided to the SO and ISSO of impacted information systems as needed.	2.2.8.c	CA-5 PM-4	LMH F
4.5.7	The SO shall ensure development and maintenance of POA&Ms to address weaknesses and deficiencies in the information system and its environment of operation, which remain after Security Authorization or other testing.	2.2.9.e	CA-2 CA-5	LMH F
4.5.8	The SO shall establish, implement, and enforce configuration management controls on all information systems and networks and address significant deficiencies as part of a POA&M.	3.7.b	CA-5 CM-3 PM-4	MH F
4.5.9	The CISO shall be responsible for prioritizing *enterprise-level* security weakness for correction or mitigation.	2.1.7.d	CA-5 PM-4	LMH F
4.5.10	The SO shall ensure creation of a POAM and be responsible for addressing and prioritizing *information system* security weaknesses for correction or mitigation.	2.2.9.e	CA-5 PM-4	LMH F
4.5.11	The ISSO shall be responsible for working with the SO to document weaknesses in POA&Ms and initiate corrective action.	Not Defined	CA-5	LMH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
4.5.12	POA&Ms shall address: (1) the known vulnerabilities in the information system, (2) the security categorization of the information systems, (3) the specific weaknesses or deficiencies in the information system security controls, (4) the importance of the identified security control weakness or deficiencies, (5) the proposed risk mitigation approach to address the identified weaknesses or deficiencies in the security controls, (6) compensating controls in place, and (7) the rationale for accepting certain weaknesses or deficiencies in the security controls.	2.2.8.d	CA-5	LMH F
4.5.13	POA&Ms shall be generated in compliance with DHS 4300A PD Attachment H - *POA&M Process Guide* and TSA POAM policy. .	3.9	CA-5	LMH F
4.5.14	All POA&Ms shall be documented within the Security Authorization Package.	Not Defined	CA-5	LMH F
4.5.15	A POA&M shall be developed to address wireless information security vulnerabilities. These plans shall prioritize corrective actions and implementation milestones IAW defined risk levels.	4.6.1.b	CA-5 PM-4 PM-9	LMH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
4.5.16	POA&Ms shall not exceed the maximum duration for closure based on FIPS 199 impact levels for the system: **45 days (**for ***high*****), 60 days (**for ***moderate*****),** and **90 days (**for ***low*****). NOTE: Based on directions from the *DHS USM Memo titled "Strengthening DHS Cyber Defenses" (July 22, 2015),* a unique type of "High" impact level classified as "*Critical*" may be used under certain circumstances and in response to escalation in cyber related attacks. Weaknesses or vulnerabilities identified as *Critical* by the National Cybersecurity Assessment and Technical Services (NCATS) must be mitigated within 30 days. This *Critical* impact is also supported by the *Binding Operational Directive (BOD) 15-01: "Critical Vulnerability Mitigation Requirement for Federal Civilian Executive Branch Departments' and Agencies' Internet-Accessible Systems".* In these special cases, subsequent instructions shall be forthcoming and at the discretion of the IT Authorizing Official (AO). Those systems not in compliance with this internal 30-day requirement risk having their system(s) shutdown or removed from the network.**	POAM Not Defined BOD 15-01	CA-5	LMH F
4.5.17	The SO shall implement a migration plan and associated POA&Ms for legacy wireless systems and mobile devices that are not compliant with DHS or TSA policy. Operation of these noncompliant systems before and during the migration requires an approved waiver from the DHS CISO.	4.6.1.e 4.6.2.j	CA-5	LMH F
4.5.18	Waiver requests shall include POA&M identification (as applicable), description, justification, and a risk assessment, identifying remediation plans and compensating controls.	1.5.1	CA-5 PM-4	LMH F
4.5.19	The CISO shall request a waiver from the DHS CISO if a key control weakness, as prescribed in DHS 4300A Attachment R, *Compliance Framework Guide* is identified for a CFO Designated System and not remediated within twelve (12) months.	3.15.j	CA-5CA-7	MH F

3.4.6 Authorization (CA-6)

Security authorization is the official management decisions given by the Authorizing Official (a senior TSA official or executive to authorize operation of an information system and to explicitly accept the risk to TSA operations and assets, individuals and organizations). TSA requires a security authorization for each information system connecting to the network.

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
4.6.1	The CIO shall act as the AO or shall designate another Federal employee as the AO, in writing, for TSA information systems (other than those systems designated as Financial Systems, where the CFO serves as the AO).	2.1.6.b 2.2.5.b 2.2.7.b 2.2.9	CA-6	LMH F
4.6.2	The AO shall perform additional duties in compliance with NIST SP 800-37 RMF	2.1.6.c 2.1.6.g 3.9.1.h	CA-6	LMH F
4.6.3	The AO shall formally assume responsibility for the operations of each information system at an acceptable level of risk.	2.1.6.f	CA-6 PM-10	LMH F
4.6.4	Reserved			
4.6.5	Reserved			
4.6.6	The AO shall ensure that system operation with sensitive information is prohibited without an ATO.	3.9.q	CA-6	LMH F
4.6.7	The TSA CISO shall serve as the TSA Risk Executive.	2.1.5.b	PL-1 PM-9	LMH F
4.6.8	The DHS CISO shall approve the use of all TSA information system, government-owned mobile devices, and non-TSA equipment and software that process, store, or transmit sensitive information.	2.1.6 4.6.2.l 4.8.2.a	CA-6 SA-6	LMH F
4.6.9	The AO shall be responsible for the acceptance of resulting risks to TSA operations and assets, individuals, other organizations, and the Nation.	2.1.6.e 3.9.q	CA-6	LMH F
4.6.10	The AO shall periodically review the security status of individual systems to determine if the risk level remains acceptable.	2.1.6.f	CA-6	LMH F
4.6.11	The SO shall be responsible for ensuring the terms and conditions of the ATO for an information system.	3.9.r	CA-6 PM-10	LMH F
4.6.12	ATOs shall only be granted to information systems that fully comply with policy, document resultant risk within POA&Ms or have been granted appropriate waivers.	3.9.r	CA-6 CA-1 PM-10	LMH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
4.6.13	Systems shall be authorized at initial operating capability and every three (3) years thereafter, or whenever a major change occurs, whichever occurs first, or as defined by the system's ongoing authorization agreement. Per the discretion of the AO, the ATO duration may be from 6 months to 3 years. ATOs of six (6) months or less shall receive concurrence and an ATO authorization period waiver from the DHS CISO before submission to the AO for final Authorization decision.	3.9.h	CA-6 PM-10	LMH F
4.6.14	The AO may revoke an ATO of a TSA information system.	3.9.u	CA-6 CA-1	LMH F
4.6.15	An IATO may be granted at the discretion of the AO, for systems that are undergoing development, prototyping, or pilot testing for an initial period not to exceed six (6) months. IATOs provide limited authorization to operate development, testing, or prototype systems under specified terms and conditions. The AO may grant an additional six (6) month extension at their discretion under special circumstances.	3.9.i	CA-6 PL-1 PM-10	LMH F
4.6.16	All IATO request shall be carefully reviewed and assessed on a case-by-case basis by IAD SMEs and additional conditions and requirements shall be added or removed at the discretion of the CISO and AO.	3.9.i	CA-6 PL-1 PM-10	LMH F
4.6.17	Production data, including Personal Identifiable Information (PII) or Sensitive PII (SPII) shall not reside on any systems granted an IATO. An IATO does not authorize storage, access, processing, transmission or reviewing of real world production data.	3.9.i	CA-6 PL-1 PM-10	LMH F
4.6.18	Entities requesting an IATO must have an Enterprise Architecture (EA) Critical Design Review (CDR) approval letter approving the design prior to IATO implementation.	3.9.i	CA-6 PL-1 PM-10	LMH F
4.6.19	The system owner (SO) shall notify and obtain approval from IAD management prior to committing resources in the pursuit of an IATO.	3.9.i	CA-6 PL-1 PM-10	LMH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
4.6.20	In support of an IATO request, the network firewall shall be operational at all perimeter ingress and egress points and shall be tuned, configured, and settings enabled to "deny all" but to "allow by exception". These exceptions shall permit specific traffic request access to an IATO related system in direct support of the operational development and testing environment and restricts all other traffic. The firewall(s) shall not be configured with the presumptive production rules and open access from the internet is not permitted.	3.9.i	CA-6 PL-1 PM-10	LMH F
4.6.21	Firewall rule sets shall be provided to IAD SME for review and assessment in conjunction with all IATO requests.	3.9.i	CA-6 PL-1 PM-10	LMH F
4.6.22	Modification of firewall configurations supporting an approved IATO shall be permitted following approval from IAD. Firewall rules may require modification to the 'as designed' production ruleset to achieve operational readiness and support Security Authorization testing (i.e., security control assessment (SCA)).	3.9.i	CA-6 PL-1 PM-10	LMH F
4.6.23	For all IATO requests, IAD shall facilitate ISSOs with the *Nessus Vulnerability and Compliance* (NVC) plug-in tool in order to scan all IATO-related systems prior to implementation. ISSOs shall provide final/clean NVC scan results in HTML format to IAD on a monthly basis.	3.9.i	CA-6 PL-1 PM-10	LMH F
4.6.24	IATO systems requiring anti-virus (AV) and anti-malware (AM) protections within its appropriate boundaries shall have an operational, as well as updated AV/AM protections using an approved product.	3.9.i	CA-6 PL-1 PM-10	LMH F
4.6.25	IATO system audit logging reviews shall be conducted and recorded by the vendor together with ISSO on a weekly basis. The targets of the audit reviews are privileged accounts, all user access, firewall(s), and the antivirus solution.	3.9.i	CA-6 PL-1 PM-10	LMH F
4.6.26	In the event scans are conducted and cybersecurity related anomalies, incidents, or vulnerabilities are identified, the vendor shall provide a written response to IAD regarding mitigation and resolution efforts to contain of correct the finding. The IAD CND Branch Manager shall also be informed of these findings.	3.9.i	CA-6 PL-1 PM-10	LMH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
4.6.27	A DHS Trusted Internet Connection (TIC) *may* not be required in order to request an IATO. However, connectivity and interoperability achievability will need to have been scoped, socialized, and technically evaluated with positive results.	3.9.i	CA-6 PL-1 PM-10	LMH F
4.6.28	An approved systems design document (SDD) or network topology document shall be provided to IAD, which illustrates the network design and architecture of the system interconnection for which the IATO is being requested.	3.9.i	CA-6 PL-1 PM-10	LMH F
4.6.29	Internal and external data flow diagrams shall be provided to IAD that includes, but is not limited to: ports, protocols, and services enabled by the architecture for which the IATO is being requested.	3.9.i	CA-6 PL-1 PM-10	LMH F
4.6.30	The Key Decision Point three (3) milestone in the SELC shall not be passed until the ATO for the information system is granted.	3.9.i	CA-6 PL-1 PM-10	LMH F
4.6.31	IATOs shall not be used for operational systems.	3.9.i	CA-6 PL-1 PM-10	LMH F
4.6.32	The AO shall grant an IATO for a maximum period of six (6) months and may grant one (1) six (6) month extension.	3.9.i	CA-6 PL-1 PM-10	LMH F
4.6.33	Systems under an IATO shall not process sensitive information but may attach to system networks for testing purposes.	3.9.i	CA-6 PL-1 PM-10	LMH F
4.6.34	Systems that have not received a full ATO by the end of the IATO extension shall not be deployed.	3.9.j	CA-6 PM-10	LMH F
4.6.35	Documents shall remain valid during an ATO.	3.9.s	CA-6	LMH F
4.6.36	The Security Authorization Package and the Security Authorization Decision Letter (which contains the Authorization Decision, Decision Rationale, accepted Residual Risk level, and Terms & Conditions for Authorization) shall be routed from the SO (through the SCA) to the AO for ATO approval.	3.9.c	CA-6	LMH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
4.6.37	Approved waivers shall be reported in TSA's FISMA report.	1.5.1	CA-6	LMH F
4.6.38	The component CISO shall approve all waiver requests prior to submitting them to the DHS CISO.	1.5.1	CA-6	LMH F
4.6.39	Requests for waivers shall not be submitted without sufficient information and justification	1.5.1	CA-6	LMH F
4.6.40	Waivers for TSA financial systems shall be reviewed by the TSA CISO and TSA CFO prior to submittal to the DHS CISO.	1.5.1	CA-6	MH F
4.6.41	The TSA Privacy Officer shall approve all requests for waivers for Privacy Sensitive Systems prior to submitting them to the DHS CISO.	1.5.1	CA-6	MH F
4.6.42	The TSA AO shall concur on any waiver request that results in a total waiver time exceeding twelve (12) months before sending it to the DHS CISO.	1.5.1	CA-6	LMH F
4.6.43	Waivers exceeding twelve (12) months shall be reported as a material weakness in the TSA FISMA report.	1.5.1	CA-6	LMH F
4.6.44	The TSA CFO shall confirm that the published list of CFO Designated Systems from the DHS CFO contains all TSA financial systems.	2.2.7.d	CA-6	MH F
4.6.45	A waiver request for access to Internet Webmail (e.g. Gmail, Yahoo mail, AOL mail) or other personal email accounts over DHS furnished equipment or network connections or to perform Government business is submitted by memorandum for approval by the TSA CIO, then routed to the DHS CISO and DHS CIO for an IT security review and endorsement, and submitted to the Under Secretary for Management (USM) for final approval.	1.5.1.i	CA-6	LMH
4.6.46	ATOs shall be rescinded if the information system fails to comply with mandated testing and reporting requirements.	3.15.l	CA-6	LMH F
4.6.47	Information systems containing PII shall not be designated operational until a SORN has been published in the Federal Register for thirty (30) days.	3.14.4.b	CA-6	MH F
4.6.48	The Privacy Office and ISSO shall review and republish SORNs every two (2) years.	3.14.4.c	CA-6	MH F

3.4.7 Continuous Monitoring (CA-7)

TSA ensures continuous monitoring by ensuring the organization assesses security controls of information systems for compliance on a periodic basis.

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
4.7.1	The CISO shall establish a continuous monitoring strategy and program for implementation by the SO and ISSO in alignment with the DHS Performance Plan.	3.10.b	CA-7	LMH
4.7.2	The CISO shall ensure that NIST 800-53A is used for assessing the effectiveness of security controls and for quarterly and annual FISMA reporting.	3.10.c	CA-7	LMH
4.7.3	The SO shall establish continuous monitoring processes and procedures for the information system in compliance with DHS and TSA guidance.	3.10.b	CA-7 PL-1 PM-10	LMH
4.7.4	The ISSO shall consider the security impact analysis results of proposed changes to the information system and environment.	3.7.h	CM-4	LMH F
4.7.5	The SO, in collaboration with the ISSO, shall maintain an ongoing security control assessment to continuously monitor (and improve as needed) the security state of the information system in compliance with NIST 800-137.	2.1.9 3.10	CA-7	LMH
4.7.6	The ISSO shall report security status of information systems to the CISO as required by the DHS Performance Plan and DHS and TSA policy and procedures.	Not Defined	CA-7 CA-2	LMH F
4.7.7	The ISSO shall conduct security reviews of the information system in compliance with FIPS 200 and NIST SP 800-53 guidance.	3.10.c	CA-7	LMH
4.7.8	Reserved			
4.7.9	The ISSO shall ensure server administration is conducted in a secure manner.	5.4.6.f	AU-6 CA-7 CP-9 CM-6 SC-1 AU-3 AU-12	LMH F
4.7.10	The TSA Security Operations Center (SOC) is responsible for monitoring system and application logs.	2.1.11, 5.4.2	SI-4	LMH
4.7.11	Reserved			

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
4.7.12	The CISO shall establish an information system security review and assistance program to provide the SO with expert review of programs, to assist in identifying deficiencies, and to provide recommendations for bringing systems into compliance.	3.10.b	CA-7 PL-1 PM-10	LMH
4.7.13	The CISO shall ensure that independent assessors or assessment teams assess security controls in the information system on an ongoing basis and IAW Continuous Monitoring program requirements.	2.1.7 3.9	CA-7 (1)	MH
4.7.14	The CISO shall ensure the establishment of a monitoring strategy based on metrics, as defined by the DHS Continuous Monitoring strategy and the system's ongoing authorization schedule or one third (1/3) of security controls annually.	3.10 5.4.2 5.4.8	CA-7	LMH

3.4.8 Penetration Testing (CA-8)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
4.8.1	Penetration testing exercises for both physical and technical controls shall be coordinated by the SO and performed as part of a security control assessment.	Not Defined	CA-8	H
4.8.2	The AO shall approve all penetration testing methods prior to testing.	Not Defined	CA-8	H
4.8.3	The CISO shall authorize penetration testing on TSA information systems through advanced coordination with the AO, SOC, SO, ISSO, and other offices/personnel as appropriate.	Not Defined	CA-8	H

3.4.9 Internal System Connections (CA-9)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
4.9.1	The AO or delegated authority shall authorize and ensure documentation of each internal connection and security requirement to information systems prior to connection.	Not Defined	CA-9	LMH

3.5 Configuration Management (CM)

TSA IT assets operate as a homogenous environment through the proper configuration of network elements and the consistent employment of standard practices. The configuration of network elements is defined through technical standards and DHS Configuration Guidance while standard practices are enforced through the application of uniform processes and procedures. Configuration changes to TSA information systems, applications, or network components may introduce risks to this environment. In order to determine the level of risk potentially introduced and to ensure that proper approvals for risk acceptance are acquired, configuration changes to the TSA IT environment (including systems, software, infrastructure architecture, and IT assets) must be communicated and planned for appropriately.

Specific detailed configuration management guidance is also contained in TSA TS-006 *Network Intrusion Detection and Prevention Systems*, TS-007 *Host Intrusion Detection Systems*, TS-036 *Infrastructure Asset Security*, TS-037 *Server Security*, TS-025 *VPN*, and TS-049 *Information Systems Logging.*

Other guidance: DHS Inventory Methodology v11.0, NIST SP 800-12, NIST SP 800-70, NIST SP 800-100, NIST SP 800-128, OMB Memoranda 07-11, 07-18, and 08-22.

3.5.1 Configuration Management Policy and Procedures (CM-1)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
5.1.1	The CISO shall develop, disseminate, and annually review/update a formal, documented configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among TSA entities, and compliance; and formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.	2.1.3 3.7	CM-1 PL-1 PM-2	LMH F
5.1.2	The SO and ISSO shall work together to develop, and maintain a documented configuration management plan (CMP) that reflects the configuration management procedures and specific configuration controls for an information system as part of each SP.	3.7.a	CM-1 CM-9	LMH F
5.1.3	Reserved			
5.1.4	The CMP for each information system shall address purpose, scope, roles, responsibilities, coordination among TSA entities, and compliance with DHS Configuration Guidance and TSA Technical Standards.	3.7	CM-1	LMH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
5.1.5	The CMP shall encompass all Configuration Items (CI) of the information system that are configurable and/or versionable, including, but not limited to: a. Hardware b. Firmware c. Operating systems d. Network devices (including firewalls, routers, and switches) e. Authorized router and switch management stations and databases f. Software applications g. Network security assets, including intrusion detection systems (IDS) and intrusion prevention systems (IPS) h. Access rule sets and ACLs.	3.7	CM-1	LMH F
5.1.6	Each CI shall be identified within the CMP by brand, model, version/release, network topology, the logical placement of the component within the system architecture, and other distinguishing characteristics.	3.7	CM-1	LMH F
5.1.7	All TSA employees, contractors, and vendors (including managers, operators, administrators, and users of TSA IT assets) shall maintain the information system IAW the CMP.	3.7	CM-1	LMH F

3.5.2 Baseline Configuration (CM-2)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
5.2.1	The ISSO shall develop a CMP as part of the SP for the information system documenting the initial system configuration in detail.	3.7.d	CM-2 CM-9	LMH F
5.2.2	The ISSO shall update the CMP and maintain the document under configuration control to reflect all subsequent changes to the information system.	3.7.d	CM-2 CM-3 CM-9	LMH F
5.2.3	The SO shall ensure that the information system is maintained and configured per the documented CMP.	3.7 4.8.3.a	CM-2	LMH F
5.2.4	Assets not included in the DHS Technical Reference Model (TRM) or **Technical Solutions Portfolio (Tech SP)** are strictly prohibited from use within TSA.	3.1.g	CM-2 (4)	LMH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
5.2.5	The SO shall ensure that all configurations are in compliance with: the TS-036 *Infrastructure Asset Security;* DHS Sensitive Systems Handbook, Enclosure 1, including the DHS Secure Baseline Configuration Guidance; applicable TSA configuration guidance; DISA Security Technical Implementation Guides (STIGs); the Center for Internet Security (CIS)-Configuration Assessment Tool (CAT) benchmark; and TS-008 End User Assets.	3.7 4.8.3.a	CM-2	LMH F
5.2.6	The CISO shall ensure that IT assets found connected to a TSA information system and not documented within the CMP are reported as potential security violations and immediately disconnected until justified and documented.	3.7	CM-2	LMH F
5.2.7	The configuration baseline for Basic Input Output System (BIOS) for all applicable IT assets shall be reset to the default manufacturer setting before disposal. See TS-073 for BIOS Protection.	Not Defined	MP-6	LMH
5.2.8	Workstations, laptops, and tablets shall be configured and managed in compliance with TS-008 End User Assets and DHS configuration guidance on the U.S Government Configuration Baseline (USGCB). Configurations shall include installation of the DHS Common Policy Object Identifier (OID), Common Policy Framework Root CA certificate, and the DHS Principal CA certificate.	3.7.e	CM-2 CM-6 CM-9	LMH F
5.2.9	Only approved end user asset peripherals (to include removable devices, keyboards, microphones, etc.) are authorized to connect to TSA's systems IAW TS-008 *End User Assets*. Headphones, speakers, and other personal assets not possessing persistent memory may be connected at the discretion of an individual's manager.	Not Defined	CM-2	LMH F
5.2.10	BIOS controls shall be protected from modification by employing controls such as restricted permissions and shall be documented in the SP.	Not Defined	CM-2	LMH F
5.2.11	Equipment such as servers, routers, switches, and hubs shall be configured and managed IAW TS-037 *Server Security* and DHS Secure Baseline Configuration Guidance.	4.8.3.a	CM-2	LMH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
5.2.12	IDS and IPS shall be configured and managed in compliance with TS-006 *NIDS*, TS-007 *HIDS*, TS-072 CCV, DHS Secure Baseline Configuration Guidance.	4.8.3.a	CM-2	LMH F
5.2.13	Database configurations shall comply with the DHS Secure Baseline Configuration Guidance as well as TSA and DHS policy.	Not Defined	CM-2	LMH F
5.2.14	The IT POC shall ensure that network printers and facsimile machines are updated to the latest version of their firmware and software at least annually.	4.12.b	CM-2	LMH F
5.2.15	The CISO shall ensure adequate physical and information security measures are implemented for all TSA-owned Private Branch Exchanges (PBX) in compliance with NIST SP 800-24 *PBX Vulnerability Analysis*.	4.4.1.a	CM-2 PE-2	LMH F
5.2.16	All Land Mobile Radio (LMR) systems shall comply with Project 25 (P25, Telecommunications Industry Association (TIA), EIA-102) security standards (where applicable).	4.6.3.g	CM-2	LMH F
5.2.17	Sponsoring organizations and contractor facilities with TSA IT assets shall conduct an audit of their respective connections on an annual basis to ensure that all existing connections are still needed, and that the access provided meets the ISA.	5.4.3.e	CM-2	LMH F
5.2.18	Approved protected network services (PNS) shall be used as cost-effective alternatives to the use of encryption for sensitive information requiring telecommunications protection.	4.5.1.a	CM-2	LMH F
5.2.19	The ISSO shall ensure the underlying email operating system is correctly secured, installed, and configured and that prohibited operating system is not used.	5.4.6.a	CM-2	LMH F
5.2.20	The ISSO shall ensure mail server software is correctly secured, installed, and configured.	5.4.6.b	CM-2 SI-6	LMH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
5.2.21	On an annual basis, the ISSO shall review and update the baseline configuration of an information system: a. Due to a change in an information system; b. Due to a system's environment change of operation such as new hardware, software, firmware, or new system connections; c. Due to a re-authorization; or d. As part of installations and upgrades IAW the configuration management process.	Not Defined	CM-2 (1)	MH F
5.2.22	Automated mechanisms shall be employed to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.	Not Defined	CM-2 (2)	H F
5.2.23	A historical log of changes for current and all previous IT asset configurations for the prior twelve (12) months shall be maintained by the SO until disposal of the system.	Not Defined	CM-2 (3) AU-6	MH F
5.2.24	Reserved			
5.2.25	Reserved			
5.2.26	The SO shall ensure that: information systems, system components, or devices (such as notebook computers, tablets, or mobile devices) being located in potentially high-risk areas implement additional security and configuration controls to counter any threats in such areas and upon return from those areas.	Not Defined	CM-2 (7)	MH F

3.5.3 Configuration Change Control (CM-3)

Only TSA tested, approved, and released configuration items shall be made part of TSA IT assets without the separate approval of TSA IT IAD. This includes all test and monitoring equipment and local prototyping laboratories, test and development environments. The CM-3 control deals with the actual installation of new IT assets (to include hardware, software, firmware, test equipment, data/traffic analysis probes and/or appliances, etc.) into the production TSA IT environment as either a controlled change or as a result of a maintenance action in support of a system's engineering life cycle process. Controlling the installation of new objects is a critical element in the defense-in-depth security approach and provides protection from direct access to systems by unauthorized individuals or applications in order to provide the Confidentiality, Integrity, and Availability of information.

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
5.3.1	The Systems Change Control Board (SCCB), as established by the CIO, shall meet twice a week to coordinate and provide oversight for configuration change control activities for all TSA prime contractor (example: Information Technology Infrastructure Program (ITIP)) supported systems.	Not Defined	CM-3	LMH F
5.3.2	Non contractor supported systems shall maintain their own equivalent SCCBs.	Not Defined	CM-3	LMH F
5.3.3	The SCCB shall be notified, authorize, and approve of all configuration changes to TSA contractor supported systems, software, hardware, infrastructure architecture, and IT assets prior to implementation.	Not Defined	CM-3	LMH F
5.3.4	The SCCB shall review and formally approve (or deny) all Requests for Change (RFCs) prior to implementation into the TSA contractor supported production environments.	Not Defined	CM-3	LMH F
5.3.5	The ISSO shall ensure that documentation associated with an approved change to an information system is updated to reflect the appropriate baseline.	Not Defined	CM-3	LMH F
5.3.6	The SCCB shall ensure that TSA contractor supported systems that interface with DHS OneNet shall have RFCs submitted to the DHS OneNet CCB.	Not Defined	CM-3	LMH F
5.3.7	The CISO shall ensure information security inclusion and oversight in the SCCB by designating IAD staff as SCCB participants with RFC voting privileges.	Not Defined	CM-3	LMH F
5.3.8	The SO of contractor-supported systems shall notify the AO immediately when any security features are disabled in response to time-sensitive, mission-critical incidents or other emergency change activity.	4.6.3.a	CM-3	LMH F
5.3.9	The CISO shall ensure activities associated with configuration-controlled changes to the system are evaluated as part of the assessment and authorization process and are periodically audited.	3.7	CM-3	LMH F
5.3.10	The SO of contractor-supported systems shall ensure all system changes are submitted to the SCCB for approval prior to implementation.	4.8.3.c	CM-2	LMH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
5.3.11	The SO shall ensure that system documentation is updated to reflect the appropriate baseline either annually or when significant system changes occur. Types of changes triggering documentation updates include: a. New threat information; b. Weaknesses or deficiencies discovered in currently deployed security controls after an information system breach; c. A redefinition of mission priorities or business objectives resulting in a change to the security category of an information system; and d. A change in an information system (to include adding new hardware, software, or firmware and establishing new connections) or the system's environment of operation.	3.7 4.10.b	CM-3 CM-8 SA-5	LMH F
5.3.12	Documented changes to TSA contractor supported systems shall include configuration identification, configuration change management, configuration status accounting, and configuration verification and audit.	3.7	CM-1	LMH F
5.3.13	The approved TSA RFC shall be used to initiate any configuration change to TSA contractor supported systems and IT assets.	Not Defined	CM-3	LMH F
5.3.14	An RFC shall be submitted to the SCCB when a change is requested for any Configuration Items (CI) for any FISMA IT system, including, but not limited to: a. Hardware b. Firmware c. Operating systems d. Network devices including firewalls, routers, and switches e. Databases f. Software applications (enterprise level changes) g. Network security assets including IDS and IPS h. Access rule sets and ACLs i. Network configurations	Not Defined	CM-3	LMH F
5.3.15	System configuration documentation shall be protected as Sensitive, if deemed appropriate by the CISO.	4.10.d	CM-3	LMH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
5.3.16	Configuration documentation shall be maintained and be accessible to authorized personnel (including auditors) at all times.	4.10.c	CM-3 SA-5	LMH F
5.3.17	The configuration control and release procedures shall mandate development, procurement, identification, and release of affected documentation. Documentation release shall be concurrent with functional change development.	Not Defined	CM-3 PL-1	MH F
5.3.18	SCCB shall ensure the RFC tools automatically process RFCs, notify RFC approval authorities, highlight approvals that have not been received by the SCCB, inhibit change until the RFC is approved, and document completed changes to the information system.	Not Defined	CM-3 (1)	H F
5.3.19	The SO shall ensure all new and revised software and hardware is tested within a test environment, validated, and documented prior to implementation.	Not Defined	CM-3 (2)	MH F
5.3.20	Reserved			
5.3.21	The SO and ISSO shall prepare and approve RFCs prior to their submission to the SCCB.	Not Defined	CM-3	LMH F

3.5.4 Security and Privacy Impact Analysis (CM-4)

Security impact analyses are conducted by TSA to determine potential security impacts to the information system prior to change implementation. Security impact analysis shall also include an assessment of risk to understand the impact of the changes and to determine if additional security controls are required. The security impact analysis is scaled IAW the security categorization of the information system.

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
5.4.1	The ISSO shall analyze changes to the information system design, physical environment, or user community to determine potential security impacts prior to change implementation.	3.7.h	CM-4	LMH F
5.4.2	The SO and the SCCB shall include and consider the results of a security impact analysis when considering proposed changes.	3.7.h	CM-4	LMH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
5.4.3	Any addition to the allowed application set shall be validated, approved by the SCCB, and compliant with the TRM or TechSP.	Not Defined	CM-4	LMH F
5.4.4	The SO shall ensure that the CISO or IAD designated representative, and the AO is notified of all planned changes to operational information systems.	Not Defined	CM-4	LMH F
5.4.5	The AO or designated representative shall determine if re-authorization is required as a result of the scope or magnitude of changes to a system under their responsibility.	Not Defined	CM-4	LMH F
5.4.6	New software shall be tested for security impacts due to flaws, weaknesses, incompatibility, or intentional malice within a separate (nonproduction) test environment prior to installation within the production environment.	Not Defined	CM-4 (1)	H F

3.5.5 Access Restrictions for Change (CM-5)

Any changes to the hardware, software, or firmware components of the information system can potentially have significant effects on the overall security of the system. Accordingly, only qualified and authorized individuals are allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications. Additionally, maintaining records of access is essential for ensuring that configuration change control is being implemented as intended and for supporting after the fact actions should TSA become aware of an unauthorized change to the information system.

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
5.5.1	The SO shall ensure that any access to information systems is limited to authorized personnel and that only approved users are permitted to make changes to information system configurations, hardware, and software following the defined processes.	4.8.3.b	AC-3 CM-5	MH F
5.5.2	The SO shall define, document, approve, and enforce physical and logical access restrictions associated with changes to information systems.	Not Defined	CM-5	MH F
5.5.3	The SO shall ensure routine monitoring and authorization of system development, system integration, and network administration personnel.	Not Defined	SI-4	MH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
5.5.4	The SO shall ensure all personnel with access to development, test, and operational environments are: approved for access, properly cleared with TSA Personnel Security, and are U.S. Citizens.	Not Defined	AC-3	MH F
5.5.5	The SO shall ensure access restrictions are implemented in compliance with DHS and TSA policy.	Not Defined	AC-3 CM-5 PE-3	MH F
5.5.6	The ISSO shall ensure copies of software are physically protected in compliance with DHS and TSA physical security policy.	Not Defined	CM-5	MH F
5.5.7	Automated mechanisms shall be employed on IT assets to enforce access restrictions and support auditing of the enforcement actions.	Not Defined	CM-5 (1)	H F
5.5.8	The ISSO shall monitor system change logs, at least quarterly, for adherence or when indications so warrant to determine whether unauthorized changes have occurred and to ensure proper release and deployment procedures.	Not Defined	CM-5 (2)	H F
5.5.9	TheSO and ISSO shall ensure that their TSA information systems shall prevent the installation of unsigned software packages and/or packages not signed by a trusted source.	Not Defined	CM-5 (3)	H F
5.5.10	The ISSO shall be granted a clearance and access greater than or equal to the highest level of information contained on the system. It is strongly encouraged that ISSOs be cleared to the Secret level in order to facilitate intelligence sharing among information security professionals."	2.1.8.f	AC-3	MH F

3.5.6 Configuration Settings (CM-6)

Security related configuration settings refer to the configurable security-related parameters of IT products that are part of the information system that allow TSA to provide a standardized security environment for TSA IT assets including mobile devices. Configuration settings may be communicated in the form of a: security configuration checklist, lockdown guide, hardening guide, security guide, Security Technical Implementation Guide (STIG), or benchmark containing a series of instructions or procedures for configuring an information system component to meet operational requirements.

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
5.6.1	The CISO shall issue TSA-wide information guidance on configuration settings and information security architecture requirements for all TSA systems. Configuration settings based on DISA STIGs, NIST publications, or vendor specific guidance (such as Cisco SAFE or similar) shall be used or incorporated by IAD into the appropriate technical standard.	Not Defined	CM-2 CM-6	LMH F
5.6.2	The SO shall test, authorize, and approve the configurations of all new software and hardware prior to implementation.	4.8.3.c	CM-2 CM-6	LMH F
5.6.3	The CISO shall periodically audit the configurations of TSA information system components to verify configuration settings and to identify and eliminate unnecessary functions, ports, protocols, and/or services.	3.7.b 4.8.3.c	CM-3 CM-4 CM-5	LMH F
5.6.4	The CISO shall ensure DHS/USGCB or DHS/FDCC compliance. Security-relevant management processes and tools shall comply with applicable NIST standard protocols and conventions as described in NIST SP 800-126, The Technical Specification for the Security Content Automation Protocol (SCAP), including the Common Platform Enumeration (CPE), Common Configuration Enumeration (CCE), and Common Vulnerabilities and Exposures (CVE).	3.1.k 3.7.f	CM-6	LMH F
5.6.5	The SO shall ensure that TSA information systems are configured with the concept of the “most-restrictive” mode of operational requirements in compliance with DHS Sensitive Systems Handbook, Enclosure 1, DHS Secure Baseline Configuration Guidance, TSA Configuration Guidance, DISA STIGs, Center for Internet Security (CIS)-Configuration Assessment Tool (CAT) benchmark and TS-008 *End User Assets*. In cases of configuration disparity, the most restrictive and inclusive DHS policy requirements may take precedence per agreement by the AO.	3.7.g 4.8.3.a	CM-6 CM-1	LMH F
5.6.6	In cases where DHS configuration guidance is not available (and with the approval of the AO), the DISA STIGs, NSA Configuration Guidance, CIS-CAT benchmark and/or vendor specific guidance (such as Cisco SAFE or similar), shall be used.	Not Defined	CM-6	LMH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
5.6.7	The SO shall monitor and control changes to the configuration settings.	3.7.d	CM-3	LMH F
5.6.8	The SO shall request a waiver from the AO for any individual system component(s), including operating systems or applications that are not hardened or do not follow configuration guidance. Requests shall include a proposed alternative secure configuration and shall be approved by the AO prior to implementation.	3.7.g	CM-6	LMH F
5.6.9	The ISSO shall ensure that the configuration settings are documented for all active devices within the information system.	Not Defined	CM-6	LMH F
5.6.10	Security authorization documents shall be maintained under configuration management (CM) control throughout the system life cycle.	Not Defined	CM-6	LMH F
5.6.11	Reserved			
5.6.12	All TSA end user assets requiring connectivity to TSA networks and information systems shall be configured using TSA approved images (containing only an operating system and applications installed and/or validated by TSA) and approved within an authorization boundary. Any prohibited operating system shall not be used.	Not Defined	CM-6	LMH F
5.6.13	The SO shall ensure TSA Information systems employ automated mechanisms to centrally manage, apply, and verify configuration settings.	Not Defined	CM-6 (1)	H F
5.6.14	Automated mechanisms shall be employed to respond to unauthorized changes.	Not Defined	CM-6 (2)	H F
5.6.15	Reserved			

3.5.7 Least Functionality (CM-7)

Least functionality allows TSA to configure information systems to provide only essential capabilities and specifically prohibits or restricts the use of unused or unnecessary physical and logical ports and protocols. By doing so, unauthorized connections from devices, transfers of information, or tunneling can be prevented.

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
5.7.1	The SO shall ensure that information systems are configured to restrict a user or process to the least privileges or access required to perform authorized tasks.	Not Defined	CM-7	MH
5.7.2	The SO shall ensure that information systems are configured to provide only essential capabilities by specifically prohibiting or restricting the use of unused or unnecessary physical and logical ports and protocols.	Not Defined	CM-7	LMH
5.7.3	The SO shall ensure that communications are consistent with TS-019 Network Communications Protocols and TS-002 Encryption policies.	Not Defined	CM-7	LMH
5.7.4	The use of add-on devices is only authorized when explicitly approved within an authorization boundary by the AO.	4.6.2.m	AC-19 CM-7	LMH
5.7.5	Functions that can record or transmit sensitive information via video, Infrared (IR), or Radio Frequency (RF) shall be disabled in areas where sensitive information is discussed.	4.6.2.m 4.6.2.3.b	CM-7 AC-19	LMH
5.7.6	The SO shall ensure that wireless capabilities for peripheral equipment are disabled.	4.8.5	CM-7	LMH
5.7.7	In cases where valid mission requirements or equipment limitations prevent disabling wireless capabilities, the SO shall ensure compliance with DHS 4300A and obtain a waiver in accordance with this policy.	4.8.5	CM-7	LMH
5.7.8	The ISSO shall ensure that network printers, copiers, and facsimile machines are configured for least required functionality.	4.12.c	CM-7	LMH
5.7.9	Firewalls and PEPs shall be configured to prohibit any protocol or service that is not explicitly permitted.	5.4.5.b	CM-7	LMH
5.7.10	Telnet shall not be used to connect to any DHS or TSA computer. A connection protocol such as Secure Shell (SSH) that employs secure authentication (two-factor, encrypted, key exchange) and is approved by the CISO shall be used instead. The Telnet protocol shall be disabled on all TSA IT assets, unless a specific waiver is granted by the CISO.	5.4.5.d	CM-7 SC-7 SC-8 SC-9 SC-13	LMH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
5.7.11	File Transfer Protocol (FTP) shall not be used to connect to or from any DHS or TSA computer. A connection protocol that employs secure authentication (two-factor, encrypted, key exchange) and is approved by the CISO shall be used instead. The FTP protocol shall be disabled on all TSA IT assets, unless a specific waiver is granted by the CISO.	5.4.5.e	CM-7 SC-7 SC-8 SC-9 SC-13	LMH
5.7.12	The ISSO shall ensure that remote desktop connections, such as Microsoft's Remote Desktop Protocol (RDP), are not used to connect to or from any TSA computer without the use of an authentication method that employs secure authentication.	5.4.5.f	CM-7 AC-17	LMH F P
5.7.13	Peer to peer software technology is prohibited on any TSA information system.	5.4.9.a	CM-7 SA-6	LMH
5.7.14	Maintenance ports shall be disabled during normal system operation and enabled only during approved maintenance activities.	4.8.3.e	CM-7 (1)	MH
5.7.15	The ISSO shall review the information system at least annually to ensure all unnecessary functions, ports, protocols, and/or services are identified and eliminated.	Not Defined	CM-7 (1)	MH
5.7.16	Information systems shall employ automated mechanisms to prevent program execution in any way not intended within the published scope of an application that resides on the platform.	Not Defined	CM-7 (2)	H
5.7.17	Under TSA, the Chief Architect and CISO shall identify, review, update, "blacklist" and "whitelist" any applications or software program not authorized (or authorized) to be executed in an information system. See the ***Enterprise Architecture Information Repository (EAIR)*** and the ***DHS TRM*** links for additional information.	Not Defined	CM-7 (4)	M

3.5.8 System Component Inventory (CM-8)

The security of the TSA IT enterprise is dependent on the consistent and proper configuration of all IT infrastructure and end user assets. Missing, stolen, or unaccounted IT assets may be considered a

material weakness and can adversely affect the TSA security posture. The periodic inventory of information system components is necessary to achieve effective property accountability.

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
5.8.1	The CIO shall ensure that every TSA computing resource (desktop, laptop, server, wireless mobile device, etc.) is identified as an information system or as a part of an information system (major application or general support system).	3.1.b	CM-8	LMH
5.8.2	The SO shall develop, document, and maintain an inventory of information system components to include desktops, laptops, servers, wireless mobile devices, network printers, copiers, facsimile machines, licensed software, spares, and backup hardware and software.	3.1.a 4.12.d	CM-8	LMH
5.8.3	All TSA IT assets shall be individually defined in the asset management database, have an associated asset tag for identification purposes, and be assigned to a FISMA inventoried information system.	Not Defined	CM-8	LMH
5.8.4	The SO shall ensure that information systems and networks are appropriately documented in such a way as to allow others to understand system operation and configuration IAW the DHS Inventory methodology.	4.10.a	CM-8	LMH
5.8.5	The SO shall make available, via IACS, an information system inventory for auditing purposes and for designated TSA officials.	3.9.1.d 3.15.a	CM-8	LMH
5.8.6	The SO shall update the inventory of information system components as an integral part of component installations, removals, and information system updates.	3.7	CM-8 (1)	MH
5.8.7	TSA information systems shall employ automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.	Not Defined	CM-8 (2)	H
5.8.8	TSA systems shall employ automated mechanisms to detect the addition of unauthorized components/devices into an information system.	Not Defined	CM-8 (3)	MH
5.8.9	All non-authorized devices shall be denied network access and the SOC shall be notified upon discovery so that appropriate action may follow.	Not Defined	CM-8 (3)	MH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
5.8.10	The ISSO shall maintain property accountability information for individuals responsible for information system components, including names, positions, and roles of each responsible individual.	Not Defined	CM-8 (4)	H
5.8.11	The ISSO shall verify that all components within the authorization boundary of an information system are either inventoried as a part of the system or recognized by another system as a component within that system.	3.1.a	CM-8 (5)	MH
5.8.12	Automated mechanisms shall be employed on a monthly basis to detect the presence of unauthorized software on TSA information systems and notify designated TSA officials.	Not Defined	CM-8	LMH
5.8.13	The CISO shall ensure that each IT component acquired is explicitly assigned to an information system, and that the SO acknowledges this assignment.	Not Defined	CM-8 (9)	LMH

3.5.9 Configuration Management Plan (CM-9)

The configuration management plan defines detailed processes and procedures for how configuration management is used to support SELC/Agile activities at the information system level. The plan describes how: (1) to move a change through the change management process; (2) configuration settings and configuration baselines are updated; (3) the information system component inventory is maintained; (4) development, test, and operational environments are controlled; and (5) documents are developed, released, and updated.

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
5.9.1	The SO shall develop, document, and implement configuration management plans (CMPs) for the information system that includes the configuration items and addresses roles, responsibilities, and configuration management processes and procedures throughout the entire SELC.	3.7.a 3.7.d	CM-9	MH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
5.9.2	Development, test, pilot, prototype, and other non-production environments shall be compliant with established baseline configurations and authorized, in writing, by the CISO and AO prior to implementation in a production environment to ensure protection of configuration information and software code. See TS-070 *Secure Code and Software Assurance Development* for additional information and guidance.	Not Defined	CM-9	LMH
5.9.3	Development, test, and other non-production environments shall not store, process, or use live and/or production TSA official data.	Not Defined	CM-9	LMH
5.9.4	Development, test, and other non-production environments shall not have a direct or indirect link to a TSA operational system or to live and/ or production TSA sensitive data.	Not Defined	CM-9	LMH
5.9.5	Reserved			

3.5.10 Software Usage Restrictions (CM-10)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
5.10.1	The SO shall ensure that: a. proper usage of software and associated documentation is IAW contract agreements and copyright laws; b. proper tracking of software and associated documentation is protected by an authorized quantity of licenses in order to control copying and distribution; and c. proper controls are in place to prevent the use of any peer-to-peer (P2P) networking or file sharing technology to ensure this capability is not used for unauthorized distribution, display, performance, or reproduction of copyrighted work.	4.8.4.b 5.4.9	CM-10	LMH
5.10.2	The SO shall ensure the information system only uses software and associated documentation in compliance with contract agreements and copyright laws.	Not Defined	CM-10	LMH
5.10.3	The ISSO shall ensure the information system employs tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution.	Not Defined	CM-10	LMH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
5.10.4	The SO shall ensure that users do not duplicate copyrighted software or remove copyrighted software from government equipment without the express written permission of the CIO.	Not Defined	CM-10	LMH
5.10.5	Individual users shall be personally liable for any software copyright violations committed on government systems under their control.	Not Defined	CM-10	LMH
5.10.6	All applications utilized within TSA shall be on the approved applications list and bound by Group Policy Object (GPO). Anything that is not explicitly allowed shall be denied.	Not Defined	CM-10	LMH
5.10.7	Allowable software applications shall be limited to a minimal, controlled, and tested library.	Not Defined	CM-10	LMH

3.5.11 User-Installed Software (CM-11)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
5.11.1	The SO shall enforce and ensure that non-GFE software or applications are not installed on any TSA information systems by users since such action is prohibited (see *Computer and Personal Electronic Device Access Agreement (CAA)* for additional details). See the ***Enterprise Architecture Information Repository (EAIR)*** and the ***DHS TRM*** links for additional information. For additional software/application inquiries, contact the *Software Management Group (SMG) Application Team* at applications@tsa.dhs.gov. Also see **TSA MD 1400.14 *Software Management*** for general guidance.	4.8.2.a	CM-11	LMH F

3.5.12 Information Location (CM-12)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
5.12.1	Place holder	TBD	TBD	TBD

3.6 Contingency Planning (CP)

3.6.1 Contingency Planning Policy and Procedures (CP-1)

TSA contingency plans or planning (CP) is developed to reduce risk to an acceptable level and support the restoration of systems, critical information, and services at all levels (to include Network Operations Center (NOC), server farms, and remote sites). Effective CP begins with the development of the TSA CP policy and subjection of each information system to a business impact analysis (BIA). The TSA BIA establishes processes for identifying the critical information and services of TSA systems, IT assets, and the resources required to support them. The BIA is a key step in implementing the CP controls in NIST SP 800-53 and in the CP process overall. Contingency plans and Continuity of Operations Plans (COOP) provide the procedures for the recovery should an incident render the system or facility inoperable for a period of time. COOP applies to mission essential functions of federal government departments and agencies. The CP provides guidelines for ensuring that necessary personnel and resources are available for both disaster preparation and response, and that the proper activity is performed to permit timely restoration of TSA information and services. The COOP is mandated by HSPD-20/NSPD-51, PPD-40, FCDs 1 and 2, and the National Continuity Policy Implementation Plan (NCPIP); the CP is mandated by FISMA.

DHS has adapted NIST guidance regarding CP-related activities to meet mission requirements. NIST Special Publication (SP) 800-34 Revision 1, *Guide to Contingency Planning for Federal Systems* provides additional guidance beyond DHS MD 4300A and this Handbook. Information System Contingency Plans (ISCPs or CPs), as defined by NIST, are the focus of this section. Additional guidance is established such as definitions for key terms including Maximum Tolerable Downtime (MTD), Recovery Time Objective (RTO), and Recovery Point Objective (RPO) and detailed CP processes.

Specific detailed guidance of the information security requirements on contingency planning policy and procedures is contained in the TSA TS-002 *Encryption* and TS-017 *Controlled Access Areas*.

Other Guidance: DHS *Security Operations Concept of Operations*, OMB Memorandum A-130, Appendix III, NIST SP 800-34 *Contingency Planning Guide for Federal Information Systems and 800-58 Security Considerations for Voice Over IP Systems.*

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
6.1.1	The CISO shall ensure the development, dissemination, and maintenance of a formal, documented contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among TSA elements, and compliance.	3.5.1.h	CP-1	LMH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
6.1.2	The CISO shall ensure a list of mission-critical information systems is formally documented and updated by the SOC as needed in support of the TSA COOP and in compliance with the DHS *Security Operations Concept of Operations*. These systems shall be covered by alternate processing sites. Mission-critical systems shall be systems that have: a. A High Availability potential impact level, or b. Been specifically designated by the CIO as critical to the DHS mission.	2.1.11 3.5	CP-1 CP-7 CM-8	LMH
6.1.3	The SO shall ensure preparation and maintenance of plans and procedures to provide continuity of operations for the information system.	3.5.1.h	CP-1	LMH
6.1.4	The SO shall ensure each system has contingency capabilities commensurate with the FIPS 199 Availability potential impact level in compliance with DHS MD 4300A. The minimum contingency capabilities for each impact level follow: High/Critical Impact – System functions and information shall have a high priority for recovery after a short period of loss (24 hours or less). Moderate Impact – System functions and information shall have a moderate priority for recovery after a moderate period of loss (72 hours or less). Low Impact – System functions and information shall have a low priority for recovery after prolonged loss (14 calendar days or less).	3.5.2.d	CP-1 CP-2	LMH
6.1.5	The SO shall ensure the Availability of critical resources and facilitate the CP in an emergency situation.	Not Defined	CP-1	LMH
6.1.6	All Chief Financial Officer (CFO) Designated Systems requiring high availability shall be validated via Blanket Purchase Agreement (BPA) and Business Impact Assessment (BIA) efforts, identified in Component continuity of operations plans, and reported to the DHS Mission Essential Systems List.	3.5.1.d	CP-1	H
6.1.7	The ISSO shall develop a contingency plan, such as the use of a fallback identification technology, to implement in case of an RFID security breach or system failure.	4.6.4.c	SC-9 CP-1	LMH

3.6.2 Contingency Plan (CP-2)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
6.2.1	The SO shall develop a CP consistent with DHS 4300A PD Attachment K *IT Contingency Plan Template* or other DHS provided template for the information system that: a. Identifies essential missions and business functions and associated contingency requirements; b. Provides recovery objectives, restoration priorities, and metrics (including RTOs and RPOs); c. Addresses contingency roles, responsibilities, assigned individuals with contact information; d. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; e. Details backup operations including frequency of incremental and full backups and backup storage; f. Addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented; and g. Is reviewed and approved by the AO.	3.5.2	CP-1 CP-2	LMH
6.2.2	The minimum recovery time objectives (RTO) for the information system recovery in the CP shall be as follows depending on the Availability: High – Resumption of operations shall occur within 24 hours or per the timeline directed by the TSA Administrator. Moderate – Resumption of operations shall occur within 72 hours or per the timeline directed by the TSA Administrator. Low – Resumption of operations shall occur within 14 calendar days or per the timeline directed by the TSA Administrator. Deviations from the minimum RTO shall require AO approval.	Not Defined	CP-2	LMH
6.2.3	The minimum recovery point objectives (RPO) for the information system recovery shall be defined within the CP.	Not Defined	CP-2	LMH
6.2.4	The CISO shall ensure the CP clearly and accurately documents the three essential phases: Activation and Notification, Recovery, and Reconstitution.	3.5.2.e	CP-1 CP-2	LMH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
6.2.5	The SO shall review and approve the CP for each TSA information system on behalf of the CIO.	3.5.2.b	CP-1 CP-2	LMH
6.2.6	The ISSO shall review the CP for the information system at least annually and revise the plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing on behalf of the SO.	3.5.2.e	CP-1 CP-2	LMH
6.2.7	The ISSO shall ensure deficiencies found in the contingency plan are recorded, tracked, and corrected.	Not Defined	CP-1	LMH
6.2.8	The CISO shall ensure that contingency planning activities are coordinated with incident handling activities.	3.5	CP-2	LMH
6.2.9	The SO shall coordinate contingency plan development with supporting TSA elements for the information system with the TSA COOPs and the National Cyber Incident Response Plan.	Not Defined	CP-2 (1)	MH
6.2.10	The SO shall ensure capacity planning is conducted so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.	4.5.1.b	CP-2 (2) CP-8	H
6.2.11	The SO shall ensure the CP includes resumption of critical missions and business functions upon contingency plan activation based on RTOs and RPOs documented within the CP and authorized by the AO.	Not Defined	CP-2 (3)	H
6.2.12	The AO or designated official shall ensure that a Continuity of Operations Plan (COOP) is developed in order to ensure continuity of information system mission operations under all circumstances.	3.5.1.b	CP-2 (4)	H
6.2.13	The AO or designated official shall develop, test, implement, and maintain a comprehensive COOP to ensure the recovery and continuity of essential information system functionalities. This shall ensure little or no loss of information system operational continuity and shall sustain that continuity until full information system restoration at primary processing locations.	3.5.1.b	CP-2 (5)	H
6.2.14	The AO or designated official shall ensure that critical information systems are identified to support essential missions and business functions.	Not Defined	CP-2 (8)	MH

3.6.3 Contingency Training (CP-3)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
6.3.1	The SO shall ensure that contingency training is provided to key personnel IAW the potential impact level for the Availability security objective for the information system. The minimum contingency planning for each impact level follows: High – All personnel involved in contingency planning efforts shall be identified and trained in their contingency planning and implementation roles, responsibilities, procedures, and logistics. This training shall incorporate simulated events. Refresher training shall be provided at least annually. Moderate – All system personnel involved in contingency planning efforts shall be trained. Refresher training shall be provided at least annually. Low – Training shall not be required.	3.5.2.g	CP-3	LMH
6.3.2	The CIO shall ensure all information system support personnel involved with COOP efforts are identified and trained in the procedures and logistics of the disaster recovery and business continuity plans.	3.5.1.e	CP-1 CP-3 AT-3	LMH
6.3.3	The CIO or designated official shall ensure that contingency training such as drills or simulated events are conducted to facilitate effective response by personnel in crisis situations and IAW the availability security objective.	3.5.2.g	CP-3 (1)	H

3.6.4 Contingency Plan Testing (CP-4)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
6.4.1	The CIO shall ensure the development, testing, implementation, and maintenance of a comprehensive COOP supported by system CPs to ensure the continuity and recovery of essential TSA functionality.	3.5.1.b	CP-2 CP-4	LMH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
6.4.2	The ISSO shall perform annual contingency plan testing for each information system IAW the Availability security objective. The minimum contingency testing for each impact level shall be as follows: High/Critical – System recovery roles, responsibilities, procedures, and logistics in the CP shall be used to recover from a simulated contingency event at the alternate processing site within a year prior to authorization. The system recovery procedures in the CP shall be used to simulate system recovery in a test facility at least annually. Moderate – System personnel shall review roles, responsibilities, and procedures in the CP. This shall be achieved by performing a walk-through/tabletop exercise annually. Low – CP contact information shall be verified and updated at least annually.	3.5.2.f	CP-4 CP-7	LMH F
6.4.3	The ISSO shall document the results of the contingency plan test within the IT Contingency Plan Test Results (CPTR) in compliance with the DHS Performance Plan.	Not Defined	CP-4 CP-7	LMH F
6.4.4	Reserved			
6.4.5	The CISO shall ensure that all CPs are tested annually and are in compliance with TSA and DHS policy.	3.5.2.f	CP-4	LMH F
6.4.6	The SO shall coordinate CP testing for the information system with the TSA COOP and the National Cyber Incident Response Plan.	3.5.2.h	CP-4 (1)	LMH
6.4.7	The CP shall be tested within a year prior to authorization to recover from a simulated contingency event at the alternate processing site to familiarize contingency personnel with the facility and available resources and to evaluate the site's capabilities to support contingency operations.	3.5.2.f	CP-4 (2)	H F
6.4.8	Reserved			
6.4.9	CPs shall include a full recovery and restoration of the information system to a known state as part of contingency plan testing.	Not Defined	CP-4 (4)	H F

3.6.5 Contingency Plan Update (CP-5) (Withdrawn)

Withdrawn and incorporated into CP-2.

3.6.6 Alternate Storage Site (CP-6)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
6.6.1	The location of the local backup site and the alternate backup site shall be clearly defined and documented within the CP and all off-site backup media shall be protected.	4.3.1.b	CP-6	MH
6.6.2	The SO shall ensure the alternate storage site is physically secured to an equivalency of the primary storage site, using access controls in compliance with TS-017 *Controlled Access Areas.*	Not Defined	CP-6 PE-17	MH
6.6.3	The SO shall ensure that the necessary agreements are in place to permit the storage and recovery of backup information for the information system at the alternate storage site.	Not Defined	CP-6	MH
6.6.4	The SO shall, at a minimum, identify and account for geographic area, accessibility, security capabilities, and environmental elements when selecting an alternate storage facility.	Not Defined	CP-6	MH
6.6.5	The alternate storage site shall be separated from the primary storage site so as not to be susceptible to the same hazards.	Not Defined	CP-6 (1) PE-18	MH
6.6.6	The alternate storage site shall be a minimum of 50 miles from the primary site and not susceptible to the same physical hazards (for example, not along the same coast line).	Not Defined	CP-6 (1) PE-18	MH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
6.6.7	When selecting an alternate storage facility and vendor, the following criteria shall be considered: a. Geographic area: distance from the information system and the probability of the storage site being affected by the same disaster as the system's primary site; b. Accessibility: length of time necessary to retrieve the data from storage and the storage facility's operating hours; c. Security: security capabilities of the shipping method, storage facility, and personnel; all shall meet the data's security requirements; d. Environment: structural and environmental conditions of the storage facility such as temperature, humidity, fire prevention, and power management controls; and e. Cost: cost of shipping, operational fees, and disaster response/recovery services.	Not Defined	CP-6 (1) PE-18	MH
6.6.8	The SO shall ensure alternate storage sites are configured to facilitate recovery operations IAW the RTOs and RPOs for the information system as defined in the CP.	Not Defined	CP-6 (2)	H
6.6.9	The SO shall use a risk assessment to identify potential accessibility problems and outline explicit mitigation actions to the alternate storage in the event of an area-wide disruption or disaster.	Not Defined	CP-6 (3)	MH

3.6.7 Alternate Processing Site (CP-7)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
6.7.1	The SO shall identify an alternate processing site for the resumption of information system operations for critical missions and business functions when the primary processing capabilities become unavailable.	Not Defined	CP-7	MH F
6.7.2	The CIO shall ensure that necessary agreements are in place to permit the resumption of TSA information system operations for critical missions and business functions.	Not Defined	CP-7	MH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
6.7.3	The SO shall ensure that equipment and supplies required to resume operations are available at the alternate site or service level agreements are in place to support delivery to the site IAW the recovery time and recovery point objectives for the information system as defined in the CP.	Not Defined	CP-7	MH F
6.7.4	The SO shall ensure that the alternate processing site provides information security measures equivalent to that of the primary site.	Not Defined	CP-7	MH F
6.7.5	The alternate processing site shall be separated from the primary processing site so as not to be susceptible to the same hazards.	Not Defined	CP-7 (1) PE-18	MH F
6.7.6	The alternate processing site shall be a minimum of 50 miles from the primary site and not susceptible to the same physical hazards (for example, not along the same coast line).	Not Defined	CP-7 (1) PE-18	MH F
6.7.7	When selecting an alternate processing vendor and facility, the following criteria shall be considered: a. Geographic area: distance from the information system and the probability of the processing site being affected by the same disaster as the system's primary site; b. Accessibility: length of time necessary to retrieve the data from the processing site and the site's operating hours; c. Data Security: security capabilities of the shipping method, processing facility, and personnel; d. Environment: structural and environmental conditions of the processing facility such as temperature, humidity, fire prevention, and power management controls; and e. Cost: cost of shipping, site operational fees, and disaster response/recovery services.	Not Defined	CP-7 (1) PE-18	MH F
6.7.8	The SO shall identify potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outline explicit mitigation actions within the CP.	Not Defined	CP-7 (2)	MH F
6.7.9	The SO shall develop alternate processing site agreements that contain priority-of-service provisions IAW Availability potential impact levels identified in the CP.	Not Defined	CP-7 (3)	MH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
6.7.10	The SO shall ensure the alternate processing site configuration is maintained and ready to be used as the operational site supporting critical TSA missions and business functions.	Not Defined	CP-7 (4)	H F
6.7.11	Reserved			

3.6.8 Telecommunications Services (CP-8)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
6.8.1	The SO shall establish alternate telecommunications services to permit the resumption of information system operations IAW the Availability security objectives identified in the CP for essential missions and business functions of the information system.	4.5.1	CP-8	MH F
6.8.2	The SO shall ensure that the necessary alternate telecommunications service agreements are in place to permit the resumption of information system operations for critical missions and business functions.	4.5.1	CP-8	MH F
6.8.3	The SO shall develop primary and alternate telecommunications service agreements that contain priority of service provisions IAW the information system's Availability security objective.	Not Defined	CP-8 (1)	MH F
6.8.4	The SO shall request telecommunications service priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.	Not Defined	CP-8 (1)	MH F
6.8.5	The SO shall obtain alternate telecommunications services with consideration for reducing the likelihood of sharing a single point of failure with primary telecommunications services.	Not Defined	CP-8 (2)	MH F
6.8.6	The SO shall obtain alternate telecommunications service providers that are separated from primary service providers so as not to be susceptible to the same hazards.	Not Defined	CP-8 (3)	H F
6.8.7	The SO shall ensure primary and alternate telecommunications service providers have contingency plans to provide required support to the IS.	Not Defined	CP-8 (4)	H F

3.6.9 System Backup (CP-9)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
6.9.1	The ISSO shall ensure the information backup is performed and transported to the alternate storage site in compliance with TSA BIA, business continuity, and disaster recovery plans, and the information system's overall security objective. The minimum timeline shall be as follows: High – Incremental backups shall occur on a daily basis and full backups shall occur on a weekly basis. Moderate – Incremental backups shall occur on a weekly basis and full backups shall occur on a monthly basis. Low – Incremental backups shall occur on a monthly basis and full backups shall occur on a quarterly basis. Deviations from these minimum timelines shall be approved by the AO.	3.5.2.c 4.11	CP-9	LMH
6.9.2	ISSOs shall ensure implementation of backup policies and procedures for every information system. Specifically, the ISSO shall ensure the information stored within the backup includes both user level and system level data. User level data shall include information such as information entered by the user and/or processed by the system. In contract, system level data shall include items such as the system technical configurations and software code.	3.5.2.c 4.11.c	CP-9	LMH
6.9.3	The ISSO shall ensure information system documentation (including security-related documentation) is incorporated into the backup.	Not Defined	CP-9	LMH
6.9.4	The SO shall ensure the backup storage location protects the backup information IAW the information system's Confidentiality and Integrity impact levels and TSA media protection policy.	4.3.1.a	CP-9	LMH
6.9.5	The SO shall ensure data backup operations continually function IAW the information systems recovery objectives to ensure valid data may be obtained as needed for incident investigations or system recovery.	Not Defined	CP-9	LMH
6.9.6	The SO shall approve all backup methods.	Not Defined	CP-9	LMH
6.9.7	The CISO shall ensure implementation of backup procedures for all TSA information systems.	3.5.2.c	CP-9	LMH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
6.9.8	Backup data shall be encrypted at the same level or higher than required for its source data.	Not Defined	CP-9 MP-4	LMH
6.9.9	The ISSO shall test backup information to verify media reliability and information Integrity as part of the annual CPT.	Not Defined	CP-9 (1)	MH
6.9.10	The ISSO shall ensure operational samples of backup information are used as part of contingency plan testing in support of the restoration of selected information system.	3.5.2	CP-9 (2)	H
6.9.11	The ISSO shall ensure backup copies of the operating system and other critical information system software, as well as copies of the information system inventory (including hardware, software, and firmware components) and documentation are stored in a separate facility from the operational location.	Not Defined	CP-9 (3)	H
6.9.12	The SO shall ensure the secure transfer of applicable information system backups to the alternate storage site IAW TSA backup policy, security authorization documents and TS-002 Encryption policy.	4.11.d	CP-9 (5)	H

3.6.10 System Recovery and Reconstitution (CP-10)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
6.10.1	The SO shall ensure CP is established and implemented to allow information system recovery to a known state after disruption, compromise, or failure.	5.4.4.m	CP-10	H
6.10.2	The SO shall establish procedures for notification during recovery and reconstitution of operations including problem escalation, status awareness for stakeholders, and status awareness for end users.	Not Defined	CP-10	LMH
6.10.3	The SO shall ensure documentation is generated and collected after reconstitution of operations including: - Activity logs; - Functionality and data testing results; - Lessons learned documentation; and - After Action Reports.	Not Defined	CP-10	LMH
6.10.4	Reserved			

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
6.10.5	The SO shall ensure transaction recovery is implemented for transaction-based systems.	Not Defined	CP-10 (2)	MH
6.10.6	The SO shall ensure the capability exists to properly restore and reconstitute information system components back to its operational state for the system IAW backup policy and security authorization documents.	Not Defined	CP-10 (4)	H
6.10.7	Reserved			
6.10.8	Reserved			
6.10.9	Reserved			
6.10.10	Transaction-based systems (e.g. database management systems, transaction processing systems) shall implement transaction rollback and transaction journaling, or technical equivalents.	5.7.e	CP-10	LMH

3.6.11 Alternate Communications Protocols (CP-11)

Currently, this control does not apply to any control baselines, nor does it apply to Privacy or Financial systems.

3.6.12 Safe Mode (CP-12)

Currently, this control does not apply to any control baselines, nor does it apply to Privacy or Financial systems.

3.6.13 Alternative Security Mechanisms (CP-13)

Currently, this control does not apply to any control baselines, nor does it apply to Privacy or Financial systems.

3.7 Identification and Authentication (IA)

All users of TSA IT assets shall be positively authenticated by the network prior to each network session.

Other guidance: HSPD-12, OMB Memorandum 04-04, FIPS Publications 140-2 and 201; NIST Special Publications 800-12, 800-16, 800-50, 800-63, 800-73, 800-76, 800-78, 800-115.

3.7.1 Identification and Authentication Policy and Procedures (IA-1)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
7.1.1	CISO shall ensure the development, dissemination, and maintenance of a formal, documented identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among TSA entities, and compliance.	Not Defined	IA-1	LMH F
7.1.2	The CISO shall establish documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.	Not Defined	IA-1	LMH F
7.1.3	The SO shall ensure the implementation of identification and authentication procedures using mechanisms that provide the capability to assign network actions to unique entities (to include users or processes acting on the behalf of users).	Not Defined	IA-1	LMH F

3.7.2 Identification and Authentication (Organizational Users) (IA-2)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
7.2.1	The SO shall ensure that information systems uniquely identify and authenticate users and processes operating on behalf of users.	5.1.b	IA-1 IA-2	LMH F
7.2.2	The SO shall ensure that user access is controlled and limited based on positive user identification and authentication mechanisms that support the minimum requirements of access control, least privilege, and system Integrity.	5.1.a	IA-1 IA-2	LMH F
7.2.3	A user who departs TSA temporarily for authorized reasons such as a sabbatical, break in contract funding, etc., and returns to the identical position and duties, may have their account identifier disabled for the duration of their absence and re-enabled upon their return to duty. If the departure from the original position and duties is or becomes permanent or the user returns to a different position and duties, the old account identifier and related permissions shall be deleted and a new account identifier created. Reuse of an account identifier shall be authorized by the direct line federal supervisor for all users, and also by the COR for contractors.	Not Defined	IA-2	LMH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
7.2.4	Where applicable, password, passphrase and/or PIN management shall be consistent with the requirements stated in TS-001 Passwords/PINs policy. Throughout this document, the word "password" is used for ease of discussion. Where used, it should be interpreted to include passphrases and PINs, as well as passwords. See **DHS CISO Memo dated August 30, 2017, Alignment of Password Policy with NIST SP 800-63B** for additional guidance. Also see **DHS Memorandum from the CIO on *Mobile Device Management on Password Guidance*** dated December 12, 2017.	Not Defined	IA-2	LMH F
7.2.5	Privileged account management shall be accomplished in compliance with Privileged Access policy.	Not Defined	IA-2	LMH F
7.2.6	For purchases or fee transactions using credit cards, Components comply with Payment Card Industry Data Security Standard (PCI DSS).	3.14.7.a	IA-2	LMH F
7.2.7	Reserved			
7.2.8	ISSO shall implement authentication IAW with account type.	Not Defined	IA-2	LMH F
7.2.9	ISSO shall document the applicability of e-authentication requirements for systems that allow online transactions. Programs considering e-authentication are required to consult their privacy officer to determine whether a change is significant to warrant a new or updated PTA, thus initiating the review of privacy risks and how they shall be mitigated.	3.14.7.e	IA-2	LMH F
7.2.10	The ISSO 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*.	3.14.7.b	IA-2	LMH F
7.2.11	The SO shall ensure the implementation of the technical requirements described in NIST SP 800-63-3, Digital Identity Guidelines, at the appropriate assurance level for those systems with e-authentication requirements.	3.14.7.c	IA-2	LMH F
7.2.12	The ISSO shall ensure that each SP reflects the e-authentication status of the respective system.	3.14.7.d	IA-2 PL-2	LMH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
7.2.13	Reserved			
7.2.14	Reserved			
7.2.15	Reserved			
7.2.16	Electronic signatures (confirmed with a digital certificate) are preferred to pen and ink or facsimile signatures in all cases, except where pen and ink signatures are required by public law, E.O., or other TSA requirements.	1.6.1.a	IA-2	LMH F
7.2.17	Reserved			
7.2.18	Information systems shall accept electronic signatures whenever the signature's digital certificate is current, electronically verifiable, and issued by a medium or high assurance DHS Certification Authority or other medium or high CA under the Federal Bridge Certification Authority (FBCA) or Common Authority.	1.6.1.c	IA-2	LMH F
7.2.19	Information systems shall accept and be able to verify Personal Identity Verification (PIV) credentials issued by other federal agencies as proof of identity.	1.6.1.d	IA-2	LMH F
7.2.20	PIV credentials shall be used as the primary means of logical authentication for TSA systems; all IT systems shall operate with authentication mechanisms that do not use usernames and passwords. Currently, PINs for PIV card-enabled users do not expire and shall have a minimum six-digit PIN when logging into the network using a PIV card. PINs cannot have more than two consecutive numbers and shall be mixed. See NIST SP 800-63-2 *Electronic Authentication Guideline* for information.	5.1.g HSPD-12 NIST SP 800-73-4	IA-2	LMH F
7.2.21	As mandated by the Government Paperwork Elimination Act (GPEA) and OMB M-00-10, TSA shall provide for the use and acceptance of electronic signatures when practicable.	1.6	IA-2	LMH F
7.2.22	Systems shall use multifactor authentication for local access to privileged accounts.	Not Defined	IA-2 (3)	MH F
7.2.23	Systems shall use multifactor authentication for local access to general user accounts.	Not Defined	IA-2 (4)	H F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
7.2.24	PIV card authentication shall be implemented to allow TSA employees and contractors access to TSA systems including remote access.	5.1.h	IA-2 (12)	LMH F
7.2.25	PIV authentication shall use user based enforcement (UBE) for general user and privileged user accounts. This enforcement controls the interactive logon for each account to allow PIV card authentication to the TSA system.	5.1.h	IA-2 (12)	LMH F
7.2.26	Systems shall support PIV card authentication. Users shall report lost, stolen, or inadvertently destroyed PIV cards to the DHS PCI by email at OneCardSSD@hq.dhs.gov and to the SPOC, who shall supply a temporary password account for logon. Users shall report forgotten or misplaced PIV cards to the SPOC, who shall supply a temporary password account for logon, which shall expire 24 hours after creation. Users also report to the DHS PCI by email at OneCardSSD@hq.dhs.gov	5.1.h 5.1.n 5.1.o	IA-2 (12) HSPD-12	LMH F
7.2.27	Systems shall use replay-resistant authentication (to include TLS, challenge-response onetime-time authenticators) mechanisms for network access to privileged accounts.	Not Defined	IA-2 (8)	MH F
7.2.28	Systems shall use replay-resistant authentication (to include TLS, challenge-response onetime-time authenticators) mechanisms for network access to general users accounts.	Not Defined	IA-2 (9)	H F
7.2.29	The SO shall ensure that information systems implement multifactor authentication for network access to *privileged* accounts.	5.1.i	IA-2 (1)	LMH F
7.2.30	The SO shall ensure that information systems implement multifactor authentication for network access to general user accounts.	Not Defined	IA-2 (2)	MH F
7.2.31	The information system shall implement multifactor authentication for remote access to privileged and general user accounts.	5.4.1.b	IA-2 (11)	MH F
7.2.32	The information system shall accept and electronically verify PIV credentials.	Not Defined	IA-2 (12)	LMH F

3.7.3 Device Identification and Authentication (IA-3)

The information system typically uses either shared known information (to include Media Access Control [MAC] or Transmission Control Protocol/Internet Protocol [TCP/IP] addresses) for identification or TSA authentication solution (to include IEEE 802.1x and Extensible Authentication Protocol [EAP], Radius server with EAP-Transport Layer Security [TLS] authentication, and Kerberos) to identify and authenticate devices on local and/or wide area networks.

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
7.3.1	The ISSO shall ensure the information system is configured to uniquely identify and authenticate all devices that process TSA information before establishing a connection.	3.14.7.i	IA-3	MH
7.3.2	The devices requiring unique identification and authentication shall be defined by: type, specific device, or by a combination of type and device as deemed appropriate by TSA.	Not Defined	IA-3	MH
7.3.3	The required strength of the device authentication mechanism shall be determined by the security categorization of the information system.	Not Defined	IA-3	MH
7.3.4	Reserved			
7.3.5	Reserved			
7.3.6	Reserved			
7.3.7	IEEE 802.1x port authentication with PIV shall be used as an acceptable alternative to MAC based port security.	Not Defined	IA-3	LMH

3.7.4 Identifier Management (IA-4)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
7.4.1	The SO shall oversee the management of information system identifiers for users and devices with the authorization of the AO.	Not Defined	IA-4	LMH F
7.4.2	Identifiers shall uniquely identify an individual or device by assigning the identifier to the intended party or device.	5.2.e	IA-4	LMH F
7.4.3	The ISSO shall ensure the reuse of a user identifier (ex.: John Smith1) following departure is prevented within ninety (90) days after last use.	Not Defined	IA-4	LMH F
7.4.4	Reserved			

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
7.4.5	PINs shall be treated as passwords to the extent possible given technical constraints in compliance with TS-001 *Passwords/PINs*, on the systems they support.	Not Defined	IA-4	LMH F
7.4.6	Reserved			
7.4.7	Information such as SSNs, birth dates, or other PII shall not be used as logon IDs.	5.2.b	IA-4	LMH F
7.4.8	Reserved			
7.4.9	Reserved			
7.4.10	The ISSO shall ensure the information system *suspends* user identifiers after *thirty (30) days* of inactivity for all systems. A user whose identifier has been suspended for inactivity will be required to have their supervisor contact the SPOC to be returned to active status.	Not Defined	IA-4	LMH F
7.4.11	The ISSO shall ensure the information system *disables* user identifiers after *ninety (90) days* of inactivity for systems with LOW impacts for the Confidentiality security objective.	5.1.c	IA-4	L F
7.4.12	The ISSO shall ensure the information system *disables* user identifiers after *forty-five (45) days* of inactivity for systems with HIGH and MODERATE impacts for the Confidentiality security objective.	5.1.c	IA-4	MH F
7.4.13	The ISSO shall ensure the use of group access, which shall be approved by the appropriate AO, is limited to situations dictated by operational necessity or criticality for mission accomplishment. Note: Shared and group accounts are prohibited for all systems categorized as High Value Assets (HVAs).	5.1.1.d 1	IA-4	MH F
7.4.14	All TSA email systems are required to use the common naming convention with distinguishing identifiers for military officers, contractors, foreign nationals, and U.S. Government personnel from other departments and agencies.	5.4.6.j	IA-4	LMH F

3.7.5 Authenticator Management (IA-5)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
7.5.1	The ISSO shall ensure the identity of the individual and/or device receiving the authenticator is verified as part of the initial authenticator distribution.	Not Defined	IA-5	LMH F P
7.5.2	The ISSO shall ensure the initial authenticator content for authenticators is established as documented in the SP.	5.1	IA-5	LMH F P
7.5.3	The password* shall: • Not contain the user's account name or parts of the user's full name that exceed two consecutive characters • Be at least eight characters in length • Contain characters from three of the following four categories: o English uppercase characters (A through Z) o English lowercase characters (a through z) o Base 10 digits (0 through 9) o Non-alphabetic characters (for example: !, $, %) o Not contain consecutive identical characters and shall have at least a 75% change in content from the previous password * Derived from the DHS Windows Server 2008 Configuration Guide v2015 (Paragraph 2.1.2 *Password Policy Settings*) located at: http://dhsconnect.dhs.gov/org/comp/mgmt/cio/iso/Pages/sscg.aspx	5.1.1.a	IA-5	LMH F P
7.5.4	The ISSO shall ensure establishment and implementation of administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators.	Not Defined	IA-5	LMH F P
7.5.5	The ISSO shall ensure that the default content of authenticators is changed upon information system installation.	Not Defined	IA-5	LMH F P
7.5.6	The ISSO shall establish minimum and maximum lifetime restrictions within the SP.	Not Defined	IA-5	LMH F P
7.5.7	The ISSO shall ensure the changing/refreshing of authenticators as defined within the SP.	Not Defined	IA-5	LMH F P

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
7.5.8	The ISSO shall ensure the protection of authenticator content from unauthorized disclosure, access, and modification.	Not Defined	IA-5	LMH F P
7.5.9	The ISSO shall ensure the implementation of steps requiring users to take, and having devices implement, specific measures to safeguard authenticators.	Not Defined	IA-5	LMH F P
7.5.10	The CISO shall oversee and ensure successful employment of public key infrastructure (PKI) on TSA IT assets.	Not Defined	IA-5	LMH F P
7.5.11	Users of TSA information systems shall not share identification or authentication materials of any kind including PIV cards, PINs, passphrases or passwords, nor shall any TSA user allow any other person to operate any TSA system by employing the user's identity. PIV cards and PINS shall not be shared with system administrators.	5.1.d 5.1.1.c 5.2.c	IA-5	LMH F P
7.5.12	In unique cases where an IT asset is shared, each user shall have an individual PIV card for access.	Not Defined	IA-5	LMH F P
7.5.13	Wireless mobile devices shall not be used to store, process, or transmit combinations, personal identification numbers (PIN), or sensitive information in unencrypted formats.	4.6.2.c	AC-19 IA-5	LMH F P
7.5.14	The ISSO shall determine and enforce the appropriate frequency for changing PINs and passwords (when applicable) in compliance with appropriate guidance documentation (if published).	5.1.1.b	IA-5	LMH F P
7.5.15	The ISSO shall ensure the information system prohibits PINs and/or passwords from being embedded in scripts or source code. See also TS-070 Secure Code and Software Assurance Development policy.	5.1.1.e	IA-5	LMH F P
7.5.16	The ISSO shall ensure the information system stores all passwords/PINs/passphrases in encrypted form.	5.1.1.f	IA-5	LMH F P
7.5.17	All new information systems or those undergoing major upgrades shall use or support DHS PIV credentials.	3.14.7.h	IA-5	LMH F P
7.5.18	The ISSO shall ensure user passwords conform to password conventions specified in the passwords/PINs policy. See **DHS CISO Memo dated August 30, 2017, Subject: Alignment of Password Policy with NIST SP 800-63B** for additional guidance.	5.1.1.a	IA-5 (1)	LMH F P

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
7.5.19	The ISSO shall ensure private keys are allocated in a secure manner and protected from unauthorized release.	5.5.3.g	IA-5 (2)	LMH F P
7.5.20	Any Certificate Authority established within the TSA shall be subordinate to the DHS root Certificate Authority.	5.5.2	IA-5 (2)	LMH F P
7.5.21	The ISSO shall configure PKI-based authentication to enforce authorized access to the corresponding private key and map the authenticated identity to the user account.	5.5.2	IA-5 (2)	LMH F P
7.5.22	Registration to receive TSA PKI certificates and PIV cards shall be carried out in person before a CISO-approved registration authority (RA) or local registration authority (LRA) with authorization from the recipient's government supervisor.	5.5.2	IA-5 (3)	LMH F P
7.5.23	Reserved			
7.5.24	Reserved			
7.5.25	Reserved			
7.5.26	Reserved			
7.5.27	Reserved			
7.5.28	Existing physical and logical access control systems shall be compatible with PIV technology, in compliance with NIST 800-116, *A Recommendation for the Use of PIV Credentials in PACS* and DHS guidance.	3.14.7.f	IA-5 PL-5	LMH F
7.5.29	All new information systems under development shall be enabled to support NIST and DHS PIV credentials prior to being made operational.	3.14.7.g	IA-5 (12) PL-5	LMH F
7.5.30	The information system, for hardware token-based authentication, employs mechanisms that satisfy and complies with encryption requirements of FIPS 140-2, Security Requirements for Cryptographic Modules.	5.4.1.b	IA-5 (11)	LMH F P

3.7.6 Authenticator Feedback (IA-6)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
7.6.1	Information system shall be designed and configured to obscure and not to display authenticators in plain text during the logon or authentication process.	5.1.1.g	IA-6	LMH

3.7.7 Cryptographic Module Authentication (IA-7)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
7.7.1	The SO shall ensure information systems use mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, E.O.s, directives, DHS policy, and TSA encryption policy in compliance with TSA TS-002 *Encryption.*	5.5.1.a	IA-7	LMH
7.7.2	The SO shall ensure the information system uses only cryptographic modules that are FIPS PUB 197 (AES-256) compliant and have received FIPS PUB 140-2 validation at the level appropriate to their use.	5.5.1.c	IA-7	LMH
7.7.3	All offices with encryption applications under TSA authority shall develop encryption plans in compliance with TS-002 *Encryption* for sensitive information systems based on information types, information status (at rest or in transit), or specific purpose (to include non-repudiation).	5.5.1.b	IA-7	LMH
7.7.4	TSA-owned USB drives shall use at least AES256 encryption per policy and in compliance with TSA TS-002 *Encryption*.	4.3.1.d	IA-7	LMH
7.7.5	RFID technology shall be evaluated to determine whether or not tag cloning is a significant business risk. If such a significant risk exists, then tag transactions shall be cryptographically authenticated.	4.6.4.f	IA-7 PM-9	LMH

3.7.8 Identification and Authentication (Non-Organizational Users) (IA-8)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
7.8.1	The SO shall ensure systems uniquely identify and authenticate non-TSA users, as well as processes acting on behalf of non-TSA users.	Not Defined	IA-8	LMH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
7.8.2	The CISO shall ensure the process described in OMB M-04-04, *E-Authentication Guidance for Federal Agencies* is followed for reviewing and clearing non-TSA users.	Not Defined	IA-8	LMH
7.8.3	The CISO shall ensure that information system accepts and electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies.	3.14.7	IA-8 (1)	LMH
7.8.4	The information system shall accept Federal Identity, Credential and Access Management (FICAM)-approved third-party credentials.	3.14.7	IA-8 (2)	LMH
7.8.5	The information system shall conform to FICAM-issued profiles.	Not Defined	IA-8 (4)	LMH

3.7.9 Service Identification and Authentication (IA-9)

Currently, this control does not apply to any control baselines, nor does it apply to Privacy or Financial systems.

3.7.10 Adaptive Identification and Authentication (IA-10)

Currently, this control does not apply to any control baselines, nor does it apply to Privacy or Financial systems.

3.7.11 Re-Authentication (IA-11)

Currently, this control does not apply to any control baselines, nor does it apply to Privacy or Financial systems.

3.7.12 Identity Proofing (IA-12)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
7.12.1	Place Holder	TBD	TBD	TBD

3.8 Individual Participation (IP)

3.8.1 Individual Participation Policy and Procedures (IP-1)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
8.1.1	Place Holder	TBD	TBD	TBD

3.8.2 Consent (IP-2)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
8.2.1	Place Holder	TBD	TBD	TBD

3.8.3 Redress (IP-3)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
8.3.1	Place Holder	TBD	TBD	TBD

3.8.4 Privacy Notice (IP-4)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
8.4.1	Place Holder	TBD	TBD	TBD

3.8.5 Privacy Act Statement (IP-5)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
8.5.1	Place Holder	TBD	TBD	TBD

3.8.6 Individual Access (IP-6)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
8.6.1	Place Holder	TBD	TBD	TBD

3.9 Incident Response (IR)

Incident response (IR) deals with the actions required to respond appropriately and deal with events that have or may adversely impact information security. All managers, operators, and users of TSA IT assets have the responsibility to recognize, report, and escalate issues related to information security to the proper responsible individuals and take appropriate action.

An information system security incident is an event that has actual (or the potential for) adverse effects on computer or network operations. Such incidents can result in mission degradation, fraud, waste, or abuse; can compromise information; or can cause loss or damage to property or

information. An incident can result from a computer virus, other malicious software code, employee malfeasance, or a system intruder, either internal or external.

Specific detailed guidance of the information security requirements on incident response is contained in TS-006 *Network Intrusion Detection and Prevention Systems*, TS-007 *Host Intrusion Detection Systems*, TS-008 *End User Assets*, TS-016 *Remote Access*, TS-017 *Controlled Access Areas*, TS-014 *Communications Security*, TS-022 *Public Key Infrastructure*, and TS-024 *Radio Frequency Identification (RFID).*

Guidance can be found in: DHS 4300A PD Attachment F *Incident Response*; FIPS Publications 199 and 200; NIST Special Publications 800-12, 800-16, 800-50, 800-61, 800-83, 800-84, 800-100, 800-115.

3.9.1 Incident Response Policy and Procedures (IR-1)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
9.1.1	The CISO shall develop, disseminate, and annually review/update a documented IR policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among TSA entities, and compliance, along with formal, documented procedures to facilitate the implementation of the IR policy and associated controls.	2.1.3	IR-1 IR-8 PM-9	LMH
9.1.2	The CISO shall develop and publish internal computer security IR plans and incident handling procedures and provide copies to the DHS Enterprise Security Operations Center (ESOC). These procedures shall include a detailed CM process for modification of security device configurations.	4.9.1.k	IR-1 CM-1	LMH F
9.1.3	All information security incidents determined to be violations of information security policy shall be reviewed by the CISO prior to adjudication.	Not Defined	IR-4	LMH
9.1.4	Any known violations of security in regards to information systems shall be reported to the proper authorities immediately (TSA SPOC and immediate supervisor).	3.12	IR-6 PS-8	LMH
9.1.5	Reserved			

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
9.1.6	The CISO shall have the authority to suspend an individual's access to TSA facilities and sensitive information or systems based on conditions that raise a security concern, if there is a reasonable belief that the individual's continued access to TSA's facilities and its sensitive information and systems is not in the best interest of TSA. The CISO shall take into consideration any identified mitigating factors when making this decision.	4.2.1	PE-3	LMH
9.1.7	The TSA SOC shall establish and maintain a continuous IR capability; respond to detected faults, attacks, events, or incidents; and communicate incident reports to external organizations that may be affected.	Not Defined	IR-1	LMH
9.1.8	The TSA SOC shall be operationally subordinate to the DHS ESOC, which provides operational oversight and guidance.	4.9.b	IR-1	LMH
9.1.9	The TSA SOC shall implement procedures and provide guidance on how to respond rapidly to developing incidents.	Not Defined	IR-1	LMH
9.1.10	The TSA SOC shall utilize IR Testing and Exercise scenarios published by the DHS CISO, as required.	4.9.1.p	IR-1	LMH
9.1.11	Reserved			
9.1.12	The SOC shall be under the direction of a Government employee who shall be present at all times.	4.9.l	IR-1	LMH
9.1.13	TSA SOC shall follow the *DHS Privacy Incident Handling Guidance*.	3.14.6.e	IR-1 SI-1	LMH

3.9.2 Incident Response Training (IR-2)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
9.2.1	The CISO shall provide training to personnel at least annually in their IR roles and responsibilities with respect to the information system.	4.9.1.q	IR-2 AT-3	LMH F
9.2.2	The SO shall provide IR training that includes user training in the identification and reporting of suspicious activities, both from external and internal sources.	Not Defined	IR-2 (1)	H F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
9.2.3	The CISO shall ensure end users are trained using an IR support resource that offers guidance and assistance to users of TSA systems for the handling and reporting of security incidents.	Not Defined	IR-2	LMH F

3.9.3 Incident Response Testing (IR-3)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
9.3.1	The CISO shall ensure IR *testing and exercises* are conducted annually in coordination with the DHS CISO.	4.9.1.q	IR-3	MH F
9.3.2	IR testing and exercises shall incorporate automated mechanisms to thoroughly and effectively test/exercise the IR capability.	Not Defined	IR-3	H F
9.3.3	The CISO shall ensure the *coordination of incident response planning* with the DHS CISO.	4.9.1.q	IR-3 (2)	MH F

3.9.4 Incident Handling (IR-4)

Unauthorized activities within TSA are identified in this section. This list is not all-inclusive and all suspected incidents shall be reported.

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
9.4.1	The CISO shall ensure the implementation of an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.	2.1.11	IR-4	LMH F
9.4.2	Incident handling activities shall be coordinated with contingency planning activities.	Not Defined	IR-4	LMH F
9.4.3	Incident handling capability shall incorporate lessons learned from ongoing incident handling activities into IR procedures, training, and testing/exercises, and implements the resulting changes accordingly.	Not Defined	IR-4	LMH F
9.4.4	Upon receiving a suspicious/unsolicited email, users are asked to forward the email to TSA-SPAM@tsa.dhs.gov.	Not Defined	IR-4 PL-4	LMH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
9.4.5	For sensitive security issues such as observing or receiving a non-password protected SSI document, which will require immediate mitigation, users shall advise the TSA Security Operations Center (SOC) via TSA-CSIRT@tsa.dhs.gov or voice on 1-877-242-4533.	Not Defined	IR-4 PL-4	LMH F
9.4.6	For all other security issues such as, for example, observing someone plug-in a non-GFE thumb-drive or flash-drive into a GFE laptop or plugging a non-GFE laptop into a network port, users shall call the TSA SPOC on 1-800-253-8571 and report the same.	Not Defined	IR-4 PL-4	LMH F
9.4.7	Unauthorized physical or logical access to workstations, servers, network devices, and all other TSA IT assets shall be prohibited and handled as incidents	Not Defined	IR-4 PL-4	LMH F
9.4.8	Unauthorized physical access to equipment and cabling areas (to include local area network (LAN) room, computer rooms, telephone closets, wire closets, wire troughs, equipment storage closets, etc.) shall be prohibited and handled as incidents.	Not Defined	IR-4 PL-4	LMH F
9.4.9	Incidents involving the loss, compromise, or inadvertent destruction, of COMSEC equipment or key shall be reported to the appropriate TSA COMSEC Custodian. in compliance with TS-014 *COMSEC*.	4300B	IR-4	LMH F
9.4.10	TSA COMSEC Custodian shall report incidents involving loss, compromise, or inadvertent destruction of TSA COMSEC equipment or key within 24 hours to the DHS Central Office of Record and the NSA in compliance with TS-014 *COMSEC*.	4300B	IR-4	LMH F
9.4.11	Users shall immediately report any inappropriate or suspicious handling of PII controlled by TSA to their Program Manager.	3.14.6.d	IR-4	LMH F
9.4.12	All incidents involving PII shall be coordinated with the TSA Privacy Office and TSA CISO for evaluation and reporting of the incident to the TSA CSIRT and subsequent reporting to the DHS ESOC.	3.14.6.a	IR-4 IR-6	LMH F
9.4.13	Suspected or confirmed incidents involving PII shall be immediately reported to the SPOC and/or TSA Privacy Office, regardless of the manner of occurrence.	3.14.6.b	IR-4 IR-6	LMH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
9.4.14	The TSA Privacy Officer and CISO shall jointly evaluate the incident, and the CISO shall report the incident to the TSA SOC.	3.14.6.b	IR-4 IR-6	LMH F
9.4.15	The SOC shall immediately report any privacy incidents to the DHS CSIRT/SOC.	3.14.6.a	IR-4 IR-6	LMH F
9.4.16	For suspected or confirmed incidents of improper destruction of PII, proper methods of destruction of PII are defined in TSA MD 3700-4 *Handling Sensitive Personally Identifiable Information.*	3.14..1. e	IR-4	LMH F
9.4.17	In the event of a PII mishandling incident, remediation actions shall be consistent with the requirements of *The Privacy Act*, 5 U.S.C. § 552a.	Not Defined	IR-4	LMH F
9.4.18	Any loss, theft, or damage to a computer system, software, or sensitive data shall be promptly documented and reported to the SPOC; the SPOC shall notify the corresponding ISSO.	Not Defined	IR-4	LMH F
9.4.19	SOCs shall ensure that personnel are appropriately cleared to access the Joint Worldwide Intelligence Communications System (JWICS). SOC managers are free to determine the number and type of personnel to be cleared, but at least one cleared person shall be available per shift. (This person may be on call.) A government officer shall be available continuously for IR and management.	4.9.f	IR-4	LMH F
9.4.20	The CISO shall oversee the support of incidents, internal and external assessments, and on-going SELC support.	5.4.8.b	IR-4	LMH F
9.4.21	The CISO shall ensure weekly IR tracking is performed for TSA CFO designated systems.	3.15.g	IR-5	MH F
9.4.22	The SOC shall have the capability to process intelligence information at the collateral level or above.	4.9.e	IR-4	LMH F
9.4.23	An automated mechanisms shall be used to support the incident handling process.	2.1.10	IR-4 (1)	MH F
9.4.24	In order to mitigate disruptive events concerning systems or components of a system, a coordinated effort shall be made to quickly assess the reported information and initiate an appropriate response.	Not Defined	IR-4	LMH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
9.4.25	The CISO shall ensure the correlation of incident information and individual incident responses in order to achieve an enterprise-wide perspective and awareness of incident responses.	Not Defined	IR-4 (4)	H F

3.9.5 Incident Monitoring (IR-5)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
9.5.1	The SOC shall monitor, document, and report incident investigation and incident remediation activities to the CISO until the incident is resolved.	Not Defined	IR-5	LMH
9.5.2	Security-related events on TSA systems shall be logged and audit trails saved in compliance with the TS-049 Information System Logging policy.	5.3.d	IR-5	LMH F
9.5.3	The ISSO and SO shall be notified of any security-related events for the information system, and they shall review logs and report incidents to the SOC. Corrective measures shall be prescribed, as needed.	Not Defined	IR-5	LMH F
9.5.4	The CISO shall ensure weekly IR tracking is performed for TSA CFO designated systems.	3.15.g	IR-5	LMH F
9.5.5	Automated tools and mechanisms shall be implemented and used to assist in the tracking of security incidents and in the collection and analysis of incident information.	Not Defined	IR-5 (1)	H F

3.9.6 Incident Reporting (IR-6)

Detailed guidance on incident reporting is located in DHS 4300A PD Attachment F *Incident Response and Reporting*, Section 3.0.

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
9.6.1	All TSA employees and contractors shall immediately report violations and suspected incidents to the SPOC.	4.9	IR-6	LMH F
9.6.2	The SPOC shall immediately report violations to the SOC.	4.9	IR-6	LMH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
9.6.3	The SOC shall report significant incidents to the DHS ESOC via EOCOnline (https://eoconline.dhs.gov) as soon as possible but not later than one hour after discovery of the incident. Other means of reporting, such as calling (1-877-DHS1NET) or emailing DHS.ESOC@hq.dhs.gov are acceptable, but the Component positively verifies that notification, if not submitted via EOConline, is acknowledged by the DHS ESOC.	4.9.1.b	IR-6	LMH F
9.6.4	The SOC shall ensure significant HSDN incidents are documented with a preliminary report that shall be provided to the HSDN Government Watch Officer or DHS ESOC within one hour. An initial detailed report shall be provided to the DHS ESOC as soon as possible but not later than one hour from "validation" via secure communications. Subsequent updates and status reports shall be provided to the DHS ESOC every twenty-four (24) hours via HSDN SOC ONLINE until incident resolution or when new information is discovered. Significant incidents are reported individually on a per incident basis and shall not be reported in the monthly summary report.	4.9.1.c	IR-6	LMH F
9.6.5	The SOC shall report minor incidents via the DHS ESOC portal (https://eoconline.dhs.gov) within 24 hours of validation. HSDN incidents or incidents involving SECRET information shall be documented in a summary report and sent via secure email to the HSDN SOC.	4.9.1.d	IR-6	LMH F
9.6.6	The SOC shall report on information security operations status and incident reporting to the DHS as required.	5.4.4.e	IR-6	LMH F
9.6.7	The SOC shall report incidents to the DHS ESOC in compliance with the *DHS ESOC CONOPS* and not directly to the US-CERT or other external entity.	4.9.1.f	IR-6	LMH F
9.6.8	The SOC shall coordinate all external law enforcement involvements through the DHS ESOC and obtain guidance from the DHS ESOC before contacting local law enforcement. Exceptions are only made during emergencies where there is risk to life, limb, or destruction of property. In cases of emergency notification, TSA personnel shall notify the DHS ESOC as soon as possible, by the most expedient means available.	4.9.2.a	IR-6	LMH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
9.6.9	Security Incidents shall include law enforcement (LE) or counter intelligence (CI) elements, such as maintaining a chain of custody. All incidents containing a LE/CI aspect shall be coordinated with the DHS CSO through the DHS ESOC.	4.9.2.b	IR-6	LMH F
9.6.10	The SOC shall report incidents in the weekly incident report, negative reports are required.	Not Defined	IR-6	LMH F
9.6.11	Theft or suspected theft of any end user asset shall be reported to the TSA SPOC within twenty-four (24) hours of detection.	Not Defined	IR-6	LMH F
9.6.12	Any TSA user discovering a suspected or confirmed privacy incident shall coordinate with the TSA SOC, TSA Privacy Officer, and/or TSA CISO to evaluate and subsequently report the incident to the DHS ESOC immediately upon discovery.	3.14.6.a 3.14.6.b	IR-6 IR-7 AU-1	LMH F
9.6.13	Reserved			
9.6.14	TSA personnel shall also report suspected or confirmed privacy incidents or incidents involving PII to the TSA Privacy Officer immediately upon discovery/detection, regardless of the manner in which it might have occurred.	3.14.6.d	IR-6	LMH F
9.6.15	Reserved			
9.6.16	Automated tools and mechanisms shall be implemented and used to assist in the reporting of security incidents.	4.9	IR-6 (1)	MH F

3.9.7 Incident Response Assistance (IR-7)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
9.7.1	Reserved			
9.7.2	TSA IAD shall establish and maintain a forensic capability, as well as a full SOC capability.	4.9.g	IR-7	LMH F
9.7.3	The SO shall employ automated mechanisms to increase the availability of IR related information and support.	Not Defined	IR-7 (1)	MH F

3.9.8 Incident Response Plan (IR-8)

TSA's mission, strategies, and goals for IR help determine the structure of its IR capability and contribute to the uniform approach to responding to incidents.

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
9.8.1	The CISO shall ensure TSA systems have a formal, focused, and coordinated approach to responding to incidents.	Not Defined	IR-8	LMH
9.8.2	The SO shall develop the IR plan for the system.	Not Defined	IR-8	LMH
9.8.3	The IR plan shall provide the information system with a roadmap for implementing its IR capability.	Not Defined	IR-8	LMH
9.8.4	The IR plan shall describe the structure and organization of the incident response capability.	Not Defined	IR-8	LMH
9.8.5	The IR plan shall provide a high-level approach for how the incident response capability fits into the overall TSA mission.	Not Defined	IR-8	LMH
9.8.6	The IR plan shall meet the TSA-specific requirements, which relate to mission, size, structure, and functions.	Not Defined	IR-8	LMH
9.8.7	The IR plan shall define reportable incidents.	Not Defined	IR-8	LMH
9.8.8	The IR plan shall provide metrics for measuring the incident response capability.	Not Defined	IR-8	LMH
9.8.9	The IR plan shall define the resources and management support needed to effectively maintain and mature the IR capability.	Not Defined	IR-8	LMH
9.8.10	The IR plan shall be reviewed, approved and published by the TSA SOC and copies provided to the DHS ESOC upon request and as part of the security control assessment.	2.1.11 4.9.1.k	IR-8 IR-1	LMH
9.8.11	Copies of the IR plan and changes to existing plans shall be distributed to all affected system support personnel.	Not Defined	IR-8	LMH
9.8.12	The IR plan shall be revised to address system changes, TSA changes, and problems encountered during plan implementation, execution, or testing.	Not Defined	IR-8	LMH
9.8.13	The CISO, in coordination with the DHS CISO, shall provide an incident response capability and plan to ensure IR testing and exercises are conducted annually.	4.9.1.q	IR-8	LMH

3.9.9 Information Spillage Response (IR-9)

Currently, this control does not apply to any control baselines, nor does it apply to Privacy or Financial systems.

3.9.10 Integrated Information Security Analysis Team (IR-10)

Currently, this control does not apply to any control baselines, nor does it apply to Privacy or Financial systems.

3.10 Maintenance (MA)

System maintenance can have a significant impact on the security of the network and associated data. This control provides direction to minimize the possibility of a negative impact on network operations and security through proper maintenance actions. Maintenance, in this context, deals with activity that evaluates operational network assets to determine the potential for failure, or that repairs failed items in order to return the operational network to a normal state.

Specific detailed guidance on associated information security requirements for configuration changes and related system maintenance activities are contained in TS-002 Encryption and TS-046 Media Sanitization and Disposition.

3.10.1 System Maintenance Policy and Procedures (MA-1)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
10.1.1	The CISO shall develop, disseminate, and annually review/update a formal, documented information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among TSA entities, and compliance; and formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.	2.1.3	MA-1	LMH
10.1.2	The SO shall develop and maintain formal, documented procedures to facilitate the implementation of the maintenance policy and associated system maintenance controls for each information system.	4.8.3.g	MA-1	LMH
10.1.3	Technical support, auditing, and other access required for maintenance by non-TSA parties shall be explicitly covered in the contracts governing those relationships.	Not Defined	MA-1	LMH
10.1.4	SO is responsible for the maintenance of hardware, software, and related components in compliance with all TSA and DHS policy.	Not Defined	MA-1	LMH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
10.1.5	The SO shall ensure that adequate resources shall be provided for the proper performance and requirement maintenance activities for TSA information systems.	Not Defined	MA-1	LMH
10.1.6	The SO shall ensure all maintenance is performed in a manner that does not negatively impact the security or functionality of the information or information system.	Not Defined	MA-1	LMH
10.1.7	The Information System Security Officer (ISSO) shall ensure all scheduled and unscheduled preventative maintenance is documented in the on-site maintenance log.	Not Defined	MA-1	LHM

3.10.2 Controlled Maintenance (MA-2)

Maintaining information systems is critical for performance. TSA controls maintenance by scheduling, documenting, and reviewing records of repairs on information systems IAW manufacturer or vendor specifications or TSA requirements and ensuring that changes do not negatively impact the security or functionality of the system.

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
10.2.1	Hardware and software components within the TSA IT enterprise environment shall have maintenance performed on a routine basis including, at a minimum, IAW manufacturer or vendor specifications.	Not Defined	MA-2	LMH
10.2.2	Configuration changes shall be subject to the SCCB for approval.	Not Defined	MA-2	LMH
10.2.3	Non-emergency maintenance shall be pre-approved and scheduled in advance.	Not Defined	MA-2	LMH
10.2.4	The SO shall ensure users are given advanced notice of scheduled system maintenance and system downtime.	Not Defined	MA-2	LMH
10.2.5	All scheduled preventative maintenance and unscheduled maintenance shall be documented in the on-site maintenance log.	Not Defined	MA-2	LMH
10.2.6	The SCCB shall approve the removal of the information system or system components from TSA facilities for off-site maintenance or repairs.	Not Defined	MA-2	LMH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
10.2.7	The ISSO shall ensure oversight is provided to all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location.	Not Defined	MA-2	LMH
10.2.8	System changes shall be verified prior to returning to operational status to ensure that controls are still functioning properly following maintenance or repair actions.	Not Defined	MA-2	LMH
10.2.9	In the maintenance of hardware assets, maintenance logs shall include the name of component, location, rack, elevation, part, and serial number.	Not Defined	MA-2	LMH
10.2.10	In the maintenance of software components, maintenance logs shall include the software product name, name and location of software component (to include server, laptop, workstation, etc.) housing the software, and, if appropriate, the rack, elevation, part, and serial number.	Not Defined	MA-2	LMH
10.2.11	The SO shall ensure that, whenever possible, all IT equipment is properly sanitized per in compliance with TS-046 Media Sanitization and Disposition policy to remove all information from associated media prior to removal from TSA facilities or TSA contractor areas for off-site maintenance or repairs.	Not Defined	MA-2 MA-4 (3)	LMH
10.2.12	Maintenance records for the information system shall include date and time of maintenance, name of the individual performing the maintenance, name of escort (if necessary), a description of the maintenance performed, and a list of equipment removed or replaced (including ID numbers if applicable).	Not Defined	MA-2	MH
10.2.13	An automated mechanism shall be employed to schedule, conduct, and document maintenance and repairs as required, producing up-to-date, accurate, complete and available records of all maintenance and repair actions needed, in process, and completed.	Not Defined	MA-2 (2)	H

3.10.3 Maintenance Tools (MA-3)

The intent of this control is to address the security-related issues arising from the hardware and software brought into the information system specifically for diagnostic and repair actions (to include a hardware or software packet sniffer that is introduced for the purpose of a particular maintenance activity). Hardware and/or software components that may support information system maintenance, yet are a part of the systems authorization (to include the software implementing “ping,” “ls,”

"ipconfig," or the hardware and software implementing the monitoring port of an Ethernet switch) are not covered by this control.

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
10.3.1	The SO shall ensure that all information system maintenance tools are approved, controlled, monitored for proper use, and maintained on an ongoing basis.	Not Defined	MA-3 MA-4	MH
10.3.2	Maintenance tools brought into the facility by maintenance personnel, including diagnostic and test equipment used to conduct maintenance on the information system, shall be inspected for obvious improper modifications.	Not Defined	MA-3 (1)	MH
10.3.3	Media containing diagnostic and test programs shall be checked for malicious code before use in the information system.	Not Defined	MA-3 (2)	MH
10.3.4	The removal of maintenance equipment shall be in compliance with the terms of the contract. Maintenance equipment approved for removal shall be verified as either not containing TSA information on the equipment, be sanitized or destroyed, or be retained within TSA in compliance with TS-046 per Media Sanitization and Disposition.	Not Defined	MA-3 (3)	H

3.10.4 Nonlocal Maintenance (MA-4)

TSA shall identify and authenticate components and techniques used in establishing non-local maintenance and diagnostic sessions as required by IA-2. TSA shall control the use of non-local maintenance through policy, monitoring controls, and documenting these in the SP. Non-local maintenance is also referred to as remote maintenance.

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
10.4.1	The SO shall ensure that remote maintenance and diagnostic activities of information systems are authorized, monitored, and controlled.	Not Defined	MA-4	LMH
10.4.2	The SO shall ensure that remote maintenance of information systems, including the network printers, copiers, and facsimile machines, is conducted only from within TSA networks.	4.12.e	MA-4	LMH
10.4.3	Remote maintenance shall be performed in compliance with TSA policy and the information system's SP.	Not Defined	MA-4	LMH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
10.4.4	If maintenance planning does not include performing remote maintenance, the SO shall ensure that remote maintenance capabilities are disabled on the information system.	4.12.e	MA-4	LMH
10.4.5	Remote maintenance shall be authorized in advance by the SO and monitored or performed by a TSA employee with knowledge to detect any inappropriate action.	Not Defined	MA-4	LMH
10.4.6	Remote maintenance paths to the firewalls and Policy Enforcement Points (PEPs) shall be encrypted in compliance with TS-002 *Encryption*.	5.4.4.c	MA-4	LMH
10.4.7	The ISSO shall develop, maintain, and perform a monthly review of information systems logs for remote maintenance.	Not Defined	MA-4	LMH
10.4.8	Maintenance logs for remote maintenance and diagnostic sessions shall include a chronological list of each remote diagnostic session, the name of the individual performing the maintenance, the TSA monitor's name (if required), date, time of session, ticket number, and any other relevant information for tracking purposes.	Not Defined	MA-4	LMH
10.4.9	All ports or services used to perform maintenance shall be closed or terminated once maintenance is complete.	4.8.3.e	MA-4	LMH
10.4.10	A local site representative shall be in communication with the remote diagnostic site for the duration of the remote diagnostic session and to verify remote session completion or disconnect.	Not Defined	MA-4	LMH
10.4.11	The expiration of all session tokens used during the remote diagnostic session shall be verified immediately after remote session disconnect.	Not Defined	MA-4	LMH
10.4.12	The SO shall ensure strong identification and authentication techniques are employed in the establishment of remote maintenance and diagnostic sessions.	Not Defined	MA-4	LMH
10.4.13	All passwords used during the remote diagnostic sessions shall be changed immediately after remote session disconnect.	Not Defined	MA-4	LMH
10.4.14	IAD shall audit remote maintenance and diagnostic session including review of the maintenance records of the sessions.	Not Defined	MA-4	MH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
10.4.15	The ISSO shall document within the SP the installation and use of remote maintenance and diagnostic connections.	Not Defined	MA-4 (2)	MH
10.4.16	The SO shall ensure that remote maintenance and diagnostic services be performed from an information system that implements a level of security at least as high as that implemented on the system being serviced.	Not Defined	MA-4 (3)	H
10.4.17	IT assets to be serviced remotely shall be disconnected from the information system prior to non-local maintenance or diagnostic services. After the service is performed, the IT asset shall be inspected for potentially malicious software and surreptitious implants and be sanitized before being reconnected to the information system.	Not Defined	MA-4 (3)	H

3.10.5 Maintenance Personnel (MA-5)

TSA maintains procedures for maintenance personnel. All personnel required in assisting TSA with diagnostic or maintenance of information systems shall adhere to TSA policy.

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
10.5.1	The ISSO shall develop and maintain a list of cleared vendor personnel authorized to perform maintenance on TSA information systems. This list shall include the on-call personnel (to include employees, contractors, or others), their approved data access level, and their authorization to perform maintenance and repair on TSA infrastructure and end user assets.	4.12.f 4.8.3.h	MA-5	LMH
10.5.2	Each TSA location, including CAAs and ISRAs, shall use the vendor maintenance lists to verify access prior to allowing maintenance or repairs.	Not Defined	MA-5	LMH
10.5.3	Individuals contracted directly by TSA (and holding a PIV card) for the purpose of monitoring and maintaining TSA equipment shall be allowed access to TSA IT assets to perform proper maintenance. A federal manager or designee shall be onsite to answer any questions and to monitor events. See contract requirements for additional information.	4.8.3.h	MA-5	LMH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
10.5.4	Maintenance personnel without a PIV card and not on the approved maintenance personnel list shall be first vetted, cleared, authorized to perform the maintenance task, and subsequently escorted at all times by a TSA employee who has the knowledge to detect any inappropriate action while monitoring maintenance activities. See contract requirements for additional information.	4.8.3.h 4.12.g	MA-5	LMH
10.5.5	Maintenance on IT devices performed using a different user's identity shall be performed only when that user is present. The user shall log in and observe all maintenance actions. Users shall not share their authentication information with maintenance personnel.	4.8.3.i	MA-5	LMH
10.5.6	SO shall ensure that IT assets, including network printers, copiers, alarm control systems, and facsimile machines, are configured to restrict administrator access to authorized individuals or groups.	4.12.f	MA-5	LMH
10.5.7	All vetted and cleared maintenance personnel authorized to access TSA IT assets shall be U.S. citizens with only a few exceptions approved by the CSO.	4.1.1.e	MA-5 PS-3	LMH
10.5.8	The SO shall: a. Implement procedures for maintenance personnel who have appropriate security clearances and are U.S. citizens to include the following requirements: (1) Maintenance personnel shall be escorted and supervised during the performance of maintenance and diagnostic activities on the information system by approved and cleared organizational personnel who have appropriate access authorizations, and are technically qualified; and (2) Prior to initiating maintenance or diagnostic activities, all information within the information system shall be protected from inadvertent information disclosure. b. Develop and implement alternate security safeguards in the event an information system component cannot be protected from information disclosure, removed, or disconnected from the system. See *TSA MD 2800.7 Access Control and Issuance of HQ Photo Access Badge* for additional information.	4.8.3.h	MA-5 (1)	H

3.10.6 Timely Maintenance (MA-6)

Information systems require regular maintenance to be efficient. TSA shall obtain maintenance support and/or have spare parts available in a timely manner.

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
10.6.1	Spare or backup parts and equipment shall be maintained for critical TSA IT assets to preserve mission capabilities.	Not Defined	MA-6	MH
10.6.2	Spare or backup parts and equipment shall be maintained to the current system configuration and available for replacement into *operational systems* in one day or less.	Not Defined	MA-6	M
10.6.3	Spare or backup parts and equipment shall be maintained to the current system configuration and available for replacement into *mission critical operational systems* in one hour or less.	Not Defined	MA-6	H

3.11 Media Protection (MP)

The data processed by, or used in, the operation of TSA IT assets may require access or distribution restrictions based on the content's sensitivity. MP is applicable to all TSA IT media (to include hard drives, optical disks, USB flash/stick memory, thumb-drives, etc.).

The term *marking* is used when referring to the application or use of readable security attributes. Labeling refers to the application or use of security attributes with regard to internal data structures within an information system. This control defines marking and labeling requirements for IT media and applies to all TSA media, at rest or in transit, produced or used in support of all TSA operations including production and test (or development) environments.

Sanitization is the process of removing information from media such that data recovery is not possible and includes removing all classified labels, markings, and activity logs. Three types of sanitization are recognized and accepted by the TSA: clearing, purging, and destruction. Each type of sanitization has unique methods appropriate for different media. TSA requires that all IT media containing TSA data be sanitized prior to reuse or disposal.

Specific detailed guidance of the information security requirements on media protection is contained in the TSA Technical Standards (TS) TS-002 *Encryption*, TS-008 *End User Assets*, TS-016 *Remote Access*, TS-025 *Virtual Private Networks (VPNs)*, TS-046 *IT Media Sanitization*, TS-049 *Information Systems Logging*.

Guidance can be found in: FIPS Publication 199; NIST Special Publications 800-56, 800-57, 800-60, 800-88, and 800-111.

3.11.1 Media Protection Policy and Procedures (MP-1)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
11.1.1	The CISO shall develop, disseminate, annually review, and update a formal, documented media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among TSA entities, and compliance; and formal, documented procedures to facilitate the implementation of the media protection policy and associated controls.	Not Defined	MP-1	LMH
11.1.2	CISO shall establish procedures to ensure that paper and electronic outputs from systems containing sensitive information are protected.	4.3.1.f 4.3.1.g	MP-1	LMH

3.11.2 Media Access (MP-2)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
11.2.1	Only *TSA-approved* and *furnished* removable media issued by the User's supervisor, including FIPS 140-2 / AES-256 encrypted USB flash-memory, thumb-drives and/or external hard drives, will be used to connect, store, move and/or process any TSA related data on any TSA-approved equipment. Prior to use, these thumb-drives and external hard drives must first be tracked via the Sunflower Inventory System and each device must have a red-and-white TSA-U.S. Government Property asset tag. For a detailed list of TSA-approved and supervisor-issued encrypted removable media, contact the IAD IA Policy team. See ***Approved Products Page*** for primary and secondary encrypted thumb-drives authorized by TSA. NOTE: Secondary thumb-drives must only be used in the event the primary series is not viable. Users must never obtain or purchase any thumb-drives or external drives on their own either online or via store purchase, and must never connect these unauthorized devices to any TSA-approved equipment.	4.3.1.c	MP-2	LMH F
11.2.2	Non-GFE removable media shall not be connected to TSA IT assets.	4.3	MP-2	LMH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
11.2.3	Sensitive PII contained within a non-routine or ad hoc Computer Readable Extract (CRE) (to include CREs not included within the boundaries of a source security plan) shall not be removed, physically or otherwise, from a TSA facility without written authorization from the Information Owner responsible for ensuring that the disclosure of the CRE data is lawful and in compliance with this and applicable TSA privacy and security policy.	3.14.5.d	AC-3 MP-2	LMH F
11.2.4	Unless approved by the AO, TSA GFE-removable media such as a USB: thumb-drive, flash-drive, stick, or other external drive shall ***not*** be connected to any non-GFE hardware such as a personal: laptop, desktop, tablet, smartphone, contractor issued or any other personal device.	4.3.1.c	MP-2 AC-20	LMH F
11.2.5	Reserved			
11.2.6	Reserved			
11.2.7	Reserved			

3.11.3 Media Marking (MP-3)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
11.3.1	TSA personnel shall appropriately mark media and other physical information system output (to include electronic documents created) indicating distribution limitations, handling stipulations, and applicable security markings.	4.3.2.a	MP-3	MH
11.3.2	Unclassified media shall be marked and labeled in compliance with current applicable authorities including: a. 49 C.F.R. Parts 15 and 1520 *Sensitive Security Information;* b. TSA *SSI: Policies and Procedure Guide.* c. DHS MD 11042.1 *Safeguarding Sensitive but Unclassified (For Official Use Only) Information;* and d. TS-013 Media Marking.	4.3.2.a	MP-3	MH
11.3.3	TSA Administrator is the designating authority for TSA SSI.	Not Defined	MP-3	MH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
11.3.4	Media determined to be classified pursuant to E.O. 13526 shall use marking guidance issued by the Information Security Oversight Office (ISOO) in its Implementing Directive No. 1, *Classified National Security Information*, and effective December 29, 2009.	1.4.1	MP-3	MH
11.3.5	TSA Office of Security shall be the authority for all TSA classified media in compliance with ISOO Implementing Directive No. 1.	Not Defined	MP-3	MH
11.3.6	Reserved			
11.3.7	Reserved			

3.11.4 Media Storage (MP-4)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
11.4.1	All media with resident data (to include diskettes, optical discs, hard drives, flash-media, thumb-drives, etc.) containing sensitive information (FOUO, SSI, SPII, PII, etc.), including backup media and MEM, shall be placed in a secure location when not in use and throughout the media's lifecycle from creation through sanitization. Refer to TS-002 *Encryption.*	4.3.1.a	MP-4	MH F
11.4.2	A locked, secure location for storage of diskettes, removable flash- memory and media, optical disks including DVD and CDs, and other documents containing private, sensitive, or restricted data shall be available to the user within or near the user's primary workspace.	Not Defined	MP-4	MH F
11.4.3	Access to lockable storage areas (to include keys, combinations, etc.) shall be restricted to a minimum number of authorized individuals and shall be controlled in compliance with TS-014 Communications Security policy. *(COMSEC).*	Not Defined	MP-4	MH F
11.4.4	CAAs shall have lockable storage to store all sensitive data during times when the area is unoccupied or the data is not required.	4.3.1.a	MP-4	MH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
11.4.5	When contacting an authorized and cleared person via phone to discuss sensitive information, TSA personnel shall not leave a recorded message containing sensitive information on any voice mail system. In the event the receiver does not pick up, just simply hang-up and call again at a later time.	4.4.3.a	MP-4	MH F
11.4.6	Reserved			
11.4.7	All database extracts containing PII shall only be printed by authorized users and destroyed within ninety (90) days of generation. A notice of destruction shall be sent to the information owner of the PII upon destruction. Should the PII extract be required to be maintained for more than 90 days, the information owner shall be notified and a new destruction date established.	3.14.5.f	MP-4	MH
11.4.8	The SO shall ensure that media access for the information systems is restricted to approved personnel only.	Not Defined	MP-4	MH
11.4.9	Prior to handling, TSA personnel, contractors, and others working on behalf of TSA with access to TSA data and media shall receive training on its proper handling, processing, and controlling.	Not Defined	MP-4	MH
11.4.10	ISSO shall implement automatic physical and logical access controls designed to reduce risk of unauthorized access by removable media.	Not Defined	MP-4	MH

3.11.5 Media Transport (MP-5)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
11.5.1	The CISO shall ensure procedures are developed for handling paper and electronic outputs, and transporting or mailing sensitive media.	4.3.1.h 3.14.1	MP-5	MH
11.5.2	SO shall ensure protection of sensitive digital and non-digital media during transport outside of controlled access areas.	4.3.1.h	MP-5	MH
11.5.3	The SO shall ensure accountability for information system media during transport outside of controlled areas.	4.3.1.h	MP-5	MH
11.5.4	The SO shall ensure the activities associated with transport of media are restricted to authorized personnel.	Not Defined	MP-5	MH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
11.5.5	TSA personnel shall follow the procedures established by DHS MD 11042.1, *Safeguarding Sensitive But Unclassified (FOUO) Information*, for the transportation or mailing of sensitive media and restrict pickup, receipt, and delivery to authorized personnel.	4.3.1.h 4.3.2.b	MP-5	MH
11.5.6	TSA personnel shall secure unclassified GFE laptops when transporting them by using non-descript carrying cases or containers and storing them in secure, locked locations when left unattended while transporting them outside of TSA facilities.	4.3.2	MP-5	MH
11.5.7	TSA personnel shall ensure GFE laptops are marked with appropriate contact information applied in a readily visible location.	Not Defined	MP-5	MH
11.5.8	Reserved			
11.5.9	The ISSO shall ensure documentation requirements for activities associated with the transport of information system media are defined IAW the sensitivity and FIPS 199 Confidentiality potential impact level of the information.	Not Defined	MP-5	MH
11.5.10	ISSO shall establish and review chain-of-custody documentation requirements for systems under their control at least annually.	4.11.g	MP-5	H
11.5.11	Chain of custody records shall identify all custodians, unique media characteristics, dates, and times of transfer and access to media, and geographic locations through which media travels and is stored.	Not Defined	MP-5	H
11.5.12	Reserved			
11.5.13	During transport outside of controlled areas, sensitive data shall use encryption methods outlined in TS-002 Encryption policy.	Not Defined	MP-5 (4)	MH

3.11.6 Media Sanitization (MP-6)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
11.6.1	The SO shall ensure TSA IT media is sanitized using a TSA-approved sanitization method prior to disposal, reuse, or transfer of custody to any entity for purposes other than media sanitization.	4.3.3.a	MP-6	LMH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
11.6.2	All unclassified media sanitization, reuse, and disposal actions shall comply with the minimum requirements set forth in NIST SP 800-88 *Guidelines for Media Sanitization* using only TSA approved standards and tools to perform sanitization in compliance with TS-046 IT Media Sanitization and Disposition policy.	Not Defined	MP-6	LMH
11.6.3	Media containing classified information, pursuant to E.O. 13526, shall be sanitized by destruction consistent with NSA and CSS *Storage Device Declassification Manual,* DHS 4300B Policy Directive *National Security Systems, Sanitization of IT Media* and TS-046 *IT Media Sanitization and Disposition*.	Not Defined	MP-6	LMH
11.6.4	Unclassified IT media shall be sanitized per TSA policy on SOP and TS-046 *IT Media Sanitization and* Disposition.	Not Defined	MP-6	LMH
11.6.5	TSA IT asset inventory lists shall be maintained and updated to reflect the current configuration, location, and owner of the affected assets throughout the sanitization process.	4.3.3.b	MP-6	LMH
11.6.6	Sanitization records shall be maintained by the SO in compliance with TS-046 *IT Media Sanitization and Disposition.*	4.3.3.b	MP-6	LMH
11.6.7	The SO shall: a. use TSA Form 1412 *Media Sanitization Certificate* to formally sanitize information system media, b. enforce dual-authorizations for the sanitization of information system media to ensure sanitization occurs as intended and to protect against errors and false claims of having performed the sanitization actions, c. sanitize media using two independent and technically qualified individuals to perform the task IAW applicable federal standards, policies, and procedures, d. ensure one individual *Conducts* the sanitization task while the other *Validates* or *Verifies* this task, and e. ensure that the representative signing at the bottom of TSA Form 1412 that *Validates* the sanitization process is not from the same organization.	Not Defined	MP-6	LMH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
11.6.8	TSA media shall only be reused within TSA in compliance with TS-046 *IT Media Sanitization and Disposition.*	Not Defined	MP-6	LMH
11.6.9	Only current and approved TSA images shall be applied to TSA media.	Not Defined	MP-6	LMH
11.6.10	Deleting a file shall not be a valid method for sanitizing media and shall not be used for sanitization.	Not Defined	MP-6	LMH
11.6.11	Verification of successful media sanitization shall be conducted by individuals other than those performing the sanitization. in compliance with TS-046 *IT Media Sanitization and Disposition.*	Not Defined	MP-6	LMH
11.6.12	Personnel performing or verifying sanitization shall be trained in equipment and tool operation, approved techniques, and procedures on an annual basis. in compliance with TS-046 *IT Media Sanitization and Disposition.*	Not Defined	MP-6	LMH
11.6.13	Reserved			
11.6.14	Degaussing, Secure Erase (for ATA hard drives only), and other methods, as identified in the NIST SP 800-88 *Guideline for Media Sanitization* and DOD 5220.22-M *Data Sanitization Method*, shall be the only approved methods permitted for purging media.	Not Defined	MP-6	LMH
11.6.15	Reserved			
11.6.16	The CISO shall ensure memory and hard drives do not leave TSA facilities. The old memory and hard drives are to be replaced and destroyed as sensitive media.	4.12.h	MP-6	LMH
11.6.17	TSA printer locations shall have shredders and TSA-approved sensitive material disposal bins available for use.	Not Defined	MP-6	LMH
11.6.18	All ad hoc CREs shall be documented, tracked, and validated every ninety (90) days after their creation to ensure that their continued authorized use is still required or that they have been appropriately destroyed or erased.	3.14.5.e	AU-11 AU-6 MP-6	LMH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
11.6.19	Ad hoc CREs shall be destroyed or erased within ninety (90) days unless the information included in the extracts is required beyond that period. Permanent erasure of the extracts or the need for continued use of the data shall be documented by the information owner and audited periodically by the TSA Privacy Officer.	3.14.5.f	MP-6 AU-11	MH F
11.6.20	Mobile devices shall be sanitized of all information before being reused by another individual, office, or DHS Component or placed in indefinite storage; mobile devices that are being disposed of, recycled, or returned to the owner or manufacturer shall first be sanitized using approved procedures.	4.6.2.i	MP-6	LMH
11.6.21	Chain of custody shall be established and documented throughout media sanitization activities.	Not Defined	MP-6 (1)	H
11.6.22	Reserved			
11.6.23	The SO shall periodically ensure the testing of all sanitization software, tools, and equipment.	4.3.3.c	MP-6 (2)	H
11.6.24	The ISSO shall ensure that portable, removable storage devices are sanitized prior to connecting such devices to the information system prior to first use within TSA and when the devices have been subjected to conditions of potential compromise (to include lost and then returned by non TSA personnel).	Not Defined	MP-6 (3)	H

3.11.7 Media Use (MP-7)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
11.7.1	The CISO shall ensure that TSA-owned removable media (and usage of the same) is not connected to any non-TSA information system unless the AO has determined that the risk is acceptable based on compensating controls and published acceptable use guidance.	4.3.1.e	MP-7	LMH
11.7.2	The CISO shall prohibit the use of portable storage devices in enterprise information systems when such devices have no identifiable owner.	Not Defined	MP-7 (1)	MH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
11.7.3	SD memory cards shall not be used with any GFE mobile device to include non-iPhones (e.g., feature phones) and MiFi mobile hotspots without prior written approval of the TSA Authorizing Official (AO). Laptop SD Card readers shall not be used for any purpose without prior written approval of the TSA AO.	Not Defined	MP-7	LMH

3.11.8 Media Downgrading (MP-8)

Currently, this control does not apply to any control baselines, nor does it apply to Privacy or Financial systems.

3.12 Privacy Authorization (PA)

3.12.1 Privacy Authorization Policy and Procedures (PA-1)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
12.1.1	Place Holder	TBD	TBD	TBD

3.12.2 Authority to Collect (PA-2)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
12.2.1	Place Holder	TBD	TBD	TBD

3.12.3 Purpose Specification (PA-3)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
12.3.1	Place Holder	TBD	TBD	TBD

3.12.4 Information Sharing with External Parties

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
12.4.1	Place Holder	TBD	TBD	TBD

3.13 Physical and Environmental Protection (PE)

Measures are taken to ensure protection of TSA operations including perimeter protection using fixed or mobile post guards, controlled access systems, employee identification, proper labeling of areas and material, establishment of redundant systems, and other control methods. This policy provides complementary policy related to information security and TSA physical security governance.

3.13.1 Physical and Environmental Protection Policy and Procedures (PE-1)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
13.1.1	The CISO shall support the TSA Chief Security Officer (CSO) in the development, dissemination, and annual review and update of a formal, documented physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among TSA entities, and compliance. The CISO shall also support the CSO in establishing formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.	Not Defined	PE-1	LMH
13.1.2	The CISO shall support and ensure the development and maintenance of information security policy is conducted addressing physical and environmental protection controls which, combined with the TSA Program of Requirements (POR), provides measures to protect information systems, equipment, and data against possible loss, theft, destruction, damage, hazardous conditions, fire, malicious actions, and natural disasters.	Not Defined	PE-1	LMH
13.1.3	The TSA Office of the Chief Security Officer POR shall be adhered to for construction and security equipment requirements of interior space in facilities provided by the General Services Administration (GSA) and those provided by TSA components directly, whether leased or Government-owned.	Not Defined	PE-1	LMH
13.1.4	Reserved			
13.1.5	Physical controls shall be based on the level of sensitivity, to include classification and risk, determined in compliance with DHS and TSA security policy as reflected in this and other relevant documents.	4.2.1.c 4.2.2.a	PE-1 PM-9	LMH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
13.1.6	Physical and environmental security that maximizes information system and network protection from unauthorized physical access and denial of service (DoS) through environmental system failure shall be implemented.	Not Defined	PE-1	LMH
13.1.7	Reserved			
13.1.8	COMSEC equipment shall be stored in the manner specified in NSTISSC 4001, 4005 and E.O. 13526 similar to material in the same classification level.	Not Defined	PE-1	MH

3.13.2 Physical Access Authorizations (PE-2)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
13.2.1	Areas containing information system servers, controlled interface equipment, associated peripherals, communication equipment, patch panels, etc., or areas where restricted actions occur (to include information assurance monitoring, system administration, etc.) shall be deemed Information Security Restricted Areas (ISRA).	Not Defined	PE-2	LMH F
13.2.2	Access to ISRAs shall be limited to authorized personnel. The list of authorized personnel shall be reviewed at least annually. IT closets located in either an ISRA or public area shall have an Emergency Contact List (ECL) on both the inside and outside of the IT closet door. A copy shall be placed inside the cabinet in the event the outside list is remove or misplaced.	4.2.1.a	PE-2	LMH F
13.2.3	Information Security Restricted Areas (ISRAs) shall be clearly labeled and will have an up-to-date access control list (ACL) posted inside the door in compliance with DHS and TSA physical access policy. Standalone IT cabinets containing IT related equipment and located in an open non-ISRA will have signage on the interior of the IT cabinet door and shall adhere to standard operational security practices.	Not Defined	PE-2	LMH F
13.2.4	Reserved			
13.2.5	Reserved			

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
13.2.6	Visitors will sign-in upon entering DHS facilities housing information systems, equipment, and data. Visitors shall be escorted during their tour and sign-out upon departure. Per National Archives and Records Schedule (GRS) 5.6, Items 110 and 111, Visitor Control Files. Registers or logs used to record names of outside contractors, service personnel, visitors, employees admitted to areas, and reports on automobiles and passengers. Item 110 For areas under maximum security. Destroy 5 years after final entry or 5 years after date of document, as appropriate. Item 111 For other areas. Destroy 2 years after final entry or 2 years after date of document, as appropriate.	4.2.1.d	PE-2	LMH F
13.2.7	ISRA requirements shall extend to TSA IT assets located at non-TSA facilities and non-TSA IT assets and equipment hosting TSA data.	4.2.1.e	PE-2	LMH F
13.2.8	The ISSO shall maintain a record of all physical access by both visitor and authorized individuals.	Not Defined	PE-2	LMH

3.13.3 Physical Access Control (PE-3)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
13.3.1	All IT assets shall be physically protected by access control systems that require positive identification and authentication.	Not Defined	PE-3	LMH F
13.3.2	For all ISRA areas: keys, combinations, or other access devices shall be secured and released only to properly cleared and authorized individuals.	Not Defined	PE-3	LMH F
13.3.3	Hard copies of system security documentation, such as software configurations, stored at either primary or alternate processing locations shall be physically protected.	4.3.1.b	PE-3 CP-6	LMH F
13.3.4	The SO shall enforce physical access authorizations to the information system independent of the physical access controls for the facility.	Not Defined	PE-3 (1)	H F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
13.3.5	The CISO shall ensure controls are in place for deterring, detecting, restricting, and regulating access to sensitive areas and that these controls are sufficient to safeguard against possible loss, theft, destruction, damage, hazardous conditions, fire, malicious actions, and natural disasters.	4.2.1.b	PE-3	LMH
13.3.6	Visitor access shall be limited to those work areas requiring their presence.	4.2.1.d	PE-3	LMH F

3.13.4 Access Control for Transmission (PE-4)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
13.4.1	The SO shall ensure controlled physical access to information system distribution and transmission lines within TSA facilities.	Not Defined	PE-4	MH
13.4.2	Protective measures to control physical access to information system distribution and transmission lines shall be used including: locked wiring closets, disconnected or locked spare jacks, and protection of cabling by conduit or cable trays. An emergency contact list (ECL) shall be visibly posted on IT cabinets in or around the IT closet area.	Not Defined	PE-4	MH
13.4.3	Physical protections shall be implemented to help prevent eavesdropping or in transit modification of unencrypted transmissions.	4.2.1.f	PE-4	MH
13.4.4	Reserved			

3.13.5 Access Control for Output Devices (PE-5)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
13.5.1	TSA users shall ensure sensitive information contained on paper and on electronic devices are not left unattended on a printer for example and are protected from those without a valid business need-to-know.	4.3.1.f	PE-5	MH
13.5.2	Information system output devices including monitors, printers, and audio devices shall be configured and operated IAW their categorization level.	Not Defined	PE-5	MH

3.13.6 Monitoring Physical Access (PE-6)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
13.6.1	SO shall ensure physical access to the information system is monitored to detect and respond to physical security incidents.	4.2	PE-6	LMH
13.6.2	Reserved			
13.6.3	The reviewer of ISRA logs shall coordinate results of reviews and investigations with the TSA SOC.	Not Defined	PE-6	LMH
13.6.4	Facilities Security Managers shall monitor surveillance equipment and recognize real-time physical intrusion alarms.	Not Defined	PE-6 (1)	MH
13.6.5	Airports own and operate their respective closed circuit televisions (CCTVs). In the rare event that DHS or TSA owns and operate an off-network CCTV, see physical security policy regarding CCTVs and related posting of signage at: **DHS PIA CCTV Systems, July 2012** for details. In short, it states that "All DHS CCTV systems shall provide notice of the surveillance camera. Signs are to be posted in public areas, in written format or pictograms."	Not Defined	PE-6 (3)	LMH
13.6.6	Reserved			

3.13.7 Visitor Control (PE-7) (Withdrawn)

Withdrawn and incorporated into PE-2 and PE-3.

3.13.8 Visitor Access Records (PE-8)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
13.8.1	Visitors will: sign-in upon entering DHS or TSA facilities housing information systems, equipment, and data; and be escorted during their stay; as well as sign-out upon departure. Access by non-DHS contractors or vendors will be limited to those work areas requiring their presence and these guests will be escorted at all times. Per **National Archives and General Records Schedule (GRS 5.6) Item 110 and 111 (DAA-GRS-20170006-0014),** Visitor Control Files, page 100. See information on registers or logs used to record names of outside contractors, service personnel, visitors, employees admitted to areas, and reports on automobiles and passengers. Under the section for areas under maximum security, destroy 5 years after final entry or 5 years after date of document, as appropriate. For other areas, destroy 2 years after final entry or 2 years after date of document, as appropriate. These records include the name/organization of the person visiting, signature of the visitor, form(s) of identification, date of access, time of entry and departure, purpose of visit, name, and organization of person visited.	4.2.1.d	PE-8	LMH
13.8.2	The Site Security Officer or Facility Security Manager shall review ISRA visitor access records.	Not Defined	PE-8	LMH
13.8.3	The Site Security Officer or Facility Security Manager responsible for the ISRA shall maintain and review access records.	Not Defined	PE-8 (1)	H
13.8.4	Reserved			

3.13.9 Power Equipment and Cabling (PE-9)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
13.9.1	The SO shall ensure the protection of power equipment and power cabling for the information system from damage and destruction.	Not Defined	PE-9	MH

3.13.10 Emergency Shutoff (PE-10)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
13.10.1	ISRAs, including facilities containing concentrations of information system resources, for example, data centers, server rooms, and mainframe computer rooms, shall provide the capability of shutting off power to the information system or individual system components in emergency situations.	4.2.1.h	PE-10	MH
13.10.2	Each ISRA shall have emergency shutoff switches or devices to facilitate safe and easy access for personnel.	4.2.1.h	PE-10	MH
13.10.3	Emergency power shutoff capabilities shall be protected from unauthorized activation.	4.2.1.h	PE-10	MH
11.10.4	Reserved			

3.13.11 Emergency Power (PE-11)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
13.11.1	Redundant, non-municipal power with battery transfer isolation shall be maintained for critical TSA IT assets. Other redundant power systems shall be maintained in a tested and operational status.	Not Defined	PE-11	MH
13.11.2	A short-term uninterruptible power source shall be installed in the ISRA to facilitate an orderly shutdown of the information system in the event of a primary power source loss.	4.2.1.h	PE-11	MH
13.11.3	A long-term alternate power supply shall be installed in the ISRA for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.	Not Defined	PE-11 (1)	H

3.13.12 Emergency Lighting (PE-12)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
13.12.1	The Facility Security Manager shall employ and maintain automatic emergency lighting for the information system in the TSA facility that activates in the event of a power outage or disruption and that illuminates emergency exits and evacuation routes within the facility.	4.2.1.i	PE-12	LMH

3.13.13 Fire Protection (PE-13)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
13.13.1	The Facility Security Manager shall employ and maintain fire suppression and detection devices or systems (to include sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors) for the TSA facility information systems that are supported by an independent energy source. When a centralized fire suppression system is not available, Class C fire extinguishers (which are designed for use with electrical fire and other types of fire) shall be readily available. Each Class C fire extinguisher shall be located in such a way that a user would not need to travel more than 50 feet to retrieve it.	Not Defined	PE-13	MH
13.13.2	The Facility Security Manager shall employ fire detection devices or systems for the ISRA information system that activate automatically and notify TSA and emergency responders in the event of a fire.	Not Defined	PE-13 (1)	H
13.13.3	The Facility Security Manager shall employ fire suppression devices or systems for the ISRA information system that provides automatic notification of any activation to TSA and to emergency responders in the event of a fire.	Not Defined	PE-13 (2)	H
13.13.4	IT cabinets will have available fire extinguishers or a fire suppression system within 50 feet of cabinets for the protection of information system related equipment.	Not Defined	PE-13 (3)	MH

3.13.14 Temperature and Humidity Controls (PE-14)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
13.14.1	Temperature and humidity levels in computer processing and storage areas will be kept between 64.4 and 80.6 degrees Fahrenheit with 20% to 60% relative humidity (RH).	4.2.1.i	PE-14	LMH

3.13.15 Water Damage Protection (PE-15)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
13.15.1	Information system(s) shall be protected from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.	4.2.1.i	PE-15	LMH
13.15.2	Each ISRA shall employ automated mechanisms that, without the need for manual intervention, protect the information system from water damage in the event of a water leak.	Not Defined	PE-15 (1)	H

3.13.16 Delivery and Removal (PE-16)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
13.16.1	The Facilities Manager shall authorize, monitor, and control all IT assets entering and exiting each ISRA and maintain records of those items.	4.2.1.j	PE-16	LMH F
13.16.2	The Facilities Manager shall enforce authorizations for entry and exit of information system components by restricting access to delivery areas and isolating the areas from the information system and media libraries.	Not Defined	PE-16	LMH F
13.16.3	COMSEC devices shall be hand-carried or shipped via registered mail through USPS registered mail, FedEx or Defense Courier Service (DCS).	Not Defined	PE-16	MH F

3.13.17 Alternate Work Site (PE-17)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
13.17.1	Information systems shall maintain alternate work sites.	Not Defined	PE-17	MH
13.17.2	SO shall assess the effectiveness of security controls at alternate work sites on an annual basis.	Not Defined	PE-17	MH
13.17.3	SO shall ensure communication capabilities exist at the alternate backup site in the event the primary site is unavailable.	Not Defined	PE-17	MH

3.13.18 Location of System Components (PE-18)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
13.18.1	Reserved			
13.18.2	Reserved			
13.18.3	All TSA information system components including end user devices shall be adequately protected within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access or theft.	4.2.1.b	PE-18	MH
13.18.4	All end user assets shall be configured to prevent the unauthorized use of the device, associated input devices (to include keyboards, mice, etc.), floppy drives, and stored programs when left unattended by intended user(s) in a facility.	Not Defined	PE-18	MH
13.18.5	The SO shall ensure adequate physical and IT security is provided for all TSA-owned PBX in compliance with the DHS and TSA physical security policy.	4.4.1.a	PE-18	MH
13.18.6	Each ISRA shall be designed with consideration given to physical and environmental hazards in its risk mitigation strategy.	Not Defined	PE-18 (1)	H

3.13.19 Information Leakage (PE-19)

Currently, this control does not apply to any control baselines, nor does it apply to Privacy or Financial systems.

3.13.20 Asset Monitoring and Tracking (PE-20)

Currently, this control does not apply to any control baselines, nor does it apply to Privacy or Financial systems.

3.13.21 Electromagnetic Pulse Protection (PE-21)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
13.21.1	Place Holder	TBD	TBD	TBD

3.13.22 Component Marking (PE-22)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
13.22.1	Place Holder	TBD	TBD	TBD

3.14 Planning (PL)

This family is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the security planning family.

Specific guidance related to the implementation of security program control and review on TSA IT assets is contained in the following TSA TSs: TS-008 *End User Assets*, TS-016 *Remote Access*, TS-021 *General Telephony*, TS-023 *Voice over Internet Protocol (VoIP)*, and TS-025 *Virtual Private Networks (VPNs*). User understanding and acceptance of applicable policy and legal requirements concerning the operation of computer equipment and access to network resources within the TSA is captured in TS-017 *Controlled Access Areas*.

Guidance can be found in: 5 C.F.R. 731.106(a); OMB Circular A-130; OMB Memorandum 03-22; NIST Special Publications (SP) 800-12, 800-18, 800-37, 800-66, 800-100. TSA MD 1100.73-5 *Employee Responsibilities and Conduct*.

3.14.1 Planning Policy and Procedures (PL-1)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
14.1.1	The CISO shall develop, disseminate, and annually review and update a formal, documented security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among TSA entities, and compliance. The CISO shall establish formal, documented procedures to facilitate the implementation of the security planning policy and associated controls.	Not Defined	PL-1 PM-2	LMH
14.1.2	The SSI Program Office shall review program and system Sensitive Security Information Threshold Analyses (SSITA) and Sensitive Security Information Impact Assessments (SSIIA) documents, providing approval as appropriate.	Not Defined	PL-1	LMH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
14.1.3	A thorough, annual review of the TSA security planning program shall be conducted in compliance with FISMA requirements. This review shall report on the degree to which security requirements have been implemented, significant deficiencies discovered, remedial actions taken or in progress to correct deficiencies, and level of compliance with NIST standards.	Not Defined	PL-1	LMH
14.1.4	The security planning policy shall be internally reviewed, updated, and approved by the CISO at least annually.	Not Defined	PL-1	LMH
14.1.5	The protection of systems shall be documented in an SP in compliance with OMB Circular A-130, Appendix III, and FISMA.	3.1.e	PL-1	LMH
14.1.6	Reserved			
14.1.7	All operational information systems shall comply with plans, policies and procedures unless an approved waiver has been granted.	1.5.1.c	PL-1	LMH

3.14.2 System Security and Privacy Plans (SP) (PL-2)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
14.2.1	The ISSO, on behalf of the SO, shall develop and maintain a Security Plan for each system, major software application, and general support system and network segment for Security Control Assessment purposes.	3.1.c	PL-2	LMH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
14.2.2	The SP shall: a. Be consistent with TSA's enterprise architecture; b. Document mobile device security to the extent feasible and appropriate and be consistent with and complement security policy for non-mobile systems; c. Explicitly define the authorization boundary for the system; d. Describe the operational context of the information system in terms of missions and business processes; e. Provide the security categorization of the information system, including supporting rationale; f. Describe the operational environment for the information system; g. Describe relationships with or connections to other information systems; h. Provide an overview of the security requirements for the system; i. Describe the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and j. Be reviewed and approved by the AO or designated representative prior to plan implementation.	Not Defined	PL-1 PL-2	LMH F
14.2.3	The SP shall be reviewed at least every three years, whenever significant changes occur to the system, or when event triggers occur if the system is in ongoing authorization. Upon entering the Ongoing Authorization Program, OA Components authorize systems at Initial Operating Capability (IOC), through submission of an OA Admission Letter and thereafter as needed, on a time or event driven basis in accordance with OMB A-130, NIST guidance and DHS Ongoing Authorization Methodology	3.9.h	PL-2	LMH F
14.2.4	The TSA WAN, each subordinate LAN, and all MAs shall be included in the SP for which authorization boundary they fall under.	Not Defined	PL-2	LMH F
14.2.5	All SPs shall meet the requirements of the current NIST SP 800-18 *Guide for Developing Security Plans for Information Technology Systems* and DHS guidance.	Not Defined	PL-2	LMH F
14.2.6	The SP shall be reviewed by the CISO, and the final version approved by the AO.	3.1.c	PL-2	LMH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
14.2.7	The ISSO shall ensure a current copy of the SP is available for review by the CISO and AO upon request.	Not Defined	PL-2	LMH F
14.2.8	If PII and Sensitive PII can be physically removed from an information system (to include printouts, CDs, etc), the SP shall document the specific procedures, training, and accountability measures in place to ensure remote use of the data does not bypass the protections provided by the encryption.	3.14.5.b	PL-2	LMH F
14.2.9	Systems that, as part of routine business, remove Sensitive PII in the form of a CRE, (to include routine system-to-system transmissions of data, known as "routine CREs") shall address associated risks in the SP.	3.14.5.c	CA-2 PL-2 RA-2	LMH F
14.2.10	The ISSO shall plan and coordinate security plan related activities affecting the information system with the SO before conducting such activities in order to reduce the impact on other organizational entities.	Not Defined	PL-2 (3)	MH F
14.2.11	The SO shall approve all planned modifications to the information system requiring review by the SCCB prior to change implementation.	Not Defined	PL-2	LMH F
14.2.12	The ISSO shall use the proper waiver request process for any remediation action that cannot be completed within the time period specified in POA&M policy.	3.9.r	PL-2	LMH F
14.2.13	Remediation actions delinquent to the plan by more than one month shall be brought to the attention of the CISO.	Not Defined	PL-2	LMH F
14.2.14	The TSA CFO shall ensure that a fulltime dedicated ISSO is assigned to each CFO designated system without collateral duties. CFO designated system ISSOs may be assigned to more than one CFO designated system.	3.15.k	PL-2	MH F

3.14.3 Security Plan Update (PL-3) (Withdrawn)

Currently, this control does not apply to any control baseline, nor does it apply to Privacy or Financial systems.

3.14.4 Rules of Behavior (ROB) (PL-4)

The use of the warning banner serves as a reminder to all users that the computers they are accessing are Government computers. The DHS CISO stipulates that a warning banner statement be displayed on all DHS systems during logon. The most current language can be found on the DHS CISO web page. Additionally, TSA requires the use of the TSA Acceptable Use Warning Banner, generated by the Office of Human Capital (OHC).

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
14.4.1	The CISO shall establish and make readily available to all information system users, the rules that describe their responsibilities and expected behavior with regard to TSA information and information system usage. The SO may provide additional guidance on their system specific behavioral requirements.	4.1.2.a	PL-4	LMH
14.4.2	Reserved			
14.4.3	The SO shall employ technologies to monitor and enforce these rules of behavior as appropriate for the information system, including, but not limited to, web filtering.	Not Defined	PL-4	LMH
14.4.4	The SO shall develop and implement different sets of rules of behavior based on user roles and responsibilities, for example, differentiating between the rules that apply to privileged users and rules that apply to general users.	Not Defined	PL-4	LMH
14.4.5	TSA users shall follow the prescribed rules of behavior for the information system.	2.2.11.a	PL-4	LMH
14.4.6	The TSA OHC acceptable use warning banner message shall be displayed immediately after users log on to TSA systems to remind users of their responsibilities and conduct, to the extent technologically feasible.	5.2.3	AC-8 PL-4	LMH
14.4.7	The CISO shall ensure that TSA users are trained regarding rules of behavior and that each user signs a copy prior to being granted user accounts or access to information systems or data.	4.1.2.b	AT-1 AT-2 PL-4	LMH
14.4.8	Each TSA workstation, laptop, and tablet shall be assigned to a specific individual as the custodian responsible for compliance with all applicable rules of behavior and acceptable use policy who serves as the custodian of the information contained on that device. An individual or onsite manager shall have general responsibilities for a designated training room desktop.	Not Defined	PL-4	LMH
14.4.9	TSA employees shall use Government office equipment and TSA systems or computers for authorized purposes only.	4.8.4.a	PL-4 PS-6	LMH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
14.4.10	TSA employees shall only use wired telephones or GFE cellular phones with the assurance of privacy when discussing sensitive information and consider their surroundings with regard to unauthorized personnel from eavesdropping on discussions.	4.4.2.a 4.6.2.1.a	PL-4 SC-7	LMH
14.4.11	Reserved			
14.4.12	Pagers shall not be used to transmit sensitive information.	4.6.2.2.a	PL-4	LMH
14.4.13	Limited personal use of TSA email and Internet services is authorized for TSA employees in compliance with TSA ROB	4.8.4.b	PL-4	LMH
14.4.14	The following activities shall be prohibited on TSA information systems: social networking, peer-to-peer networking, software or music sharing or piracy, online gaming, webmail, unofficial Instant Messaging (IM), hacking, and the viewing of pornography, unofficial streaming of audio or video, or other offensive content in compliance with TS -030 *Internet Site Access*.	4.8.4.b	PL-4	LMH
14.4.15	The TSA CISO shall provide written approval before a laptop computer or other mobile computing device is taken outside of the United States or its territories.	4.6.2.v	PL-4	LMH
14.4.16	TSA users shall follow rules of behavior and explicit restrictions on the use of social media or networking sites and posting organizational information on public websites.	Not Defined	PL-4 (1)	MH

3.14.5 Privacy Impact and Risk Assessment (PIA) (PL-5) Withdrawn

Withdrawn and incorporated into Appendix J, AR-2.

3.14.6 Security–Related Activity Planning (PL-6) (Withdrawn)

Withdrawn and incorporated into PL-2.

3.14.7 Concept of Operations (PL-7)

Currently, this control does not apply to any control baselines, nor does it apply to Privacy or Financial systems.

3.14.8 Security and Privacy Architecture (PL-8)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
14.8.1	a. The CISO, in coordination with the Chief Architect, shall ensure that requirements are issued for the development of an information security architecture for an information system that: (1) Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information; (2) Describes how the information security architecture is integrated into and supports the enterprise architecture; and (3) Describes any information security assumptions about, and dependencies on, external services; b. The SO shall ensure the review and update of the information security architecture on a monthly basis in order to reflect updates in the enterprise architecture; and c. The SO shall ensure that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and the organizational procurements and acquisitions.	3.1.g	PL-8	MH

3.14.9 Central Management (PL-9)

Currently, this control does not apply to any control baselines, nor does it apply to Privacy or Financial systems.

3.14.10 Baseline Selection

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
14.10.1	Place Holder	TBD	TBD	TBD

3.14.11 Baseline Tailoring

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
14.11.1	Place Holder	TBD	TBD	TBD

3.15 Program Management (PM) – Moved to Section 3.21

3.16 Personnel Security (PS)

Several laws and regulations require the TSA to protect its information from loss, misuse, or unauthorized access to, or modification of, its information. To that end, TSA shall ensure that only individuals meeting the trustworthiness requirements associated with sensitive security and/or critical data are allowed to access TSA official information. This control applies to all TSA employees, contactors, and any other personnel (including DHS equivalent personnel) using an IT resource to access TSA information.

Specific detailed guidance on personnel security requirements is located with the Office of Security and the Office of Human Capital.

Other guidance: DHS Instruction 121-01-007 *Suitability Screening Requirements for Contractor Employees*, TSA MD 2800.71 *Pre-Employment Investigative Standards for TSA Non-Screener Employees and Contractors*, TSA MD 1100.30-10 *Employee Exit Clearance Procedures*, off boarding *Contractor Separation Instruction Worksheet*, TSA Form 1402 *Separating Non-Screener Employee and Contractor IT Certificate*, DHS Form 11000-6 *Non-Disclosure Agreement (NDA)*, TSA Form 1403 *Computer and Personal Electronic Device Access Agreement (CAA)*, TSA Form 1429 *Privileged Access Request*, TSA MD 1100.75-3 *Addressing Performance and Conduct Problems*, and the *Standards of Ethical Conduct for Employees of the Executive Branch*.

3.16.1 Personnel Security Policy and Procedures (PS-1)

TSA shall ensure that only individuals meeting the trustworthiness requirements associated with sensitive information data are allowed to access TSA information.

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
16.1.1	Under TSA, the Chief of Personnel Security Division, Office of Security, under the direction of the Chief Security Officer (CSO) shall: develop, disseminate, review, and update their personnel security risk assessment policy. This assessment shall address: purpose, scope, roles and responsibilities, management commitment, personnel security risks, coordination among TSA entities, and documented procedures to facilitate the implementation of risk assessment policy.	Not Defined	PS-1	LMH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
16.1.2	The SO shall ensure that support for, and access to, information systems is provided in compliance with the DHS Instruction 121-01-007 *Suitability Screening Requirements for Contractor Employees* and the *DHS Acquisition Regulation (HSAR).*	4.1.1.c 4.1.1.d 4.1.1.e 4.1.1.f	PS-1	LMH
16.1.3	The CISO shall support the CIO and TSA leadership with their responsibilities to ensure implementation and compliance DHS Instruction 121-01-007 *Personnel Suitability and Security Program.*	Not Defined	PS-1	LMH

3.16.2 Position Risk Designation (PS-2)

Positions within TSA are assigned risk designations consistent with the Office of Personnel Management policy and guidance. Screening criteria is specified as part of this designation, such as training and background information.

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
16.2.1	Access to information systems shall be based on position sensitivity levels and shall be designated for all federal and contractor positions that use, develop, operate, or maintain information systems in compliance with TSA Human Capital Management Policy 731-1, *Policy on Determining Position Sensitivity Designations for all TSA Positions.*	4.1.1.a	PS-2 PS-3 PS-7	LMH
16.2.2	The CISO shall review and revise the position risk designations annually.	4.1.1.a	PS-2	LMH
16.2.3	Reserved			
16.2.4	The CISO shall determine if any additional screening criteria is necessary for information security positions or if explicit information security role appointment requirements are met by incumbents.	Not Defined	PS-2 PS-3 PS-7	LMH

3.16.3 Personnel Screening (PS-3)

All personnel given access to TSA IT assets undergo background screening consistent with the requirements of their position's description.

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
16.3.1	Only citizens of the United States of America shall be granted access to TSA information networks.	4.1.1.e	PS-3	LMH F
16.3.2	Requests for exception to U.S. citizenship requirements shall be consistent with DHS 4300A PD.	1.5.2.	PS-3	LMH F
16.3.3	Additional compensating controls shall be maintained for foreign nationals, based on nations' lists maintained by the DHS CSO.	Not Defined	PS-3	LMH F
16.3.4	Positions shall be held by personnel that have favorably adjudicated background investigations commensurate with the defined position sensitivity level and level of information accessed.	4.1.1.b	PS-3	LMH F
16.3.5	No federal employee shall be granted access to TSA information systems without having a favorably adjudicated Tier 2 Investigation (formerly Moderate Risk Background Investigation (MBI)). It is defined in DHS Instruction 121-01-007, *Personnel Suitability and Security Program, Chapter 2, Federal Employee/Applicant Suitability Requirements,* and TSA MD 2800.71 *Pre-Employment Investigative Standards for TSA Non-Screener Employees and Contractors.* In cases where non-DHS Federal employees have been investigated by another Federal agency, TSA personnel security organizations may, whenever practicable, use these investigations to reduce investigation requests, associated costs, and unnecessary delays (Chapter 2, paragraph G). Active duty United States Coast Guard (USCG) and other personnel subject to the Uniform Code of Military Justice (UCMJ) shall be exempt from this requirement.	4.1.1.c	PS-3	LMH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
16.3.6	No contractor personnel shall be granted access to TSA systems without having a favorably adjudicated Background Investigation (BI) as defined in *DHS Acquisition Regulation* (HSAR), DHS Instruction 121-01-007 *Personnel Suitability and Security Program, Chapter 3, Excepted Service Federal Employee and Contractor Employee Fitness Requirements, and* TSA MD 2800.71 *Pre-Employment Investigative Standards for TSA Non-Screener Employees and Contractors.* In cases where contractor personnel have been investigated by another Federal agency, TSA personnel security organizations may, whenever practicable, use these investigations to reduce investigation requests, associated costs, and unnecessary delays (Chapter 3, paragraph G).	4.1.1.d 4.1.1.f	PS-3	LMH F
16.3.7	Background checks shall be refreshed in compliance with TSA MD 2800.71 *Pre-Employment Investigative Standards for TSA Non-Screener Employees and Contractors* and DHS Instruction 121-01-007 *Personnel Suitability and Security Program.*	4.1	PS-3	LMH F
16.3.8	The CISO shall ensure privileged access users shall be appropriately screened on entry into the privileged access position. Privileged access positions include access to administrative roles on any information system connected to the TSA operational environment or processing production data.	Not Defined	PS-3	LMH F

3.16.4 Personnel Termination (PS-4)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
16.4.1	Logical and physical access terminations for all personnel terminations shall be processed in compliance with TSA MD 1100.30-10 *Employee Exit Clearance Procedures.*	4.1.6.a	PS-4	LMH F
16.4.2	The SO shall ensure that privileged access accounts are terminated upon employee termination and this change is documented per policy.	Not Defined	PS-4	LMH F
16.4.3	Exit interviews for all personnel terminations shall be processed in compliance with TSA MD 1100.30-10 *Employee Exit Clearance Procedures.*	Not Defined	PS-4	LMH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
16.4.4	TSA Form 1402 *Separating Non-Screener Employee and Contractor IT Certificate* shall be completed by the separating employee and signed by the employee's supervisor in compliance with TSA MD 1100.30-10 *Employee Exit Clearance Procedures.*	Not Defined	PS-4	LMH F
16.4.5	The signed TSA Form 1402 *Separating Non-Screener Employee and Contractor IT Certificate* shall be maintained by the individual's supervisor for federal employees, and by the COR for contractors and retained IAW the TSA retention schedules. The COR shall also securely retain the off boarding *Contractor Separation Instructions Worksheet* as provided by the vendor for departing contractors.	Not Defined	PS-4	LMH F
16.4.6	Supervisors shall ensure that TSA information system-related property, media and IT assets are recovered from the departing individual with a documented chain of custody are transferred to an authorized individual for reuse or proper sanitization.	Not Defined	PS-4 PS-5	LMH F
16.4.7	Supervisors shall ensure that access to TSA information and information systems formerly controlled by the departing individual is transferred to an authorized individual.	Not Defined	PS-4 PS-5 MP-5 MP-6	LMH F
16.4.8	Reserved			

3.16.5 Personnel Transfer (PS-5)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
16.5.1	Logical and physical access for personnel who are reassigned to new official duty locations within TSA or transferred to other Federal agencies shall be processed in compliance with TSA MD 1100.30-10 *Employee Exit Clearance Procedures.*	4.1.6.b	PS-5	LMH F
16.5.2	Reserved			
16.5.3	Supervisors shall ensure the appropriate transition or revocation of access and physical assets upon personnel transfer.	4.1.6.a	PS-5	LMH F

3.16.6 Access Agreements (PS-6)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
16.6.1	All approved users for TSA IT assets and information access shall sign access agreements to acknowledge that they have read, understood, and agree to abide by the constraints associated with the information systems and/or information for which access is authorized.	Not Defined	PS-6	LMH F
16.6.2	Access agreements shall identify the responsibility of the end user and define rights, privacy, and rules of behavior required to be complied with by the user regarding TSA IT assets and information.	Not Defined	PS-6	LMH F
16.6.3	All individuals who access SSI and/or mission-critical information shall sign access agreements consistent with the level of data accessed.	Not Defined	PS-6	LMH F
16.6.4	Reserved			
16.6.5	All TSA employees and contractors shall execute a DHS Form 11000-6 *DHS Non-Disclosure Agreement (NDA)* and TSA Form 1403 *Computer and Personal Electronic Device Access Agreement (CAA)*, upon initial assignment to TSA and prior to accessing any TSA data types.	Not Defined	PS-6	LMH F
16.6.6	Other individuals not assigned to, or contractually obligated to, TSA, but granted access to TSA information, shall execute a NDA by request as determined by the SO controlling the system with the information to which access is required.	Not Defined	PS-6	LMH F
16.6.7	All TSA personnel (to include managers, employees, and contractors) shall review, understand, and sign TSA Form 1403 *Computer and Personal Electronic Device Access Agreement (CAA)* signifying understanding and acceptance of applicable policy and legal requirements concerning the operation of computer equipment and access to network resources within TSA.	Not Defined	PS-6	LMH F
16.6.8	Completed TSA Forms 1403 CAA shall be obtained and stored by immediate supervisors for all federal employees and by the COR for all contractors.	Not Defined	PS-6	LMH F
16.6.9	Privileged access users shall complete TSA Form 1429 *Privileged Access Request* and sign the *Administrative Privileged Agreement and Acknowledgement* signifying their understanding and compliance with the added responsibilities associated with elevated permissions.	Not Defined	PS-6 AC-6	LMH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
16.6.10	Access agreements shall be reviewed and updated annually.	Not Defined	PS-6	LMH F
16.6.11	The user's immediate supervisor or COR shall be responsible for ensuring that all necessary access agreements are provided to the user, signed, collected, and properly stored.	Not Defined	PS-6	LMH F

3.16.7 External Personnel Security (PS-7)

Specific personnel security requirements including general roles and responsibilities is established by the TSA for third-party providers including, for example, service bureaus, contractors, and other organizations that provide information system development, IT services, outsourced applications, and network and security management.

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
16.7.1	Third party agreements that directly, or indirectly, impact TSA IT assets or information are required and shall include explicit coverage of all relevant personnel security requirements including security roles and responsibilities for third-party personnel. This includes agreements involving processing, accessing, communicating, developing, hosting, securing or managing TSA IT assets, or adding services or products to existing information.	Not Defined	PS-7 PS-1 PS-2	LMH F
16.7.2	Personnel security requirements for third-party personnel (to include contractors) shall be in compliance with all TSA and DHS policy, and not less restrictive. This includes U.S. citizenship requirements.	Not Defined	PS-7 PS-1 PS-3 PS-6	LMH F
16.7.3	CORs and supervisors of third-party personnel (contractors) shall monitor compliance with personnel security requirements.	Not Defined	PS-7 PS-1	LMH F

3.16.8 Personnel Sanctions (PS-8)

Processes addressing sanctions are necessary for personnel failing to comply with established information security policies and procedures. The information security policies contained in TSA MD 1400.3 TSA Information Technology Security Policy, mandate actions and specify expected behavior of individuals who use TSA IT assets in the performance of their required duties.

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
16.8.1	Federal employees found to in violation of the information security-related violations addressed in the *Standards of Ethical Conduct for Employees of the Executive Branch,* shall be subject to disciplinary action for failure to comply with TSA and DHS security policy, whether or not the failure results in criminal prosecution.	3.12.a	PS-8	LMH
16.8.2	TSA employees and contractors in violation of TSA and DHS security policy including, but not limited to, the DHS 4300A *Sensitive Systems Policy,* TSA MD 1400.3 *Information Technology Security Policy*, TSA MD 1100.73-5 *TSA Employee Responsibilities and Conduct Policy,* and signed access agreements may be subject to disciplinary action in compliance with TSA MD 1100.75-3 *Addressing Performance and Conduct Problems,* whether or not the failure results in criminal prosecution.	Not Defined	PS-8	LMH
16.8.3	TSA employees and contractors found in violation TSA and DHS IA policy are subject to having their access to TSA and DHS systems and facilities terminated, whether or not the failure results in criminal prosecution.	3.12.b	PS-8	LMH
16.8.4	All personnel with access to TSA sensitive information, who improperly disclose sensitive information, are subject to criminal and civil penalties and sanctions as applicable by law (to include the Privacy Act, etc.).	3.12.c	PS-8	LMH
16.8.5	In the evaluation of information security incidents, the type of incident (violation or infraction) and the relative severity of the incident shall be determined by the CISO.	Not Defined	PS-8	LMH
16.8.6	Any attempt to circumvent TSA security safeguards shall be subject to possible revocation of access, adverse administration action, and disciplinary action.	Not Defined	PS-8 PL-4	LMH

3.17 Risk Assessment (RA)

TSA shall manage information security risk through an ongoing risk assessment program, including risk definition, risk evaluation, risk avoidance, and/or risk acceptance as required by the Federal Information Security Modernization Act (FISMA).

Specific detailed guidance on general concepts is presented in NIST SP 800-27, *Engineering Principles for IT Security*, along with the principles and practices in NIST SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*. In addition, this control family shall be consistent with the policy presented in NIST SP 800-30, *Risk Management Guide for Information Technology Systems.*

Other Guidance: FIPS 199 Standards for Security Categorization of Federal Information and Information Systems, NIST 800-53 *Recommended Security Controls for Federal Information Systems and Organizations*.

3.17.1 Risk Assessment Policy and Procedures (RA-1)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
17.1.1	Under TSA, the CISO, in coordination with the Chief of Personnel Security Division, Office of Security, under the direction of the Chief Security Officer (CSO) shall assist in the development, dissemination, annual review and update of a formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among TSA entities, and compliance; and formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.	2.1.3	RA-1	LMH
17.1.2	The CISO shall ensure the risk management program and process is established in compliance with Federal guidelines and NIST SP 800-30 *Guide for Conducting Risk Assessments and other applicable Federal guidelines.*.	3.8.a	RA-1	LMH
17.1.3	Reserved			
17.1.4	The CISO shall continuously assess the changing threat environment.	Not Defined	RA-1	LMH
17.1.5	The CIO shall appropriate funding and associated staffing to support ongoing risk management.	Not Defined	RA-1	LMH
17.1.6	The CISO shall establish an independent TSA-wide Security Authorization security control assessment testing program.	3.8.c	RA-1	LMH

3.17.2 Security Categorization (RA-2)

TSA shall categorize information and information systems in compliance with applicable federal laws, E.O.s, directives, policies, regulations, standards, and guidance.

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
17.2.1	An impact level of *high, moderate, low* shall be assigned to each security objective (Confidentiality, Integrity, and Availability) for each information system compliant with FIPS 199 and assign security controls to those systems consistent with FIPS 200.	3.9.a	PM-10 RA-2	LMH F P
17.2.2	Security controls from NIST 800-53, and as tailored in the DHS 4300A PD Attachment M *800-53 Controls,* shall be applied specific to the security objective at the determined impact level.	3.9.a	RA-2	LMH F P
17.2.3	The AO shall review and approve security categorizations for TSA information systems.	Not Defined	RA-2	LMH F P
17.2.4	Privacy Sensitive systems shall be assigned an impact level of moderate or higher for the Confidentiality security objective.	3.14.2.e	RA-2	MH F P
17.2.5	Information systems storing, processing or transmitting SSI shall be assigned an impact level of moderate or higher for the Confidentiality and Integrity security objective.	Not Defined	RA-2	MH F P
17.2.6	All CFO Designated Systems shall be assigned a minimum impact level of “moderate” for Confidentiality, Integrity, and Availability. If warranted by a risk based assessment, the Integrity objective shall be elevated to “high.”	3.15.d	RA-2	MH F P
17.2.7	Reserved			
17.2.8	A SORN shall be required when PII is maintained by TSA in a system of records where information about an individual is retrieved by a unique personal identifier.	3.14.4.a	RA-2	LMH

3.17.3 Risk Assessment (RA-3)

Risk assessment plays an important role in the security control selection process during the application of tailoring guidance for security control baselines and when considering supplementing the tailored baselines with additional security controls or control enhancements. TSA shall assess the risk to information systems, document, and update the risk.

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
17.3.1	The ISSO shall conduct Risk Assessment for the information system, including the likelihood and magnitude of harm from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits.	3.8.b 3.9.g	RA-3 PM-9 PM-10	LMH F
17.3.2	Risk assessments shall be updated when modifications that have the potential to significantly impact risk are made to TSA information systems. Types of modifications include changes to the physical environments, system architecture, interfaces, or user community, and the identification of new threats, vulnerabilities, and other conditions that may impact the security state of the system. Event triggers may require review or update for information systems in ongoing authorization.	3.8.b	RA-3	LMH F
17.3.3	Risk assessment shall take into account the effects of system modifications on the operational risk profile of the system.	3.8.b	RA-3	LMH F
17.3.4	ISSO shall ensure risk assessment results are updated in IACS via a Security Assessment Report (SAR). Per the discretion of the AO, re-assessment of the information systems shall be conducted if warranted by the results of the risk assessment.	Not Defined	RA-3	LMH F
17.3.5	Reserved			
17.3.6	Reserved			
17.3.7	The CISO shall review recommendations for risk determinations and risk acceptability and may recommend changes to the AO and CIO.	3.8.d	RA-3	LMH F
17.3.8	Reserved			
17.3.9	When vulnerability assessment responsibilities encompass other Components beyond TSA, the CISO shall coordinate with the TSA SOC and the DHS ESOC.	5.4.8.e	RA-3	LMH F

3.17.4 Risk Assessment Update (RA-4) (Withdrawn)

This control has been withdrawn.

3.17.5 Vulnerability Scanning (RA-5)

Vulnerabilities are weaknesses that can be exploited. It should be noted that the types of vulnerabilities that shall exist and the methodology needed to determine whether the vulnerabilities are present shall usually vary depending on the nature of the information system and what SELC phase it is in.

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
17.5.1	The CISO shall be responsible for overseeing the TSA-wide vulnerability scanning program.	3.8.e	RA-5	LMH F
17.5.2	Status of vulnerability mitigation shall be reported to CISO for TSA information systems and for other systems processing TSA data.	Not Defined	RA-5	LMH F
17.5.3	The SO shall ensure vulnerability scanning is performed, open vulnerabilities are resolved per the timelines required, patches are installed per the timelines required, and all unnecessary services are eliminated or disabled for the information system per TSA and DHS policy. See also TS-026 *Patch Management* for additional information and guidelines on patching.	4.8.3.d	CM-3 RA-5	LMH F
17.5.4	TSA IT assets shall be reviewed, audited, scanned, and evaluated on a continuous basis to ensure that the system is protected as required by TSA and DHS policy and as described in the SP.	Not Defined	RA-5	LMH F
17.5.5	ISSO shall ensure that vulnerability scans, including scans at the operating system, database, and application levels, are performed monthly for each information system. Additional scans shall be performed as required by the DHS Performance Plan and the CISO.	Not Defined	RA-5	LMH F
17.5.6	Users must log onto the network at least once *every thirty (30) days* for *eight (8) continuous hours* to ensure their IT devices are protected and receive the latest updates and patches. Devices off-line for 30 days or more shall be blocked from connecting to the network and personnel shall need to contact the SPOC to reactivate their IT device and have it patched and updated before it can be reactivated on the network. See TS-026 Patch Management for details.	Not Defined	RA-5 SI-2	LMH F
17.5.7	The TSA SOC shall be notified before any automated vulnerability scans are performed.	5.4.8.f	RA-5 SI-5	LMH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
17.5.8	The results of vulnerability scans shall be analyzed for threats to the information system by the ISSO and/or IAD. The results shall be evaluated to determine the potential risk to the information system integrity and operations.	Not Defined	RA-5	LMH F
17.5.9	The resulting risks found in the vulnerability scans shall be documented and mitigated in compliance with the policy.	Not Defined	RA-5	LMH F
17.5.10	TSA networks shall be subjected to TSA-controlled simulated exploits randomly per discretion of the CISO to determine if monitoring systems are adequate to block exploit attempts.	Not Defined	RA-5	LMH F
17.5.11	Reserved			
17.5.12	The SO shall ensure the review, approval, and sign-off of all custom-developed code prior to deployment into production environments. Code review shall include inspection for security exploits. This authority may be delegated, in writing, to another TSA federal employee. See TS-070 Secure Code and Software Assurance Development guidelines. Note: When writing or editing any software or code, developers shall review secure coding practices such as, but not limited to: The Open Web Application Security Project (OWASP) guide or the SANS Top 20 guidelines. The OWASP and SANS forums serves as an internet community focused on awareness, on improving the security of applications, and can help developers improve on application/code security.	3.6.c	RA-5	LMH F
17.5.13	The SOC shall approve ISVM messages and vulnerability assessment capabilities and distribute to the SO and ISSO all ISVM alert notifications that may affect TSA computer systems. These notifications shall provide a specific timeline for required remediation and reporting based on the severity level of the vulnerability. See TS-026 *Patch Management* for ISVM-related information.	Not Defined	RA-5 SI-5	LMH F
17.5.14	Compliance with the ISVM message and vulnerability remediation shall be accomplished and reported within the specified timeframes in compliance with TS -026 Patch Management.	Not Defined	RA-5 SI-2	LMH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
17.5.15	The SO shall submit a waiver request referencing a newly created POA&M or a related existing POA&M when the requirements of the ISVM messages are unable to be met within the designated compliance timeframe.	Not Defined	RA-5 SI-2	LMH F
17.5.16	The CISO shall report the status of ISVM compliance for TSA information system (including all approved waivers regarding ISVM compliance) in the DHS ESOC Online Portal.	Not Defined	RA-5 SI-2	LMH F
17.5.17	TSA shall employ vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities scanned.	Not Defined	RA-5 (1)	MH F
17.5.18	Automated scanning tools shall be updated at least once a week with current or available configuration files and new vulnerabilities signature files prior to each use.	Not Defined	RA-5 (2)	H F
17.5.19	IAD shall employ vulnerability scanning procedures that demonstrate the breadth and depth of coverage (e.g., information system components scanned and vulnerabilities checked).	Not Defined	RA-5	LMH F
17.5.20	Vulnerability assessors shall attempt to discern what information about the information system is discoverable by adversaries.	Not Defined	RA-5 (4)	H F
17.5.21	Privileged access authorizations shall be assigned to a limited number of authorized individuals for vulnerability scanning activities.	Not Defined	RA-5 (5)	H F
17.5.22	TSA IAD shall monitor official web sites, common industry news sources, and vendor security and patch pages for vulnerability and exploit notifications of commercial vendor product vulnerability and security weakness that may affect TSA computer systems. See TS-026 *Patch Management* for information and guidance on patching.	Not Defined	RA-5	LMH F
17.5.23	Reserved			

3.17.6 Technical Surveillance Countermeasures Survey (RA-6)

Currently, this control does not apply to any control baselines, nor does it apply to Financial systems.

3.17.7 Risk Response (RA-7)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
17.7.1	Place Holder	TBD	TBD	TBD

3.17.8 Privacy Impact Assessment (RA-8)

Currently, this control does not apply to any control baselines, nor does it apply to Financial systems.

3.17.9 Criticality Analysis (RA-9)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
17.9.1	Place Holder	TBD	TBD	TBD

3.18 System and Services Acquisition (SA)

Specific detailed guidance of the information assurance requirements on input, processing, and output control is contained in the TSA Technical Standards TS-002 *Encryption* and TS-028 *Web Applications*.

References may be found in: NIST SPs 800-12, 800-35, 800-53A, 800-60, 800-64 and 800-100. FIPS Publications 199 and 200.

3.18.1 System and Services Acquisition Policy and Procedures (SA-1)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
18.1.1	The CISO shall develop, disseminate, and annually review and update a formal, documented system and services acquisitions policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among TSA entities, and compliance. This will include documented procedures to facilitate the implementation of the system and services acquisitions policy and associated controls.	2.1.3	SA-1 SA-4	LMH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
18.1.2	Throughout TSA, procurement authorities shall ensure that HSAR provisions are fully enforced. Additional HSAR relevant information can be found in **the Information Technology Acquisition Review (ITAR)** link and contains a number of authoritative references. Additional details on "***Information Assurance (IA) Requirements for TSA Acquisitions related Contracts"*** can be found here. The **ITAR site** also addresses Section 508 electronic and information technology (EIT) accessibility standards and requirements. Added information on the **Federal Acquisition Regulation (FAR)** can be found **here**.	3.2.f	SA-1 SA-4	LMH
18.1.3	The CIO shall ensure that IA is considered a requirement for all systems used to input, process, store, display, or transmit sensitive or national security related information at the beginning and early-on in the acquisition process.	Not Defined	SA-1 SA-4 SA-8	LMH
18.1.4	IA shall be achieved through the acquisition and appropriate implementation of evaluated or validated Commercial-off-the-Shelf (COTS), custom code and/or other IA-enabled Information Technology (IT) products early in the procurement cycle. See TS-070 *Secure Code and Software Assurance Development* for additional information.	5.7.a	SA-1 SA-4 SA-8	LMH
18.1.5	The SO shall include information security requirements in their CPIC business cases for the current budget year and for the Future Years Homeland Security Program (FYHSP) for each information system.	3.2.a	PM-3 PM-11 SA-1	LMH
18.1.6	Procurements for services and products involving facility or system access control shall be in compliance with the TSA guidance regarding HSPD-12 implementation.	3.2.g	SA-1	LMH

3.18.2 Allocation of Resources (SA-2)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
18.2.1	The CIO shall ensure a discrete line item for IA in TSA programming and budgeting documentation.	Not Defined	SA-2	LMH
18.2.2	The CIO shall ensure a determination of information security requirements for each system is included in a mission or business process planning.	Not Defined	SA-2	LMH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
18.2.3	The SO shall ensure resources required to protect each information system are documented and allocated as part of the capital planning and investment control process.	3.2.b	SA-2	LMH
18.2.4	The SO shall ensure any request for budget includes adequate funding for the system's information security resources.	3.2	SA-2	LMH
18.2.5	The TSA Office of Acquisitions shall report all legacies and newly acquired IT assets to the CIO for tracking purposes.	Not Defined	SA-2	LMH
18.2.6	All TSA Statements of Work (SOW), Requests for Proposal (RFP), and other contractual requirements documents submitted shall contain specific IT security language as outlined in the HSAR and reviewed and approved by IAD.	Not Defined	SA-2	LMH
18.2.7	The TSA Investment Review Board shall not approve any capital investment in which the information security requirements, including those that address supply chain threats, are not adequately defined and funded.	3.2.c	PM-3 SA-2	LMH

3.18.3 System Development Life Cycle (SA-3)

The purpose of this control is to set policy for information security requirements in acquisition, management, and disposition of IT products and services. The TSA is required by FISMA to incorporate the requirements for information security into the SELC of TSA. The SELC (as complemented by the Agile manual) is a structured approach to system development and refinement and is used from system inception to system disposal. The SELC defines the procedures, approvals, and artifacts required to incorporate system modifications.

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
18.3.1	The CISO shall ensure that system security is integrated into all phases of the SELC.	3.6.a	SA-3	LMH
18.3.2	The CISO shall ensure that security requirements for sensitive information systems are incorporated into life-cycle documentation.	3.6.b	SA-3	LMH
18.3.3	The SO shall follow the practices outlined in the TSA SELC and Agile manual. All documents referencing SELC-related policy are identified in the SELC Guidance Document.	Not Defined	SA-3	LMH
18.3.4	The CISO shall ensure the IAD is sufficiently funded and staffed to support all projects in all phases of the SELC.	Not Defined	SA-3	LMH

3.18.4 Acquisitions Process (SA-4)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
18.4.1	The CISO shall ensure that information security requirements as described within this policy document are included in the acquisition of all TSA systems and services used to input, process, store, display, or transmit sensitive information. This includes: a. Security functional requirements and specifications, b. Security-related documentation requirements, and c. Developmental and evaluation-related assurance requirements.	3.2.e	SA-4	LMH
18.4.2	Solicitation documents such as RFP, SOW, and Contract Vehicles shall include security requirements, evaluation and test procedures, and operational procedures; these shall require a clear response on the part of the proposing entity.	Not Defined	SA-4	LMH
18.4.3	Statements of work and contracts shall include a provision stating that, upon the end of the contract, the contractor shall return all information and information resources provided during the life of the contract and certify that all TSA information has been purged from any contractor-owned system used to process TSA information in compliance with TSA policy.	3.3.d	SA-4	LMH
18.4.4	The requirements in solicitation documents shall allow for the updating of security controls as new threats and vulnerabilities are identified and as new technologies are implemented.	Not Defined	SA-4	LMH
18.4.5	The developer of the information system, system component, or information system service shall provide a description of the functional properties of the security controls to be employed.	3.3.g	SA-4 (1)	MH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
18.4.6	The acquisition of COTS IA and IA-enabled IT products (to be used on systems entering, processing, storing, displaying, or transmitting sensitive information) shall be given a stronger preference to products that have been evaluated and validated, as appropriate, IAW one of the following: a. The International Common Criteria for Information Security Technology Evaluation Mutual Recognition Agreement, b. The NSA and NIST National Information Assurance Partnership (NIAP) Evaluation and Validation Program, or c. The NIST FIPS validation program.	3.2 5.7.b	SA-4 SA-13	LMH
18.4.7	TSA IAD shall conduct reviews to ensure IA security requirements are included within the contract language of any outsourcing contract and are implemented and enforced.	Not Defined	SA-4	LMH
18.4.8	All authorized, cleared and vetted 3rd party vendors or contractors supporting or doing business per agreement with TSA either directly or indirectly shall comply with all applicable IT security or information assurance (IA) policies as stated in DHS 4300A Sensitive Systems Policy Directive, TSA MD 1400.3 IT Security and TSA IA Handbook and supplemental directives. This applies especially in agreements (outside of direct control by TSA personnel) involving: processing, accessing, storing, securing, communicating, developing, hosting, protecting, handling or managing TSA IT assets, services or information in an outside 3rd party facility. Audit logs of 3rd party hosted vendor system(s) shall be made available immediately to authorized TSA personnel upon request. At the end of any contractual agreement between TSA and it's prime, sub or 3rd party vendor, all TSA data shall be secured, protected and returned to TSA, and any data stored on vendor systems shall be purged, removed and certified as such by TSA and the vendor.	3.3	SA-4	LMH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
18.4.9	Acquisition documents shall require that vendors and contractors provide identifying detailed design and implementation documentation of security controls to be employed within the system, information system components, or information system services (including functional interfaces among control components) in sufficient detail to permit analysis and testing of the controls.	3.3	SA-4 (2)	H
18.4.10	The SO shall ensure that vendor or manufacturer documentation describes a high-level design of the information system in terms of subsystems and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing. The SO shall also ensure that documentation is obtained, protected, and made available to authorized government personnel.	3.3.a	SA-4 (2)	MH F
18.4.11	Reserved			
18.4.12	Acquisition documents shall require that information system components be delivered in a secure, documented configuration and the secure configuration shall be the default configuration for any software reinstalls or upgrades.	Not Defined	SA-4	LMH
18.4.13	The SO shall require the developer of the information system, system component, or information system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use.	Not Defined	SA-4 (9)	MH
18.4.14	The SO shall employ information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems. http://www.idmanagement.gov/approved-products-list	Not Defined	SA-4 (10)	LMH

3.18.5 System Documentation (SA-5)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
18.5.1	The CIO shall ensure documentation for the management, operational, and technical oversight of IT security for TSA information systems is established and maintained.	3.7 4.10	SA-5	LMH F
18.5.2	The CISO shall ensure policies and procedures at all levels of TSA business are developed to fully implement TSA IA policy in the form of TSs, SOPs, MDs, or other official TSA documents.	Not Defined	SA-5	LMH F
18.5.3	Reserved			
18.5.4	Reserved			
18.5.5	All IA related security documentation shall be maintained in a change controlled manner.	Not Defined	SA-5	LMH F
18.5.6	Appropriate IA related security documentation shall be made available to TSA users.	4.10.d	SA-5	LMH F
18.5.7	Technical Standard developers shall comply with DHS and TSA configuration management requirements.	4.10	SA-5	LMH F
18.5.8	The SO shall obtain, protect as required, and make available to authorized personnel, the administrator documentation for an information system that describes: a. Secure configuration, installation, and operation of the information system; b. Effective use and maintenance of security features/functions; c. Known vulnerabilities regarding configuration and use of administrative and/or privileged functions.	Not Defined	SA-5	LMH F
18.5.9	The SO shall obtain, protect as required, and make available to authorized personnel, the user documentation for an information system that describes: a. User-accessible security features and functions and how to effectively use those security features and functions; b. Methods for user interaction with the information system, which enables individuals to use the system in a more secure manner; and c. User responsibilities in maintaining the security of the information and information system.	Not Defined	SA-5	LMH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
18.5.10	The SO shall ensure the system documentation, including the SP, is updated annually or whenever system changes occur. Key controls prescribed in Attachment R, Compliance Framework Guide shall be identified in the SP. Such changes include: a. Reassessment of the system occurs; b. New threat information; c. Weaknesses or deficiencies discovered in currently deployed security controls after an information system breach; d. A redefinition of mission priorities or business objectives resulting in a change to the security category of the information system; and e. A change in the information system (to include adding new hardware, software, or firmware; establishing new connections) or the system's environment of operation.	4.10.b 3.15.i	PL-2 SA-5	LMH F
18.5.11	Reserved			
18.5.12	Information system documentation shall include vendor and internally-developed technical documentation, user manuals for purchased items, various plans, operational procedures, etc.	Not Defined	SA-5	LMH F
18.5.13	Reserved			
18.5.14	Both a physical and logical diagram shall be maintained by the SO for the network of the information system for each site and all installations.	Not Defined	SA-5	LMH F
18.5.15	Information system documentation shall be protected according to the highest level of classification or sensitivity of the information system documented.	Not Defined	SA-5	LMH F
18.5.16	Reserved			
18.5.17	Reserved			
18.5.18	A CONOPS document (physical and electronic copies) detailing traffic flows, operations and maintenance procedures, iOS version, IP addresses, etc. shall be maintained by the SO for information system and network operations including all site locations.	Not Defined	SA-5	LMH F
18.5.19	Reserved			

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
18.5.20	Reserved			
18.5.21	Reserved			

3.18.6 Software Usage Restrictions (SA-6) (Withdrawn)

Withdrawn and incorporated into CM-10 and SI-7.

3.18.7 User-Installed Software (SA-7) (Withdrawn)

Withdrawn and incorporated into CM-11 and SI-7.

3.18.8 Security and Privacy Engineering Principles (SA-8)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
18.8.1	The SO shall ensure the application of information system security engineering principles in the specification, design, development, implementation, and modification of the information system.	3.6.a	SA-8	MH
18.8.2	All specific IA issues shall be addressed as a prerequisite for all systems used to: enter, process, store, display, or transmit sensitive information.	3.2.e	SA-8	MH

3.18.9 External System Services (SA-9)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
18.9.1	The CISO shall ensure external information system services comply with TSA information security requirements and employ appropriate security controls in compliance with applicable federal laws and E.O.s as well as TSA and DHS directives, policies, regulations, standards, and guidance. These security controls shall be documented in the ISA.	2.1.3	SA-9	LMH F
18.9.2	The CISO shall ensure external information system services define and document government oversight and user roles and responsibilities with regard to external information system services.	Not Defined	SA-9	LMH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
18.9.3	Requirements for external information system services shall address how sensitive information is to be handled and protected at contractor sites, including any information stored, processed, or transmitted using contractor information systems. Requirements shall also include requirements for personnel background investigations and clearances and facility security.	Not Defined	SA-9	LMH F
18.9.4	No external hardware devices shall be connected to TSA IT assets or networks without prior written approval of the DHS CISO.	4.8.2.b	SA-9	LMH F
18.9.5	Security deficiencies in any outsourced operation shall require creation of a program-level POA&M.	3.3.f	PM-4 SA-9	LMH F
18.9.6	The CISO shall oversee security control compliance by external service providers.	2.1.3	SA-9	LMH F
18.9.7	The CISO shall conduct a TSA risk assessment prior to the acquisition or outsourcing of dedicated information security services.	Not Defined	SA-9 (1)	LMH F
18.9.8	The SO shall ensure that the acquisition or outsourcing of dedicated information security services is approved by the AO.	Not Defined	SA-9 (1)	LMH F
18.9.9	The SO shall ensure that providers of external information system services identify the functions, ports, protocols, and other services required for the use of such services.	Not Defined	SA-9 (2)	MH F

3.18.10 Developer Configuration Management (SA-10)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
18.10.1	The SO shall require that information system developers/integrators: a. Perform configuration management during information system design, development, testing, implementation, and operation; b. Manage and control changes to the information system; c. Implement only TSA-approved changes; d. Document approved changes to the information system; e. Track security flaws and flaw resolution.	Not Defined	SA-10	LMH
18.10.2	The development or procurement of all applications, to include Web applications, shall be performed in a manner that minimizes the potential for introduction of vulnerabilities.	Not Defined	SA-10	MH
18.10.3	Development and/or revision of applications shall follow TSA SELC Guidance as complemented by the Agile manual.	3.9.i	SA-10	MH
18.10.4	All application developers shall document any new environmental security configuration assumptions.	Not Defined	SA-10	MH
18.10.5	When writing or editing any code, developers shall be trained in the use of secure coding practices according to: TS-028 *Web Application Security* and *TS-070 Secure Code and Software Assurance Development.*	Not Defined	SA-10 SA-15 CM-7	MH

3.18.11 Developer Security Testing and Evaluation (SA-11)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
18.11.1	The SO shall ensure the information system developers/integrators, in consultation with associated security personnel (including security engineers): a. Create and implement a security control assessment plan; b. Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and c. Document the results of the security testing & evaluation and flaw remediation processes.	3.3.i	SA-11	MH
18.11.2	All applications shall be reviewed for vulnerabilities in compliance with NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment*	Not Defined	SA-11	MH
18.11.3	For every release (major and minor), developers shall verify that they have reviewed and eliminated or mitigated potential security vulnerabilities.	Not Defined	SA-11	MH
18.11.4	The SO shall ensure developers and integrators remedy vulnerabilities based on recommendations stemming from TSA's application vulnerability scanner.	Not Defined	SA-11	MH

3.18.12 Supply Chain Risk Management (SA-12)

The Transportation Security Administration (TSA) shall protect against supply chain threats by employing due diligence and care.

The measures below shall be used to ensure supply chain protection as part of a comprehensive, defense-in-depth information security strategy. A defense-in-depth approach helps to protect information systems (including the IT products that compose those systems) throughout the SELC: during design and development, manufacturing, packaging, assembly, distribution, system integration, operations, maintenance, and retirement). This is accomplished by the identification, management, and elimination of vulnerabilities at each phase of the life cycle and the use of complementary, mutually reinforcing strategies to mitigate risk.

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
18.12.1	The CISO shall ensure the protection against supply chain threats as part of a comprehensive, defense-in-depth information security strategy.	Not Defined	SA-12	H

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
18.12.2	The SO shall ensure compliance with Supply Chain Risk Management (SCRM) Plans and consider supply chain risks when prioritizing security weaknesses for mitigation.	2.2.8.f	SA-12	H
18.12.3	The SO shall ensure that risk management activities include addressing supply chain risks for the system's current, and all subsequent lifecycle phases, and documenting this activity in the SCRM Plan.	2.2.9.i	SA-12	H
18.12.4	The CFO shall ensure that supply chain risk is identified and evaluated prior to all contract awards, changes, and whenever supply chain threat information indicates the existence of unmitigated system, program, or mission risk to CFO-designated systems.	2.2.9.i	SA-12	H F
18.12.5	The SO shall include requirements for hardware, software assurances and supply chain risk management prior to acquisition of any hardware or software products. Some additional relevant information can be found in **OMB M-17-27 "Assessment and Enforcement of Domestic Preferences In Accordance with Buy American Laws".**	4.8.3.m	SA-12	H
18.12.6	The SO shall ensure that COTS hardware and software products in use by, or being considered for use in, high criticality systems shall be analyzed for supply chain risk prior to acquisition activities that procure new products, upgrade existing products, or that shall integrate these products with commercial services.	4.8.3.n	SA-12	H
18.12.7	The SO shall assign an impact level (high, moderate, low) to each C.I.A. security objective for each TSA information system, and shall apply NIST SP 800-161 controls as tailored specifically to the security objective at the determined impact level.	5.8.a	SA-12	H
18.12.8	The SO shall implement NIST SP 800-161 security controls, using the FIPS Pub 200, *Minimum Security Requirements for Federal Information and Information Systems* methodology, based on the FIPS 199 impact level established for each C.I.A security objective.	5.8.b	SA-12	H
18.12.9	Reserved			

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
18.12.10	The SO shall use the Business Impact Assessments (BIA) to determine the systems level of risk introduced by the IT supply chain and whether the risk from the threat is sufficient to require the implementation of countermeasures.	Not Defined	SA-12	H
18.12.11	The SO shall implement appropriate countermeasures, commensurate with the level of risk determined by the BIA, to protect against supply chain threats.	Not Defined	SA-12	H

3.18.13 Trustworthiness (SA-13)

Withdrawn.

3.18.14 Criticality Analysis (SA-14)

Withdrawn.

3.18.15 Development Process, Standards, and Tools (SA-15)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
18.15.1	The CISO or designated official shall require the developer of the information system, system component, or information system service to follow a documented development process that: a. Explicitly addresses security requirements; b. Identifies the standards and tools used in the development process; c. Documents the specific tool options and tool configurations used in the development process; d. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and e. Reviews the development process, standards, tools, tool options, and configurations to determine if the process, standards, tools, tool options, and configurations selected can satisfy applicable requirements.	Not Defined	SA-15	H

3.18.16 Developer-Provided Training (SA-16)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
18.16.1	The CISO shall ensure that developers of information systems, system components, or information system services provide adequate training to authorized personnel on the correct use and operation of the implemented security functions, controls, and/or mechanisms.	3.11.2	SA-16	H

3.18.17 Developer Security Architecture and Design (SA-17)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
18.17.1	The AO shall ensure that developers of information systems, system components, or information system services produce design specifications and security architecture that: a. Is consistent with and supportive of the organization's security architecture, which is established within and is an integrated part of the organization's enterprise architecture; b. Describes the required security functionality, and the allocation of security controls among physical and logical components; and c. Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection. See TS-070 *Secure Code and Software Assurance Development* for additional information.	Not Defined	SA-17	H

3.18.18 Tamper Resistance and Detection (SA-18)

Currently, this control does not apply to any control baselines, nor does it apply to Privacy or Financial systems.

3.18.19 Component Authenticity (SA-19)

Currently, this control does not apply to any control baselines, nor does it apply to Privacy or Financial systems.

3.18.20 Customized Development of Critical Components (SA-20)

Currently, this control does not apply to any control baselines, nor does it apply to Privacy or Financial systems.

3.18.21 Developer Screening (SA-21)

Currently, this control does not apply to any control baselines, nor does it apply to Privacy or Financial systems.

3.18.22 Unsupported System Components (SA-22)

Currently, this control does not apply to any control baselines, nor does it apply to Privacy or Financial systems.

3.19 System and Communications Protection (SC)

The intent of this control is to develop the required policy and procedures for the effective implementation of security controls and enhancements in the system and communications protection family that are consistent with applicable federal laws, E.O.s, directives, policies, regulations, standards and guidance. Special attention shall be made to the proper acquisition, use, and disposition of Communication Security (COMSEC) equipment, which is an important element of a total defense-in-depth strategy to information security. This area defines the manner in which COMSEC is employed by the TSA to limit information security risks associated with this technology area. Each of the policy areas defined below are derived from DHS 4300B PD and are supported by DHS procedures to implement the actions identified in DHS 4300B. COMSEC Standards are delineated in TS-014 *Communications Security*.

Specific detailed guidance of the information security requirements on system and communication protection is contained in the TSA Technical Standards (TS) TS-002 *Encryption*, TS-008 *End User Assets*, TS-016 *Remote Access*, TS-019 *Network Communications Protocols*, TS-021 *General Telephony*, TS-025 *Virtual Private Networks (VPNs)*, TS-028 *Web Applications*, TS-019 *Network Communications Protocols*, TS-037 *Server Security*, and TS-049 *Information Systems Logging.*

Guidance can be found in: NIST SPs 800-52, 800-56, 800-57, 800-81, 800-77, 800-95, 800-125 and 800-125A (D). FIPS Publications 140, 197, 199 and 200. CNSS Policy 15; NSTISSI No. 7003.

3.19.1 System and Communications Protection Policy and Procedures (SC-1)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
19.1.1	The CISO shall develop, disseminate, and annually review and update a formal, documented system and communication protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among TSA entities, and compliance; and formal, documented procedures to facilitate the implementation of the system and communications protection policy.	2.1.3	RA-1 SC-1	LMH
19.1.2	A formal, documented system and communications protection plan shall be developed and maintained by the SO.	Not Defined	SC-1 SA-5	LMH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
19.1.3	The Communication Security (COMSEC) equipment and associated cryptography tools shall be properly acquired, allocated, managed and returned, or otherwise disposed of by the TSA Central Office of Records.	Not Defined	PL-1 SC-1 MP-6	LMH
19.1.4	All TSA personnel shall practice secure use of voice and data over telephony, video teleconference and fax services.	4.4.2.a 4.5.2.a 4.5.3	SC-1 SC-7 SC-8 SC-9	LMH

3.19.2 Application Partitioning (SC-2)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
19.2.1	Reserved			
19.2.2	Non-administrative end user functionality and user interface services shall be logically separated from system management functionality including administration of servers, databases, workstations, and network devices.	5.4.4.k	SC-2 IA-2	MH F

3.19.3 Security Function Isolation (SC-3)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
19.3.1	The SO shall ensure that the information system isolates security functions from non-security functions.	5.4.4.l	SC-3	H

3.19.4 Information in Shared Systems Resources (SC-4)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
19.4.1	The SO shall ensure information systems prevent unauthorized and unintended information transfer via shared system resources, including encrypted representations of information produced by the actions of a prior user role (or the actions of a process acting on behalf of a prior user role), from being available to any current user role (or current process) that obtains access to a shared system resource (to include registers, main memory, and secondary storage) after that resource has been released back to the information system.	5.4.3.p	SC-4	MH

3.19.5 Denial of Service Protection (SC-5)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
19.5.1	The SO shall ensure information systems protect against or limits the effects of all types of denial of service (DoS) attacks.	4.6.1	SC-5	LMH
19.5.2	The SO shall ensure cost-effective countermeasures to denial of service attacks are identified and established prior to the deployment of a wireless system.	4.6.1 4.6.2.g 4.6.3	SC-5	LMH
19.5.3	TSA and DHS shall identify countermeasures to denial of service attacks and complete a risk based evaluation prior to approving the use of a wireless mobile device and a wireless system.	4.6.1.c	AC-19 PM-9 SC-5	LMH
19.5.4	TSA shall employ applicable monitoring tools to detect indicators of denial of service attacks against information systems, and shall monitor all systems to determine if sufficient resource exists to prevent effective DoS due to malicious attacks originated from internal or external sources.	4.6.1	SC-5	LMH
19.5.5	All TSA PEPs shall provide protection against denial of service attacks.	5.4.4.g	SC-5	LMH

3.19.6 Resource Availability (SC-6)

Currently, this control does not apply to any control baselines, nor does it apply to Privacy or Financial systems.

3.19.7 Boundary Protection (SC-7)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
19.7.1	The CISO shall ensure external connections to TSA systems and critical internal boundaries employ safeguards and monitoring mechanisms to secure and prevent unauthorized access to TSA information.	5.4.4	SC-7	LMH F
19.7.2	All system designs and deployments, including, but not limited to: testing, development, and production systems, within TSA shall incorporate the security trust zones model per policy as identified in TS-071 *Security Trust Zones*.	5.4.3.i	SC-7	LMH F
19.7.3	SYS logs and information transmitted outside of a trusted zone shall be encrypted per policy in compliance with TS-002 *Encryption*.	Not Defined	SC-7	LMH F
19.7.4	SYS logs and information transmitted within a trusted zone that does not communicate outside the trusted zone for any reason is protected and shall not require encryption.	Not Defined	SC-7	LMH F
19.7.5	The SOC shall administer and monitor sensors, security devices and tools, including intrusion detection sensors (IDS) and Intrusion prevention systems (IPS) employed at every ingress and egress point.	5.4.2.c	SI-4 SC-7	LMH F
19.7.6	Allowing network traffic to bypass a layer in the security trust zone architecture by either circumventing a TIC or a Policy Enforcement Point (PEP), such as an un-trusted zone communicating directly and improperly with a trusted zone, without being cleared first by a PEP is prohibited.	Not Defined	SC-4 SC-7	LMH F
19.7.7	Allowing network traffic to pass between one or more systems within the same security trust zone while bypassing PEPs is prohibited, unless approved by the AO.	Not Defined	SC-4 SC-7	LMH F
19.7.8	Communications between non-adjacent zones shall be routed through a network-based application layer firewall incorporating security measures determined by the SO to be commensurate with the highest sensitivity level of the data being processed.	Not Defined	SC-7	LMH F
19.7.9	The CISO shall ensure connections to external networks and information systems occur only through managed interfaces, consisting of boundary protection devices, in compliance with Section 16.7.5 of this handbook.	Not Defined	SC-7	LMH F
19.7.10	The SO shall ensure the information system controls routing of access, both internally and externally, and records and maintains activity logs.	Not Defined	SC-7	LMH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
19.7.11	The Internet shall be treated as an Untrusted Zone.	Not Defined	SC-7	LMH F
19.7.12	Password authentication management of all boundary protection devices, including firewalls, shall be performed.	Not Defined	SC-7	LMH F
19.7.13	Network communication protocols are prohibited between any two or more TSA security zones, unless explicitly permitted within the approved security plan.	Not Defined	SC-7	LMH F
19.7.14	The ISSO shall obtain written approval by the CISO and AO to use protocols, other than for those explicitly permitted prior to use, within the information.	Not Defined	SC-7	LMH F
19.7.15	The CISO shall direct specific Internet sites or categories to be blocked as advised by US-CERT, the TSA SOC, or other DHS-approved sources.	5.4.5.g	SC-7 SC-14	LMH F
19.7.16	Network infrastructure devices, including firewalls, routers, and switches, shall have port security enabled.	Not Defined	SC-7	LMH F
19.7.17	Servers, including pre-production servers and those in laboratory, test, or development environments, shall only operate in controlled areas.	Not Defined	SC-7	LMH F
19.7.18	When the RFID system is connected to a TSA data network, the SO shall ensure that network security controls are implemented to segregate RFID network elements, such as RFID readers, middleware, and databases, from other non-RFID network hosts.	4.6.4.e	CM-6	LMH F
19.7.19	The SO shall ensure physical access to firewalls and PEPs is restricted to authorized personnel.	5.4.4.a	AC-4 SC-7	LMH F
19.7.20	The ISSO shall ensure identification and strong authentication is implemented for the administration of firewalls and PEPs.	5.4.4.b	AC-4 SC-7	LMH F
19.7.21	The ISSO shall conduct quarterly firewall and PEP testing to ensure that the most recent policy changes have been implemented and that all applied policies and controls are operating as intended.	5.4.4.d	SC-7	LMH F
19.7.22	The TSA SOC shall ensure that reports on the status of information security operations and incident reporting are provided to the CISO, as required.	5.4.4.e	SC-7	LMH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
19.7.23	Firewalls and PEPs shall be administered in coordination with DHS security operations capabilities via the DHS ESOC or TSA SOC.	5.4.4.f	SC-7	LMH F
19.7.24	The CISO shall evaluate and approve protocols and services permitted through PEPs.	5.4.4.h	SC-7	LMH F
19.7.25	Any direct connection of TSA systems to the Internet or to extranets shall occur through DHS TIC PEPs.	5.4.5.a	SC-7	LMH F
19.7.26	The TSA Public Switched Telephone Network (PSTN) shall not be connected to DHS OneNet.	5.4.5.a	SC-7	LMH F
19.7.27	Firewalls and PEPs shall be configured to prohibit any protocol or service that is not explicitly: permitted, deny all, permit by exception.	5.4.5.b	SC-7	LMH F
19.7.28	The ISSO shall ensure appropriate network protection mechanisms are deployed to protect TSA email systems, including, but not limited to: a. Firewalls b. Proxies c. Routers d. Switches e. IDS	5.4.6.d	SC-7	LMH F
19.7.29	All host systems shall have all the necessary security detection/protection capabilities and/or tools as identified by IAD. All security protections shall be configured to generate logs to the TSA SOC's Security Information Event Management (SIEM) team for review and analysis.	5.4.2.b 2.1.11	SC-7	LMH F
19.7.30	The SO shall ensure the information system prevents unauthorized access into internal networks.	5.4.4	SC-7	LMH F
19.7.31	The SO shall limit the number of access points to the information system to allow for more comprehensive monitoring of inbound and outbound communications and network traffic.	Not Defined	SC-7 (3)	LMH F
19.7.32	Reserved			
19.7.33	Traffic flow policies shall employ security controls to protect Confidentiality and Integrity of the information being transmitted.	Not Defined	SC-7 (4)	MH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
19.7.34	Reserved			
19.7.35	The SO shall ensure each system at managed interfaces, denies network traffic by default and allows network traffic by exception (deny all, permit by exception).	Not Defined	SC-7 (5)	MH F
19.7.36	Reserve			
19.7.37	The SO shall ensure the system prevents remote devices that have established a connection with the system from communicating outside of that communication path with resources on other external networks.	Not Defined	SC-7 (7)	LMH F
19.7.38	The CISO shall ensure each high system routes TSA traffic to an un-trusted zone through authenticated proxy servers within the managed interfaces of boundary protection devices.	Not Defined	SC-7 (8)	H F
19.7.39	The information system shall fail securely in the event of an operational failure of a boundary protection device.	5.4.4.m	SC-7 (18)	H F
19.7.40	The SO, with the Chief Architect's approval, shall ensure that the network employs boundary protection mechanisms such as routers, firewalls, PEPs, etc., to separate and isolate information system components supporting different IT business functions. Such separation provides for increased protection of individual components and limits unauthorized information flows among system components.	Not Defined	SC-7 (21)	H F

3.19.8 Transmission Confidentiality and Integrity (SC-8)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
19.8.1	The SO shall ensure the information system protects the confidentiality and integrity of transmitted information.	Not Defined	AC-19 SC-8	MH
19.8.2	The SO shall ensure the system employs approved cryptographic mechanisms to recognize changes to information during transmission, unless otherwise protected by alternative physical measures.	Not Defined	SC-8 (1)	MH
19.8.3	The SO shall ensure that systems or applications that require encrypted transmission shall adhere to TS-002 Encryption policy to protect the Confidentiality of transmitted information.	Not Defined	SC-8	MH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
19.8.4	The network shall provide end-to-end encryption of network traffic for all management functions. in compliance with the TS-002 *Encryption*.	Not Defined	SC-8	MH
19.8.5	The ISSO shall ensure that appropriate transmission protections, commensurate with the highest sensitivity of information to be discussed, are in place throughout any video teleconference.	4.5.3.b	SC-8 SC-8	MH
19.8.6	Wireless tactical systems shall implement strong identification, authentication, and encryption.	4.6.3.b	SC-8	MH
19.8.7	The SO shall ensure systems employ cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures.	Not Defined	SC-8 (1)	MH

3.19.9 Transmission Confidentiality (SC-9) (Withdrawn)

Withdrawn and incorporated into SC-8.

3.19.10 Network Disconnect (SC-10)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
19.10.1	The SO shall ensure systems terminate the network connection at the end of the session or after sixty (60) minutes of inactivity, whichever occurs first.	5.2.2.c	SC-10 AC-12	MH

3.19.11 Trusted Path (SC-11)

Currently, this control does not apply to any control baselines, nor does it apply to Privacy or Financial systems.

3.19.12 Cryptographic Key Establishment and Management (SC-12)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
19.12.1	The CISO shall develop, document, and publish all Cryptographic key establishment and management requirements.	2.1.3	SC-12	LMH
19.12.2	Cryptographic key establishment and management shall be implemented in compliance with TS-002 Encryption policy.	Not Defined	SC-12	LMH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
19.12.3	TSA IAD shall implement and maintain a key management plan approved by the DHS PKI Policy Authority for information systems using PKI-based encryption.	4.6.b	IA-5 SC-12	LMH F
19.12.4	The security configuration of LMR subscriber units shall be validated via over-the-air-rekeying (OTAR) or hard rekeying using a crypto-period no longer than 180 days.	4.6.3.f	SC-12	LMH
19.12.5	Information stored on any laptop computer or other mobile computing device shall use proper encryption in compliance with TS-002 *Encryption*, for both data at rest and in motion or in transient. PINs, passwords, tokens, and PIV cards shall not be stored on or with the laptop or other mobile computing device.	4.6.2.s	AC-19 SC-12	LMH
19.12.6	Separate public and private key pairs shall be used for encryption and digital signature (or message authentication codes) by human subscribers.	5.5.3.a	SC-12	LMH
19.12.7	A single public and private key pairs shall be used by a Non-Person Entity (NPE) for encryption and digital signature by device subscribers whenever supported by the protocols native to the type of device.	5.5.3.b	SC-12	LMH
19.12.8	An authorized human sponsor shall represent each application, role, code-signing, and device subscriber when it applies for one or more certificates from a TSA CA.	5.5.3.c	SC-12	LMH
19.12.9	An authorized sponsor shall be required for TSA contractors or other affiliates who apply for one or more certificates from a TSA CA.	5.5.3.d	SC-12	LMH
19.12.10	A mechanism shall be provided for each TSA CA to enable PKI registrars to determine the eligibility of each proposed human, role, application, code signer, or device to receive one or more certificates.	5.5.3.e	SC-12	LMH
19.12.11	A mechanism shall be provided for each TSA CA to enable PKI registrars to determine and verify the identity of the authorized human sponsor for each contractor, affiliate, role, application, code signer, or device.	5.5.3.f	SC-12	LMH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
19.12.12	Human subscribers shall not share private keys and shall be responsible for their security and use. If a human subscriber discloses or shares his or her private key, the subscriber shall be accountable for all transactions signed with the subscriber's private key.	5.5.3.g	SC-12	LMH
19.12.13	Subscriber private keys shall not be used by more than one entity unless explicitly permitted by DHS policy with the exceptions of: - Authorized members of a Group Subscriber, whom may use the Group's private keys; and - Multiple systems or devices in a High availability configuration, which may use a single Key pair providing the Subject Alternative Name (SAN) field within the SSL certificate identifies all of the devices with which the key is to be shared.	5.5.3.i	SC-12	LMH
19.12.14	The SO shall maintain Availability of information in the event of the loss of cryptographic keys by users.	Not Defined	SC-12 (1)	H
19.12.15	Reserved			
19.12.16	Reserved			
19.12.17	Reserved			
19.12.18	Reserved			
19.12.19	Sponsors for non-human subscribers (role, application, code-signing, or device) shall be responsible for the security of and use of the subscriber's private keys. Every sponsor shall read, understand, and sign a "DHS PKI Device Sponsor Agreement" as a pre-condition for sponsoring non-human subscribers.	5.5.3.h	SC-12	LMH
19.12.20	Every human subscriber shall read, understand, and sign a "DHS PKI Human Subscriber Agreement" as a pre-condition for receiving certificates from a TSA CA. These signed agreements shall be maintained by the DHS and TSA PKI Management Authority.	5.5.3.j	SC-12	LMH

3.19.13 Cryptographic Protection (SC-13)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
19.13.1	Reserved			
19.13.2	The Information Owner shall coordinate with the SO to determine the data sensitivity level and corresponding cryptography and encryption requirements.	Not Defined	SC-13	LMH
19.13.3	All offices with encryption applications under TSA authority shall develop encryption plans for all information systems based on information types (to include need to know or Confidential), information status (at rest or in transit), or specific purpose (to include non-repudiation).	5.5.1.b	SC-13	LMH
19.13.4	All TSA-owned USB drives and external hard drives shall use proper encryption in compliance with TS-002 *Encryption*.	4.3.1.d	SC-13	LMH
19.13.5	Wireless mobile devices, such as iOS devices and smart phones, shall implement strong authentication, data encryption, and transmission encryption technologies. Mobile devices shall provide an authentication option for *fingerprint* or a *PIN* and with a security timeout period established.	Not Defined	AC-19 IA-7 SC-8 SC-9 SC-13	LMH
19.13.6	Only cryptographic modules that have been validated as compliance with TS-002 Encryption policy shall be procured.	5.5.1.a	SC-13	LMH
19.13.7	PII and Sensitive PII removed from a TSA or DHS facility on removable media, such as CDs, DVDs, laptops, mobile devices, shall be encrypted, unless the information is being sent to the individual as part of a Privacy Act or Freedom of Information Act (FOIA) request.	3.14.5.a	AU-11 AC-1 SC-13	LMH

3.19.14 Public Access Protections (SC-14) (Withdrawn)

[Withdrawn: Capability provided by AC-2, AC-3, AC-5, SI-3, SI-4, SI-5, SI-7, and SI-10].

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
19.14.1	The SO shall ensure all the information system protects the Integrity and Availability of publicly available information and applications.	Not Defined	SC-14	LMH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
19.14.2	The CISO shall ensure all TSA-owned, operated, controlled, or sponsored public-facing websites, or those public-facing websites affiliated with or operated on the behalf of TSA shall not reveal the following: a.) Employee directories and b.) Employee phone numbers or email addresses.	Not Defined	SC-14	LMH
19.14.3	The CISO shall ensure only TSA main phone numbers that would be listed in any public phone book are disclosed.	Not Defined	SC-14	LMH
19.14.4	The CISO shall ensure that only generic email addresses, such as support@tsa.dhs.gov, shall be displayed.	Not Defined	SC-14	LMH
19.14.5	All TSA-owned, operated, controlled, or sponsored public-facing websites, or those public-facing websites affiliated with or operated on behalf of TSA shall only contain content and links that have been approved for posting by the Content Manager (CM).	Not Defined	SC-14	LMH
19.14.6	The WCM shall review and obtain approval of content and links from the Public Affairs and Privacy Offices prior to posting.	Not Defined	SC-14	LMH
19.14.7	Management of security for Personally Identifiable Information (PII), whether acquired from the public or TSA employees, shall be in compliance with 6 C.F.R., Chapter I, Part 5, Subpart B, and Paragraph 5.31 *Security of System of Records*.	Not Defined	SC-14	LMH
19.14.8	Information systems that provide public information access (to include web servers, etc.) shall have protection mechanisms adequate for protecting the information, any resident applications, and any underlying support systems from attacks.	Not Defined	SC-14	LMH
19.14.9	Proper handling of PII when outside of a TSA Controlled Access Area (CAA) is defined in DHS MD 3700.4**,** *Handling Sensitive Personally Identifiable Information*.	Not Defined	MP-5	LMH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
19.14.10	Prohibited content on Public Facing web sites include but are not limited to: a. All content prohibited under control PL-4 Rules of Behavior b. Sensitive, FOUO, SSI, and PII information, c. Information protected under the Privacy Act, d. Internal program agenda, correspondence, and memos not appropriate for general distribution, e. Procurement-sensitive or proprietary information, and f. Operations Security (OPSEC) and Information Security (INFOSEC) material.	Not Defined	SC-14 PL-4	LMH
19.14.11	Reserved			
19.14.12	The IO shall have website content under their authority.	Not Defined	SC-7 SC-14	LMH
19.14.13	The IO shall clearly note in the footer of each webpage the Terms of Use and whether the page is authorized to display SSI information and/or information protected under the Privacy Act.	Not Defined	SC-7 SC-14	LMH
19.14.14	The IO shall ensure sites are established for only official purposes.	Not Defined	SC-7 SC-14	LMH
19.14.15	The IO shall ensure TSA websites are part of a .gov domain and shall be reflected in the website's address (URL).	Not Defined	SC-7 SC-14	LMH
19.14.16	The SO shall ensure websites are part of a system authorization boundary and documented in an SP.	Not Defined	SC-7 SC-14	LMH
19.14.17	Reserved			
19.14.18	The IO shall ensure websites contain only Official descriptions of TSA missions or entities.	Not Defined	SC-7 SC-14	LMH
19.14.19	The IO shall ensure that applicable TSA or DHS name and official logo appear on all applicable web pages.	Not Defined	SC-7 SC-14	LMH
19.14.20	The IO shall ensure websites comply with TSA and DHS records management policy.	Not Defined	SC-7 SC-14	LMH
19.14.21	Website visitors shall be notified when taken to a non-federal government site or when they are being transferred from a secure website to a non-secure website.	Not Defined	SC-7 SC-14	LMH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
19.14.22	The ISSO shall ensure that content and privacy policies are displayed when linking to a non-federal site.	Not Defined	SC-7 SC-14	LMH
19.14.23	The ISSO shall ensure that systems accessible to the public shall provide both a security and privacy statement at every entry point.	5.2.3.b	AC-8 SC-7 SC-14	LMH

3.19.15 Collaborative Computing Devices and Applications (SC-15)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
19.15.1	Implementation of collaborative computing, to include network whiteboards, cameras, and microphones, shall require specific approval of the CISO.	Not Defined	SC-15	LMH
19.15.2	The CISO shall ensure each system provides physical disconnect of collaborative computing devices in a manner that supports ease of use.	Not Defined	SC-15	LMH

3.19.16 Transmission of Security and Privacy Attributes (SC-16)

Currently, this control does not apply to any control baselines, nor does it apply to Privacy or Financial systems.

3.19.17 Public Key Infrastructure Certificates (SC-17)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
19.17.1	Processes for creating, maintaining, issuing, revoking, and otherwise managing PKI certificates shall be implemented in compliance with DHS policy.	Not Defined	SC-17	MH
19.17.2	Detailed technical requirements for PKI infrastructure operations and management shall be established according to TS-022 *Public Key Infrastructure*.	Not Defined	SC-17	MH
19.17.3	The TSA CA shall follow the requirements and process for becoming a DHS Component Internal Use NPE Root in compliance with the DHS X.509 Internal Use NPE Certificate Policy.	5.5.2.g	SC-17	MH
19.17.4	The CA shall ensure Single Internal Use NPE CA are self-signed and function as its own trust anchor.	5.5.2.h	SC-17	MH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
19.17.5	The TSA Internal Use NPE CAs shall operate under a Certification Practice Statement (CPS) in the form of a DHS NPE Configuration and Operation Practices Guide (COPG). The COPG shall comply with the DHS X.509 Internal Use NPE Certificate Policy and shall be approved by the DHS PKIPA.	5.5.2.i	SC-17	MH
19.17.6	The Internal Use NPE CA shall undergo regular PKI compliance assessments as required by the DHS X.509 Internal Use NPE Certificate Policy. The assessment findings, report, and POA&Ms shall be archived and provided to the DHS PKIPA and DHS PKIMA in compliance with the DHS X.509 Internal Use NPE Certificate Policy.	5.5.2.k 5.5.2.l	SC-17	MH
19.17.7	All operational PKI facilities shall be established in compliance with DHS X.509 Internal Use NPE Certificate Policy physical security requirements based on the CA's assurance level and its intended use. Location and protection of the CA shall be determined by its level of assurance.	5.5.2.m	SC-17	MH
19.17.8	The TSA CA shall ensure the continuity of PKI operations shall provide at least the same level of PKI Services availability as the individual and composite availability requirements of the systems and data protected by the certificates.	5.5.2.m	SC-17	MH
19.17.9	The Internal Use NPE CAs shall only issue certificates to TSA internal hardware devices and systems, which are specifically permitted by the DHS X.509 Internal Use NPE Certificate Policy.	5.5.2.n	SC-17	MH
19.17.10	Certificates issued by the TSA Internal Use NPE CAs shall not be used to encrypt sensitive data.	5.5.2.r	SC-17	MH
19.17.11	The TSA CA shall manage the content of installed product's trust stores, including: a. Leveraging automated management, such as with Microsoft Group Policy Objects (GPOs) b. Removing all certificates that have passed their expiration date c. Removing all certificates that are no longer trusted d. Removing all certificates that are no longer required	5.5.2.u	SC-17	MH
19.17.12	The CISO is responsible for management oversight of the DHS Pre-certification Authority (PCA) RA activities and personnel within TSA.	5.5.2.e	SC-17	MH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
19.17.13	DHS FPKI: For all external-facing DHS web services, compliance with OMB Memorandum 15-13 and 17-06 (use of HTTPS and HSTS) is mandatory. Federally issued certificates will not be practical for web services whose users may not always be expected to trust the issuing federal certificate authority. These web services will likely require the use of a certificate from a publicly trusted (commercial) certificate authority. These should be obtained after approval by the DHS CISO. DHS CA4-issued certificates may be practical for web services whose users can be consistently expected to trust the issuing DHS certificate authority or the federal CA trust anchor it chains to.	5.5.2.t	SC-17	MH

3.19.18 Mobile Code (SC-18)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
19.18.1	The CISO shall approve acceptable and fully tested mobile code technologies and establish usage restrictions and implementation guidance for acceptable mobile code.	4.5 4.6 5.4.5.c	SC-18	MH
19.18.2	SPs shall promulgate the provisions, procedures, and restrictions for using wireless mobile devices to download mobile code in an approved manner.	4.6.2.e	SC-18 PL-2	MH F

3.19.19 Voice over Internet Protocol (SC-19)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
19.19.1	VoIP systems shall have purpose, justification, and residual risks clearly identified in writing prior to Authorization.	4.5.4.a	SC-19 PM-9	MH
19.19.2	The SO shall ensure voice over data network implementations shall have sufficient redundancy to ensure network outages do not result in the loss of both voice and data communications.	4.5.4.b	SC-19	MH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
19.19.3	All TSA related telecommunications solutions, or modification to approved solutions, shall be reviewed and approved by the AO to ensure proper implementation of appropriate identification and authentication controls, audit logging, and Integrity controls on every element of their Voice-over-IP (VoIP) networks.	4.5.4.c	SC-19	MH
19.19.4	The SO shall ensure that physical access to voice over data network elements is restricted to authorized personnel.	4.5.4.d	SC-19	MH
19.19.5	The ISSO shall ensure that VoIP servers are dedicated to only applications required for VoIP operations (see *DISA Internet Protocol (IP) and Voice over Internet Protocol (VoIP) Security Technical Implementation Guide (STIG) for VoIP*).	Not Defined	SC-19	MH
19.19.6	Prior to implementing voice over data network technology, risk assessments and security testing shall be conducted and business justification for their use shall be provided to the TSA CISO.	4.5.4.a	SC-19	MH
19.19.7	Approved wireless headsets shall be permitted for use with VoIP telephones and shall be simple, plug-and-play units with no software or drivers required and with no persistent memory.	4.6.1.g Attch Q1	AC-18 SC-40	MH

3.19.20 Secure Name/Address Resolution Service (Authoritative Source) (SC-20)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
19.20.1	The SO shall ensure systems provide additional data origin and Integrity artifacts along with the authoritative data the system returns in response to name and address resolution queries.	Not Defined	SC-20	LMH
19.20.2	Domain Name System (DNS) Security Extensions (DNSSEC) shall be implemented in TSA systems.	5.4.3.j	SC-20	LMH
19.20.3	All TSA systems connected to OneNet and operating at moderate or high level shall utilize secure Name/Address resolution service provided by DHS OneNet.	5.4.3.k	SC-20	MH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
19.20.4	DNS security controls shall be consistent with, and referenced from, OMB Memorandum 08-23 and NIST SP 800-81 *Secure Domain Name System (DNS) Deployment Guide*.	Not Defined	SC-20	LMH
19.20.5	The SO shall ensure the information system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces and (if the child supports secure resolution services) enable verification of a chain of trust among parent and child domains.	Not Defined	SC-20	LMH

3.19.21 Secure Name/Address Resolution Service (Recursive or Caching Resolver) (SC-21)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
19.21.1	TSA information systems shall perform data origin authentication and data Integrity verification on the name and address resolution responses the system receives from authoritative sources when requested by client systems.	5.4	SC-21	LMH

3.19.22 Architecture and Provisioning for Name/Address Resolution Service (SC-22)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
19.22.1	TSA information systems that collectively provide name and address resolution service for TSA shall be fault-tolerant and implement internal and external role separation.	Not Defined	SC-22	LMH

3.19.23 Session Authenticity (SC-23)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
19.23.1	The SO shall ensure information systems provide mechanisms to protect the authenticity of communications sessions.	Not Defined	SC-23	MH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
19.23.2	The SO shall ensure each system validates session identifiers upon user logout or other session termination.	5.4.3.o	SC-23	MH

3.19.24 Fail in Known State (SC-24)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
19.24.1	The SO shall ensure systems fail to a known state in the event of a failure of the information system or a component of the system.	Not Defined	SC-24	H
19.24.2	The SO shall ensure that system logs, system backup data, and system application data is preserved if the information system fails to a known state.	Not Defined	SC-24	H

3.19.25 Thin Nodes (SC-25)

Currently, this control does not apply to any control baselines, nor does it apply to Privacy or Financial systems.

3.19.26 Honeypots (SC-26)

Currently, this control does not apply to any control baselines, nor does it apply to Privacy or Financial systems.

3.19.27 Platform--Independent Applications (SC-27)

Currently, this control does not apply to any control baselines, nor does it apply to Privacy or Financial systems.

3.19.28 Protection of Information at Rest (SC-28)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
19.28.1	The SO shall protect the Confidentiality and Integrity of information at rest through the use of encryption and hashing unless otherwise protected by alternative physical measures (such as the device being contained within an Information Security Restricted Area [ISRA]). This includes data at rest in cloud and virtual environments. See TS-072 *Cloud Computing and Virtualization* and TS-049 *Information System Audit Logging* for additional information.	4.8.2 5.2.g	SC-28	MH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
19.28.2	The ISSO shall ensure approved GFE removable media is protected by access controls employing applicable cryptographic mechanisms. in compliance with TS-002 Encryption. See this link for additional information on **TSA-approved devices** and IT products.	4.6.2.s	SC-28	MH

3.19.29 Heterogeneity (SC-29)

Currently, this control does not apply to any control baselines, nor does it apply to Privacy or Financial systems.

3.19.30 Concealment and Misdirection (SC-30)

Currently, this control does not apply to any control baselines, nor does it apply to Privacy or Financial systems.

3.19.31 Covert Channel Analysis (SC-31)

Currently, this control does not apply to any control baselines, nor does it apply to Privacy or Financial systems.

3.19.32 System Partitioning (SC-32)

Currently, this control does not apply to any control baselines, nor does it apply to Privacy or Financial systems.

3.19.33 Transmission Preparation Integrity (SC-33) (Withdrawn)

[Withdrawn and incorporated into SC-8]

3.19.34 Non-Modifiable Executable Programs (SC-34)

Currently, this control does not apply to any control baselines, nor does it apply to Privacy or Financial systems

3.19.35 Honeyclients (SC-35)

Currently, this control does not apply to any control baselines, nor does it apply to Privacy or Financial systems.

3.19.36 Distributed Processing and Storage (SC-36)

Currently, this control does not apply to any control baselines, nor does it apply to Privacy or Financial systems.

3.19.37 Out-of-Band Channels (SC-37)

Currently, this control does not apply to any control baselines, nor does it apply to Privacy or Financial systems.

3.19.38 Operations Security (SC-38)

Currently, this control does not apply to any control baselines, nor does it apply to Privacy or Financial systems.

3.19.39 Process Isolation (SC-39)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
19.39.1	The SO shall ensure that information systems maintain a separate execution domain for each executing process.	Not Defined	SC-39	LMH

3.19.40 Wireless Link Protection (SC-40)

Currently, this control does not apply to any control baselines, nor does it apply to Privacy or Financial systems.

3.19.41 Port and I/O Device Access (SC-41)

Currently, this control does not apply to any control baselines, nor does it apply to Privacy or Financial systems.

3.19.42 Sensor Capability and Data (SC-42)

Currently, this control does not apply to any control baselines, nor does it apply to Privacy or Financial systems.

3.19.43 Usage Restrictions (SC-43)

Currently, this control does not apply to any control baselines, nor does it apply to Privacy or Financial systems.

3.19.44 Detonation Chambers (SC-44)

Currently, this control does not apply to any control baselines, nor does it apply to Privacy or Financial systems.

3.20 System and Information Integrity (SI)

Information integrity control may vary according to the security level of the data. Data Integrity control measures include data access control, data segregation, data aggregation control, data fingerprinting, proper and routine backup actions, and data disaster planning and recovery. The measures for ensuring data Integrity range from access protection to loss recovery, to operational information, and backup and restoration.

Specific detailed guidance of the information security requirements on input, processing, and output control is contained in the TSA Technical Standards (TS) TS-002 *Encryption*, TS-006 *Network Intrusion Detection and Prevention Systems*, TS-007 *Host Intrusion Detection Systems*, TS-008 *End User Assets*, TS-019 *Network Communications Protocols*, TS-028 *Web Applications*, TS-46 *IT Media Sanitization and Disposition*, TS-049 *Information Systems Logging*.

Guidance may be found in: NIST Special Publications 800-12, 800-40, 800-45, 800-61, 800-83, 800-92, 800-94, 800-100. DHS 4300 PD Attachment F *Incident Response.*

3.20.1 System and Information Integrity Policy and Procedures (SI-1)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
20.1.1	The CISO shall ensure the development, dissemination, and annual review and update of a formal, documented system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among TSA entities, and compliance. The CISO shall also ensure a formal, documented procedure to facilitate the implementation of system and information of Integrity policy and associated controls that provide protection from unauthorized alteration, loss, unavailability, or disclosure of information.	2.1.3	SI-1	LMH
20.1.2	The SO shall ensure the implementation of system and information Integrity requirements.	5.1.a	SI-1	LMH
20.1.3	All TSA information system users shall be responsible for their aspects of data Integrity protection and for adhering to these requirements.	2.2.11.a Attch G	SI-1	LMH

3.20.2 Flaw Remediation (SI-2)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
20.2.1	Information system flaws or deficiencies shall be identified, resolved, and formally documented in a POA&M.	3.7.b	SI-2	LMH F
20.2.2	All system patches shall require configuration control approval and lab testing prior to controlled change release unless a risk requires immediate intervention. See TS-026 *Patch Management* for additional information.	4.8.3.d	SI-2	LMH F
20.2.3	Approval for immediate intervention (e.g., emergency change) shall require the approval of the AO, SCCB co-chairs, and the SO.	Not Defined	SI-2	LMH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
20.2.4	Information system patches shall be installed in compliance with configuration management plans and within the timeframe or direction provided by the IAD Risk Management Team. in compliance with TS-026 *Patch Management.*	3.7.c 5.6.b	SI-2	LMH F
20.2.5	All applicable vendor recommendations for security patches shall be applied to the systems using automated mechanisms after testing and approval in compliance with Policy ID 17.2.2 of this Handbook.	4.8.3.d	SI-2 (1)	H F
20.2.6	Systems shall be in compliance with TS-026 Patch Management policy.	4.8.3.d	SI-2(2)	MH F

3.20.3 Malicious Code Protection (SI-3)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
20.3.1	The CISO shall establish and enforce TSA-wide malware and phishing protection control policies. For additional information on anti-phishing and social engineering type testing, see the **Policy Outreach link, a**s well as **social engineering** policy.	3.16 5.6.a 5.4.6.g	SI-3	LMH
20.3.2	The SO shall develop and enforce procedures for implementing approved malicious code protection mechanisms to operate at information system entry and exit points, workstations, servers, and mobile computing devices on the network to detect, isolate, and/or eradicate malicious code. See also TS-070 Secure Code and Software Assurance Development policy. for additional information and guidance.	5.6.c	SI-3 AC-20	LMH
20.3.3	The ISSO shall update malicious code protection mechanisms (including signature definitions) whenever new releases are available.	5.6.c	SI-3	LMH
20.3.4	The ISSO shall configure malicious code protection mechanisms to perform periodic scans of the information system at least monthly and real-time scans of files from external sources as the files are downloaded, opened, or executed.	5.6.c	SI-3	LMH
20.3.5	The ISSO shall ensure the malicious code is blocked or quarantined once detected.	5.6.c	SI-3	LMH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
20.3.6	Reserved			
20.3.7	The ISSO shall ensure TSA assets have anti-virus software that is properly configured (using directory-based group policy enforcement) to check all files, internet downloads, and email attachments.	3.7 4.6.1.d 5.4.6.d 5.6.b	SI-3	LMH
20.3.8	Reserved			
20.3.9	The ISSO shall identify and address the receipt of false positives during malicious code detection and eradication and document resulting potential impact on the Availability of the information system.	2.1.10	SI-3	LMH
20.3.10	The SO shall ensure that the information security program adopt a defense-in-depth strategy that integrates firewalls, screening routers, wireless IDSs, antivirus software, encryption, strong authentication, and cryptographic key management to ensure information security solutions and secure connections to external interfaces are consistently enforced.	4.6.1.d	SI-3	LMH
20.3.11	Wireless mobile devices shall be operated only when current TSA TRM-approved (i.e., TechSP) versions of antivirus software and software patches are installed.	4.6.2.f	SI-3 SC-18	LMH
20.3.12	Malicious code protection mechanisms (to include antivirus software) shall be centrally managed by the CISO.	Not Defined	SI-3 (1)	MH
20.3.13	The ISSO shall ensure the information system is configured to automatically update malicious code protection mechanisms (including signature definitions).	Not Defined	SI-3 (2)	MH
20.3.14	Reserved			

3.20.4 Information System Monitoring (SI-4)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
20.4.1	Information systems shall be continuously monitored by the SOC or provide an internal continuous monitoring capability. Separately managed support systems shall, at a minimum, send their monitored security audit information (to include IDS events, local security logs, etc.) to the TSA SOC in compliance with TS-006 Network Intrusion Detection and Prevention Systems (NIDS) and TS-007 Host Intrusion Detection Systems (HIDS) policies..	4.9.1.k 5.4.2.a	SI-4	LMH
20.4.2	The TSA SOCs shall administer and monitor TSA IDS/IPS sensors and security devices.	5.4.2.c	SI-4	LMH
20.4.3	The ISSO shall ensure monitoring of events on information systems in compliance with TS-049 Information Systems Logging and relevant TSs specific to the devices in operation for the information system.	4.9.1.k 5.4.2.a	SI-4	LMH
20.4.4	The ISSO shall implement monitoring devices to detect unauthorized use and collect data to be used in risk mitigation planning.	4.9.1.k 5.4.2	SI-4	LMH
20.4.5	Threat levels and notifications shall be established when there is an indication of increased risk to TSA operations, assets, or both.	4.9.1.k 5.4.2	SI-4	LMH
20.4.6	The SO, in conjunction with the CISO and AO, shall obtain legal opinion with regard to information system monitoring activities in compliance with applicable federal laws, E.O.s, directives, policies, or regulations.	4.9.1.k	SI-4	LMH
20.4.7	A revised sensor or tool knowledge base shall be distributed to all monitoring locations within twenty-four (24) hours of update.	4.9.1.k 5.4	SI-4	LMH
20.4.8	All sensor or tool tuning shall require IAD approval and be consistently applied throughout TSA IT assets.	4.9.1.k 5.4.2	SI-4	LMH
20.4.9	Monitoring shall be performed on a schedule that ensures that all TSA IT assets are monitored on a regular basis.	4.9.1.k 5.4	SI-4	LMH
20.4.10	The log files of all IA system components shall be monitored and reviewed to detect any abnormal activity.	4.9.1.k	SI-4	LMH
20.4.11	All NIDS manager applications, firewalls, VPN managers, and HIDS managers shall be continually monitored and reviewed for abnormal activity.	4.9.1.k 5.4	SI-4	LMH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
20.4.12	Alerts of Interest (AOI) shall be evaluated as indicators of more significant activities and IA analysts shall review AOI data within one hour of occurrence.	4.9.1.k 5.4	SI-4	LMH
20.4.13	All AOIs shall be dispatched within 24 hours as one of the following: a. False positive – Appearance of a threat data in a non-threat situation (candidate for sensor tuning), b. False negative – Absence of expected data in a threat situation (candidate for sensor tuning), c. Distraction – Attempt to deceive in a threat or non-threat situation (candidate for knowledge base), d. Annoyance – Amateur attempt to gain system access (candidate for knowledge base), and e. Potential threat – Elevated to Event of Interest (EOI)	2.1.10 2.1.11 4.9.1.d 5.4	SI-4	LMH
20.4.14	EOI shall be evaluated as indicators of more significant activities and IA analysts shall review EOI within 1 hour of occurrence.	4.9.1.k 5.4	SI-4 PL-1 PM-1	LMH
20.4.15	All EOI shall be dispatched and documented within 8 hours as one of the defined threat types defined in DHS 4300A PD Appendix F *Incident Response* and may be elevated as a Potential Incident (PI) by direction of the ESOC Manager.	4.9.1.k Attch F	SI-4 PL-1 PM-1	LMH
20.4.16	All newly detected, previously unknown, or abnormal activity shall be evaluated for inclusion into the sensor or tool knowledge base.	2.2.2.a 4.9.1.k	SI-4	LMH
20.4.17	Revisions to, or tuning of, a sensor, tool, or respective knowledge base shall require the approval of the IAD.	Not Defined	SI-4	LMH
20.4.18	A revised sensor or tool knowledge base shall be distributed to all monitoring locations within 24 hours of update.	Not Defined	SI-4	LMH
20.4.19	Reserved			
20.4.20	The information system shall include automated tools to support near real-time analysis of events to include, but not limited to: NIDS, HIPS, and Firewalls.	5.4.2.a 5.4.2.d	SI-4 (2)	MH
20.4.21	Reserved			

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
20.4.22	The information system shall be configured to monitor inbound and outbound communications for unusual or unauthorized activities or conditions.	5.4.2	SI-4 (4)	MH
20.4.23	The information system shall provide near real-time alerts to the ISSO, SO, and/or SOC when indications of compromise or potential compromise occur.	5.4.2.a 5.4.2.d	SI-4 (5)	MH
20.4.24	Reserved			

3.20.5 Security Alerts, Advisories, and Directives (SI-5)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
20.5.1	IAD shall establish a robust vulnerability management capability using Information Security Vulnerability Management (ISVM) messages and supporting data received in information system security alerts, advisories, and directives from DHS and US-CERT on an on-going basis.	4.9.h	SI-5	LMH F
20.5.2	The TSA CISO shall ensure that 1) the DHS CISO is kept apprised of all pertinent matters involving the security of information systems, and 2) security-related decisions and information are distributed to the ISSOs and other appropriate persons.	4.9.i	SI-5	LMH F
20.5.3	The SOC shall generate internal security alerts, advisories, and directives (as deemed necessary) and disseminate them to TSA senior management and the DHS ESOC.	5.4.8.g	SI-5	LMH F
20.5.4	The IAD Risk Management Team shall implement security procedures, as referenced in TS-026 *Patch Management*, in compliance with established time frames and shall advise DHS of the extent of noncompliance.	4.9.2.a	SI-5	LMH F
20.5.5	The CISO, or a designated representative, shall acknowledge receipt of ISVM messages.	5.4.8.c	SI-5	LMH F
20.5.6	The SOC shall report compliance with the ISVM message within the specified timeframe. When unable to meet the designated compliance timeframe, the SOC shall submit documentation of a waiver request via the DHS ESOC Online Portal (https://eoconline.dhs.gov)	5.4.8.d	SI-5	LMH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
20.5.7	The SO shall report the security alert and advisory status of the information system to the AO, TSA CISO, and DHS CISO upon request and on a periodic basis.	5.4.8.g	SI-5	LMH F
20.5.8	All TSA information systems' security related alarm and event information shall be aggregated at a central location.	Not Defined	SI-5	LMH F
20.5.9	IAD shall use automated mechanisms to make security alert and advisory information available throughout TSA as needed.	Not Defined	SI-5 (1)	H F

3.20.6 Security and Privacy Function Verification (SI-6)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
20.6.1	The CISO shall establish policy and procedures to verify the correct operation of security functions at least annually.	5.4.4.n	SI-6	LMH
20.6.2	Security functions shall be tested in transitional states such as during system startup, restart, shutdown, and abort.	5.4.4.n	SI-6	H
20.6.3	The ISSO and SO shall be notified when security functions fail for appropriate system actions.	5.4.4.n	SI-6	H

3.20.7 Software, Firmware, and Information Integrity (SI-7)

The operation and use of TSA IT assets is bound by a set of information security policies that addresses the protection of information and system resources. Data classification and segregation of access are critical elements of overall system defense. These elements define the level of sensitivity of data, ensuring that only those personnel with both a need to know and clearance for each specific set of information has access to that information.

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
20.7.1	The SO shall implement and document a defense-in-depth approach to IA that detects unauthorized changes to software and information.	4.8.4	SI-7	LMH
20.7.2	Data classification and segregation of access shall be implemented, including requirements that personnel have a need to know with applicable clearance.	Not Defined	SI-7	LMH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
20.7.3	The detection of unauthorized, security-relevant configuration changes shall be implemented into the TSA IR capability to ensure that such detected events are tracked, monitored, corrected, and available for historical purposes.	3.7	SI-7	LMH
20.7.4	The ISSO shall reassess the Integrity of software and information by performing hashing verifications (Integrity scans) of the information system.	4.8.4	SI-7 (1)	MH
20.7.5	The ISSO shall employ automated tools that provide notification to designated individuals upon discovering discrepancies during Integrity verification.	4.8.4	SI-7 (2)	H
20.7.6	The SO shall ensure that the information system detects and automatically provides an alert when integrity violations occur.	4.8.3.h	SI-7 (5)	H
20.7.7	The SO shall ensure that the system has the capability to initiate an incident response following a detection of unauthorized changes.	4.8.3.f	SI-7 (7)	MH
20.7.8	The SO shall ensure that its systems prohibit the use of binary or machine-executable code from sources or source code with limited or no warranty and without the provision of source code (e.g., unsupported open source software).	4.8.3.f	SI-7 (14)	H
20.7.9	The CISO shall approve the tested and approved applications list including commercial software.	2.1.2 2.1.4 4.8.3.a	SI-7	LMH
20.7.10	All commercial and customized software shall be approved for release by the SCCB prior to introduction into the information system.	4.8.3.m	SI-7	LMH
20.7.11	Reserved			

3.20.8 Spam Protection (SI-8)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
20.8.1	The SO shall employ spam protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web access, or other common means.	5.4.6	SI-8	MH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
20.8.2	Spam protection mechanisms (including signature definitions) shall be updated via automated mechanisms when new releases are available in compliance with TSA configuration management policy and procedures.	5.4.6	SI-8	MH
20.8.3	The ISSO shall ensure email content within TSA email systems is secured and filtered.	5.4.6.c	AC-4 SI-8	MH
20.8.4	The ISSO shall centrally manage spam protection mechanisms.	5.4.6	SI-8 (1)	MH
20.8.5	The SO shall ensure the information system automatically updates spam protection mechanisms.	5.4.6	SI-8 (2)	MH

3.20.9 Information Input Restrictions (SI-9) (Withdrawn)

Withdrawn and incorporated into AC-2, AC-3, AC-5, and AC-6.

3.20.10 Information Input Validation (SI-10)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
20.10.1	TSA information systems shall check the validity of information inputs by validating syntax and semantics of information system inputs (to include character set, length, numerical range, and acceptable values) that are in place to verify that inputs match specified definitions for format and content.	5.7.f	SI-10	MH
20.10.2	Inputs passed to interpreters shall be prescreened to prevent the content from being unintentionally interpreted as commands.	5.7.f	SI-10	MH

3.20.11 Error Handling (SI-11)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
20.11.1	TSA information systems shall identify potentially security-relevant error conditions and generate error messages that provide information necessary for corrective actions.	5.7.h	SI-11	MH
20.11.2	TSA information systems shall not reveal information that could be used in a structured attack in error logs.	5.7.i	SI-11	MH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
20.11.3	TSA information systems shall not reveal information in administrative or error messages that could be exploited by adversaries.	5.7.i	SI-11	MH

3.20.12 Information Management and Retention (SI-12)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
20.12.1	The CISO shall establish policy and procedures that ensure output data, processing actions, and resultant outputs are protected and controlled according to FIPS 199 impact level.	4.3.4	SI-12	LMH
20.12.2	All individuals within the TSA shall perform their duties in a manner that protects data in compliance with TSA data control, disclosure, and sanitization policies including DHS MD 11042.1 *Safeguarding Sensitive but Unclassified (For Official Use Only) Information* and TS-046 *IT Media Sanitization and Disposition.*	4.3.4.a 4.3.4.b	SI-12	LMH
20.12.3	TSA information system users shall ensure that any sensitive information, particularly sensitive privacy data, is attached as an encrypted file and the recipient has a need to know when sending email to an address outside of the dhs.gov domain.	5.4.6.k	SI-12	LMH
20.12.4	TSA information system users shall ensure the proper protection of printed output. Printing of sensitive documents shall occur only when a trusted person is attending the printer.	4.3.1.g	SI-12	LMH

3.20.13 Predictable Failure Prevention (SI-13)

Currently, this control does not apply to any control baselines, nor does it apply to Privacy or Financial systems.

3.20.14 Non-Persistence (SI-14)

Currently, this control does not apply to any control baselines, nor does it apply to Privacy or Financial systems.

3.20.15 Information Output Filtering (SI-15)

Currently, this control does not apply to any control baselines, nor does it apply to Privacy or Financial systems.

3.20.16 Memory Protection (SI-16)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
17.16.1	The SO shall ensure that information system implements safeguards to protect its memory from unauthorized code execution.	Not Defined	SI-16	MH

3.20.17 Fail-Safe Procedures (SI-17)

Currently, this control does not apply to any control baselines, nor does it apply to Privacy or Financial systems.

3.20.18 Information Disposal (SI-18)

Currently, this control does not apply to any control baselines, nor does it apply to Financial systems.

3.20.19 Data Quality Operations (SI-19)

Currently, this control does not apply to any control baselines, nor does it apply to Financial systems.

3.20.20 De-Identification (SI-20)

Currently, this control does not apply to any control baselines, nor does it apply to Financial systems.

3.21 Program Management (PM)

The program management controls complement the security controls for an information system by focusing on the TSA-wide information security requirements that are independent of any particular information system and are essential for managing information security programs.

Other guidance: OMB Memorandum 02-01; HSPD 7; NIST Special Publications 800-37, 800-39, 800-39, 800-55, 800-60, 800-65; FIPS Publication 199.

3.21.1 Information Security Program Plan (PM-1)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
21.1.1	The CISO shall develop, disseminate, and annually review and update a formal, documented information security program plan that addresses purpose, scope, roles, responsibilities, management commitment, coordination among TSA entities, and compliance; and formal, documented procedures to facilitate the implementation of the information security program plan policy and associated controls.	2.1.3	PM-1 PM-2	LMH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
21.1.2	The information security program plan shall provide an overview of the requirements for the security program and a description of the security program management controls and common controls (in place or planned), where applicable, for meeting those requirements.	2.1.3 2.2.10	PM-1	LMH
21.1.3	The information security program shall provide sufficient information about the program management controls and common controls to enable an implementation that is unambiguously compliant with the intent of the plan and a determination of the risk to be incurred if the plan is implemented as intended. The Common Control Provider is an organizational official responsible for planning, developing, implementing, assessing, authorizing, and maintaining common controls.	2.1.3 2.2.10	PM-1	LMH
21.1.4	The SP shall be approved by the TSA and DHS CISOs.	3.1.c	PM-1	LMH
21.1.5	The TSA-wide information security program plan shall be reviewed annually by the CISO.	3.4	PM-1 PL-3	LMH
21.1.6	The information security plan shall be revised to address TSA changes and problems identified during plan implementation or security control assessments.	3.4	PM-1 PL-2	LMH F
21.1.7	The TSA CISO shall serve as the principal interface between the DHS CISO, TSA ISSOs, and other security practitioners.	2.1.4.a	PM-1	LMH
21.1.8	The TSA CISO shall work directly with the DHS CISO.	2.1.4.b	PM-1	LMH
21.1.9	Information security reports, such as OIG reports, regarding TSA systems shall be submitted to the CISO.	3.1.f	PM-1	LMH
21.1.10	The TSA CISOs shall define performance measures to evaluate the effectiveness of the TSA information security program.	3.4.a	PM-1	LMH
21.1.11	The CISO shall provide OMB FISMA data on a monthly basis to the DHS Compliance Officer or upon request.	3.4.b	PM-1	LMH

3.21.2 Information Security Program Roles (PM-2)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
21.2.1	The TSA CISO shall serve as the Senior Information Security Officer and have the resources to coordinate, develop, implement, and maintain a TSA-wide information security program in support of the TSA mission.	2.1.3	PM-2 PM-1	LMH

3.21.3 Information Security and Privacy Resources (PM-3)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
21.3.1	The SO shall include information security requirements in a Capital Planning and Investment Control (CPIC) business case for the current budget year and for future years in compliance with Directive 102-01 Rev 3, Acquisition Management Directive and DHS MD 4200.1, IT CPIC, and Portfolio Management.	3.2.a	PM-3 PM-11 SA-1	LMH
21.3.2	The SO shall ensure that all capital planning and investment requests include the resources needed to implement the information security program and include a documentation of all waivers to DHS and TSA information security requirements.	3.2.a	PM-3 PM-4 SA-2	LMH
21.3.3	The AO and SO shall ensure that information security requirements and POA&Ms are adequately funded, resourced, and documented in compliance with current OMB budgetary guidance.	3.2.b	PM-3	LMH
21.3.4	The SO shall ensure that information security resources are available for expenditure as planned.	3.2.a 3.2.b	PM-3 SA-2	LMH

3.21.4 Plan of Action and Milestones Process (PM-4)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
21.4.1	The CISO shall establish a process for ensuring that POA&Ms for the TSA-wide security program, TSA IT assets, and the associated TSA information systems are developed, implemented, and maintained. This process shall be documented in the *POA&M process* and in compliance with the DHS Performance Plan.	2.2.8.a 2.2.8.d	PM-4 CA-5	LMH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
21.4.2	The POA&M process shall include steps to identify vulnerabilities to TSA IT assets or data and to mitigate the resultant risk to TSA operations and assets, individuals, other organizations, and the Nation.	2.2.8.d	PM-4	LMH

3.21.5 System Inventory (PM-5)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
21.5.1	The CISO shall ensure the development, maintenance and inventory of all TSA information systems.	4.6.1.f	PM-5	LMH
21.5.2	The CISO shall ensure the implementation of the DHS *FISMA Inventory Methodology* and ensure enhancements are established as required by FISMA.	3.18.d 4.6.1	PM-5	LMH
21.5.3	All operational TSA IT assets shall be associated with an information system identified in the TSA inventory.	2.2.4	PM-5	LMH
21.5.4	The CISO shall ensure to utilize OMB guidance for developing its information systems inventories and associated reporting requirements.	4.6.1	PM-5 AC-18	LMH
21.5.5	The CISO shall ensure the review of all system applications for wireless usage, maintain an inventory of systems, and provide that inventory to the DHS CISO annually.	4.6.1.f	AC-18 PM-5	LMH
21.5.6	The SO shall maintain a current inventory of all approved mobile devices in operation.	4.6.2.h	PM-5	LMH
21.5.7	The SO shall maintain a current inventory of all approved wireless tactical systems in operation.	4.6.1.f	PM-5	LMH

3.21.6 Measures of Performance (PM-6)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
21.6.1	The CISO shall ensure the development of outcome-based metrics for measuring the effectiveness or efficiency of the information security program and the security controls employed in support of the program.	3.4	PM-1 PM-6	LMH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
21.6.2	The CISO shall implement a process for reporting the results of information security measures of performance employed in support of the program.	3.4	PM-1 PM-6	LMH
21.6.3	The ISSO shall provide quarterly and annual data on the information system's performance measures to the CISO.	3.10.c	PM-6 PL-1	LMH
21.6.4	The ISSO and IAD shall utilize the automated tool directed for use by the DHS CISO for Performance Plan reporting.	3.4.d	PM-4 PM-6	LMH

3.21.7 Enterprise Architecture (PM-7)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
21.7.1	The CIO shall develop Enterprise Architecture with considerations for information security and resulting risk to TSA operations, assets, individuals, other organizations, and the Nation in compliance with DHS Enterprise Architecture requirements.	3.1.g	PM-7 PL-1	LMH
21.7.2	An Enterprise System Security Agreement (ESSA) shall be developed for all enterprise services.	3.9.w	PM-1	LMH

3.21.8 Critical Infrastructure Plan (PM-8)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
21.8.1	The CISO shall address information security issues in the development, documentation, and update of a critical infrastructure and key resources protection plan.	3.5 4.1	PM-8	LMH

3.21.9 Risk Management Strategy (PM-9)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
21.9.1	The CISO shall develop and implement a comprehensive strategy to manage risk to TSA operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems consistently across TSA.	2.1.5 3.8.a 3.8.b 3.9.g	PM-9 PL-1	LMH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
21.9.2	The CISO shall ensure that a risk assessment is conducted whenever any modifications are made to sensitive information systems, networks, or to their physical environments, interfaces, or user community. SPs shall be updated and re-authorization conducted if warranted.	3.8.a	PM-9 PM-10 PA-3	LMH
21.9.3	The CISO shall review and update the risk management strategy at least annually or as required to address organization changes. See DHS *Cybersecurity Strategy* for additional information on risk.	2.1.5	PM-9	LMH

3.21.10 Authorization Process (PM-10)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
21.10.1	The CISO shall manage, document, track, and report the security state of TSA entrusted information systems through security authorization processes.	3.8.c 3.9.n	CM-1 PM-10	LMH F
21.10.2	The CISO shall designate individuals to fulfill specific roles and responsibilities within the TSA risk management process.	3.9	CM-1 PM-10 PS-2	LMH F
21.10.3	The CISO shall fully integrate the security authorization processes into the TSA-wide risk management program.	3.8.c 3.9.g	PM-10 CA-1 RA-1	LMH F
21.10.4	The SO shall assign a potential impact level (*high, moderate, low*) to each security objective (Confidentiality, Integrity, and Availability) for each TSA information system in compliance with NIST SP 800-53 controls.	3.9.a	PM-10 CA-1	LMH F
21.10.5	The SO shall implement the security authorization process for the information system.	3.9	PM-10 CA-1	LMH F
21.10.6	The assessments, made as part of and in support of the authorization process, shall determine the extent to which a particular design and implementation plan meets the TSA required set of security controls.	3.9.f	PM-10 CA-2	LMH F
21.10.7	The SO shall ensure that only FedRAMP CSPs are used when acquiring cloud services. See TS-072 *Cloud Computing and Virtualization* and TS-049 *Information System Audit Logging* for additional information.	3.18.a-e	AC-16 AC-20 RA-3	LM F

3.21.11 Mission and Business Process Definition (PM-11)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
21.11.1	The CIO shall define mission/business processes with consideration for information security and the resulting risk to TSA operations, IT assets, individuals, other organizations, and the Nation.	3.11.1	PM-11 PL-1	LMH
21.11.2	The CISO shall determine information protection needs arising from the defined mission/business processes and revise the processes as necessary, until an achievable set of protection needs is obtained.	3.11.1	PM-11 PL-1	LMH

3.21.12 Insider Threat Program (PM-12)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
21.12.1	The CISO shall ensure that an insider threat program is implemented to include a cross-discipline insider threat incident handling team. See **TSA MD 2800.17 *Insider Threat Program*** for additional information and policy.	2.1.3.a	PM-12	LMH

3.21.13 Security and Privacy Workforce (PM-13)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
21.13.1	The CISO shall ensure that it establishes an information security workforce development and improvement program.	2.1.3.a	PM-13	LMH

3.21.14 Testing, Training, and Monitoring (PM-14)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
21.14.1	The CISO shall ensure that it implements a process for security testing, training, and monitoring of activities associated with information systems, and that these: a. Are developed and maintained; and b. Continue to be executed in a timely manner.	2.1.3.a	PM-14	LMH
21.14.2	The CISO shall ensure that it reviews testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.	2.1.3.a	PM-14	LMH

3.21.15 Contacts with Groups and Associations (PM-15)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
21.15.1	The AO shall ensure that it establishes and institutionalizes contact with selected groups and associations within the security community: a. To facilitate ongoing security education and training for organizational personnel; b. To maintain currency with recommended security practices, techniques, and technologies; and c. To share current security-related information including threats, vulnerabilities, and incidents.	2.1.6	PM-15	LMH

3.21.16 Threat Awareness Program (PM-16)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
21.16.1	Place Holder	TBD	TBD	TBD

3.21.17 Protecting Controlled Unclassified Information (CUI) on External Systems (PM-17)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
21.17.1	Place Holder	TBD	TBD	TBD

3.21.18 Privacy Program Plan (PM-18)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
21.18.1	Place Holder	TBD	TBD	TBD

3.21.19 Privacy Program Roles (PM-19)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
21.19.1	Place Holder	TBD	TBD	TBD

3.21.20 System of Records Notice (PM-20)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
21.20.1	Place Holder	TBD	TBD	TBD

3.21.21 Dissemination of Privacy Program Information (PM-21)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
21.21.1	Place Holder	TBD	TBD	TBD

3.21.22 Accounting of Disclosures (PM-22)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
21.22.1	Place Holder	TBD	TBD	TBD

3.21.23 Data Quality Management (PM-23)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
21.23.1	Place Holder	TBD	TBD	TBD

3.21.24 Data Management Board (PM-24)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
21.24.1	Place Holder	TBD	TBD	TBD

3.21.25 Data Integrity Board (PM-25)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
21.25.1	Place Holder	TBD	TBD	TBD

3.21.26 Minimization of Personally Identifiable Information (PM-26)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
21.26.1	Place Holder	TBD	TBD	TBD

3.21.27 Individual Access Control (PM-27)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
21.27.1	Place Holder	TBD	TBD	TBD

3.21.28 Complaint Management (PM-28)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
21.28.1	Place Holder	TBD	TBD	TBD

3.21.29 Inventory of Personally Identifiable Information (PM-29)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
21.29.1	Place Holder	TBD	TBD	TBD

3.21.30 Privacy Reporting (PM-30)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
21.30.1	Place Holder	TBD	TBD	TBD

3.21.31 Supply Chain Risk Management Plan (PM-31)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
21.31.1	Place Holder	TBD	TBD	TBD

3.21.32 Risk Framing (PM-32)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
21.32.1	Place Holder	TBD	TBD	TBD

3.21.33 Privacy Impact and Risk Assessment (AR-2 Appendix J: From PL-5)

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
21.33.1	The SO shall ensure a privacy impact assessment is performed on the information system when deemed necessary as stated in the Privacy Threshold Analysis (PTA) document.	3.14 3.14.3	AR-2	P
21.33.2	The SO shall ensure compliance with the individual privacy requirements of the OMB Circular A -130, Appendix I.	3.14 3.14.3	AR-2	P
21.33.3	Reserved			
21.33.4	Reserved			

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
21.33.5	The TSA Chief Privacy Officer shall establish administrative processes that can respond to complaints, requests for corrections of health information, and track disclosures of Privacy Health Information (PHI).	3.17.d	AR-2	P
21.33.6	When collecting PHI, the information system shall issue a privacy notice to individuals concerning the use and disclosure of their PHI.	3.17.e	AR-2	P
21.33.7	A PTA shall be conducted as part of new information system development or whenever an existing system is significantly modified with regard to the information it stores, processes, or transmits. PTA artifacts expire after a maximum of three (3) years and a new PTA shall be submitted.	3.14.2.a 3.14.3.a	AR-2	P
21.33.8	The Chief Privacy Officer shall evaluate the PTA and determine if it is a Privacy Sensitive System and if the system requires a PIA and SORN.	3.14.2.c	AR-2	P
21.33.9	A PTA shall be conducted whenever an information system undergoes security authorization and the information systems shall not be designated operational until the PTA is approved.	3.14.2. b 3.14.2. d	AR-2	P
21.33.10	Reserved			
21.33.11	Programs considering the use of e-authentication shall contact the Chief Privacy Officer to determine whether a change is significant enough to warrant a new or updated PTA.	3.14.7.e	AR-2	P

4. Roles and Responsibilities

As a DHS organizational element, TSA is directed by DHS MD 0007.1, Addendum C, to follow guidance and policies as outlined within DHS MD 4300A and DHS Information Assurance (IA) Program Publications.

Effective IA depends on the involvement of all TSA divisions that acquire, develop, own, operate, or replace information system components with DHS. These TSA divisions shall participate and coordinate with DHS in the formulation and approval of TSA IA policy, as well as requirements, procedures, and IT Security risk mitigation strategies which support and compliment DHS guidance and comply with the policy and responsibilities cited herein.

TSA fosters a defense-in-depth approach to information security along with the enforcement of established information security policy that is supported and adhered to by all TSA management, employees, and contractors. TSA IA policy addresses the use of a wide range of TSA GSSs and MAs, including prototypes and telecommunications systems. Other supported mission critical data processing environments include: Business Process Support Systems, Program Delivery Systems, systems supporting IT Infrastructure, IT Special Projects, and General Office Automation.

The TSA IA policy falls directly in line with the DHS Information Security Program, which serves as a foundation for DHS components to use in establishing component IT security programs. The DHS IT Program ensures that comprehensive, uniform IT security policies are followed by each DHS component. The DHS IT Program shall provide clarification to national policies, adapt them to specific circumstances, and impose additional requirements when necessary.

The following responsibilities outlined apply to TSA specific assigned roles and duties.

4.1 Chief Information Officer

The CIO is the Government official responsible for information systems and the effectiveness and completeness of each system's IT security as well as for ensuring FISMA compliance within TSA.

Per the TSA MD 100.0 *TSA Roles and Responsibilities*:

> The Assistant Administrator for Information Technology/Chief Information Officer is responsible for:
>
> 1) Providing the vision and leadership for developing and implementing TSA's information technology (IT) strategic plan and initiatives;
> 2) Developing, coordinating, implementing, and managing central policies and procedures for all of TSA's IT requirements;
> 3) Managing and overseeing effective security architecture that protects TSA's information systems and networks from internal and external threats;
> 4) Ensuring compliance with applicable laws, rules and regulations, including the Government Performance and Results Act of 1993, the Clinger-Cohen Act, OMB Circular A-130 ("Management of Federal Information Resources"), and the Federal Information Security Modernization Act (FISMA); and
> 5) Serving as TSA's representative to the DHS Chief Information Officer Council to collaborate on Departmental IT strategies, initiatives, goals, and priorities.

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
1.1	The CIO shall establish and provide oversight of the IA Program within TSA.	2.2.4	PL-1 PM-1	LMH
1.2	The CIO shall appoint a senior federal employee in writing to serve as the CISO and the SCA. The appointment shall be countersigned by the TSA Deputy Administrator.	2.2.4	PL-1 PM-1	LMH
1.3	The CIO shall ensure that IT security concerns are addressed by the TSA Systems Configuration Control Boards, Architecture Review Board, and Investment Review Board.	2.2.4	PL-1 PM-1	LMH
1.4	The CIO shall ensure that references to Information System Security policy are included in new, renewed, or modified contracts, MOA, and MOU.	2.2.4	PL-1 PM-1	LMH
1.5	The CIO shall ensure that all information system acquisitions, Requests for Proposals (RFPs), and other contracting actions, including service life extension and decommissioning activities, include IT security requirements (as appropriate) and comply with TSA IA policy.	2.2.4	PL-1 PM-1	LMH
1.6	The CIO shall ensure that IT Security concerns are addressed in the TSA CPIC processes.	2.2.4	PL-1 PM-1	LMH
1.7	The CIO shall ensure IA performance metrics are developed, implemented, and funded.	2.2.4	PL-1 PM-1	LMH
1.8	The CIO shall ensure adequate budget is requested to provide funding for the IAD Director.	2.2.4	PL-1 PM-1	LMH
1.9	The CIO shall advise the DHS CIO of any issues regarding infrastructure protection, vulnerabilities, or issues that may affect public perception or loss of credibility.	2.2.4	PL-1 PM-1	LMH
1.10	The CIO shall coordinate with the DHS CIO and Public Affairs Office in preparation for public release of security incident information. The DHS CIO, or designated representative, has sole responsibility for public release of security incident information.	2.2.4	PL-1 PM-1	LMH
1.11	The CIO shall implement and maintain safeguards to ensure that protection is provided for all information systems and networks that collect, process, transmit, store and/or disseminate information.	2.2.4	PL-1 PM-1	LMH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
1.12	The CIO shall provide effective protection for TSA's general support systems, major application systems, and the facilities for housing or supporting the operation of such systems.	2.2.4	PL-1 PM-1	LMH
1.13	The CIO shall develop and maintain the TSA Information Security Program and shall designate the CISO who shall report directly to the CIO as principal advisor on information security matters.	2.2.4.a	PL-1	LMH
1.14	The CIO shall appoint a federal employee in writing to serve as the AO.	2.2.4	PL-1 PM-1	LMH

4.2 Chief Information Security Officer

The TSA Director of Information Assurance and Cybersecurity Division shall be designated as the TSA CISO or the Risk Executive (RE). The CISO, who could also be designated as the Information Systems Security Manager (ISSM), is the TSA official responsible for implementing TSA's IT security program under the direction of the DHS CISO including identifying, developing, and maintaining processes across the TSA IT enterprise and lines of businesses to reduce information risks, as well as responding to incidents, establishing appropriate standards and controls, and directing the establishment and implementation of cost-effective policies and procedures that are consistent with FISMA.

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
2.1	The CISO shall implement the TSA IT security program.	2.1.3	PL-1 PM-2	LMH
2.2	The CISO shall ensure that the TSA CIO and DHS CISO are kept apprised of all pertinent matters involving the security of TSA information systems.	2.1.3	PL-1 PM-1	LMH
2.3	The CISO shall review and provide input on Exhibit 300 funding documents.	2.1.3	PL-1 PM-2	LMH
2.4	The CISO shall review and approve the security of hardware and software prior to implementation into the TSA SOC.	2.1.3	PL-1, PM-2	LMH
2.5	The CISO shall ensure the TSA IT security program is structured to support TSA and appropriate FISMA and OMB requirements.	2.1.3	PL-1 PM-2	LMH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
2.6	The CISO shall develop and publish procedures necessary to implement the requirements of DHS and TSA IA policy.	2.1.3	PL-1 PM-2	LMH
2.7	The CISO shall review and approve ISSO appointments to ensure that a qualified and dedicated ISSO is appointed for each information system managed by TSA.	2.1.3	PL-1 PM-2	LMH
2.8	The CISO shall assist the AO in ensuring that each portion of the TSA information system undergoes a detailed assessment leading to formal Authorization.	2.1.3	PL-1 PM-2	LMH
2.9	The CISO shall collaborate with TSA offices to prioritize IT Security activities and resource allocation.	2.1.3	PL-1 PM-2	LMH
2.10	The CISO shall consolidate and develop IT Security responses to Congressional inquiries and inquiries from the OMB, General Accounting Office (GAO), DHS, etc., in support of TSA Assistant Administrators (AAs).	2.1.3	PL-1 PM-2	LMH
2.11	The CISO shall authorize penetration testing on TSA information systems through advanced coordination with the AO, the Office of Chief Counsel, the Acquisitions office, and SO.	2.1.3	PL-1 PM-2	LMH
2.12	The CISO shall authorize the performance of investigations, including the gathering, analyzing, and preserving of evidence to be used in the prosecution of computer crimes, based on security incident reporting, audits, or as required to facilitate requests from authorized government officials.	2.1.3	PL-1 PM-2	LMH
2.13	The CISO shall exercise oversight for all TSA security operations functions, including the Security Operations Center.	2.1.3	PL-1 PM-2	LMH
2.14	The CISO shall ensure TSA MD 1400.3, IT Security Handbook and all supporting documentation have been created, provide detailed policy and implementation information, including policies that relate to the management, operational, industrial, and technical controls, and are available on the IAD Security Policy website.	2.1.3	PL-1 PM-2	LMH
2.15	The CISO shall ensure the Security Training section within DHS FISMA Manager resource is updated at least once per quarter.	2.1.3	PL-1 PM-2	LMH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
2.16	The CISO shall ensure that external providers who operate information systems on behalf of TSA meet the same security requirements as required for information and information systems.	2.1.3	PL-1 PM-2	LMH
2.17	The CISO shall ensure an acceptable level of trust in the external service; or using compensating controls to secure information or the process flow, accepting a greater degree of risk, or reducing the functionality to the extent necessary to make the risk acceptable.	2.1.3	PL-1 PM-2	LMH
2.18	The CISO shall appoint a representative to the DHS Security Policy Working Group.	3.11.3	NA	NA
2.19	The CISO shall be the authority for interpretation, clarification, and modification of the TSA IA Management Directives, Handbooks, Technical Standards, and IAD SOPs (inclusive of all appendices and attachments).	1.7.a	PL-1	LMH
2.20	The CISO shall review and update TSA IA policy annually as needed.	1.7.b	PL-1 PM-1	LMH
2.21	The CISO shall implement and manage the TSA-wide Information Security Program in compliance with the DHS security program.	2.1.3.a	PL-1 PM-2	LMH
2.22	The CISO shall develop and manage information security guidance and procedures unique to TSA requirements.	3.1.j	PL-1 PM-1	LMH
2.23	The CISO shall submit the TSA IA policy to the DHS CISO for review annually.	3.10.a	PL-1	LMH
2.24	The CISO shall actively participate in the CISO Council.	3.11.1.a	PL-1 PM-11	LMH
2.25	The CISO shall ensure that the DHS CISO is kept apprised of all pertinent matters involving the security of TSA information systems.	3.11.1. b	PL-1 PM-11	LMH
2.26	The CISO shall ensure that security-related decisions and information, including updates to the 4300 series of security publications, are distributed to the ISSOs and other appropriate persons.	3.11.1.c	PL-1 PM-11	LMH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
2.27	The CISO shall have resources to assist with TSA compliance and policy. The CISO shall designate a Deputy CISO with full authorities, to include the roles of Risk Executive (RE) and Security Control Assessor (SCA) upon the absence of the CISO. The CISO and Deputy CISO shall be TSA employees.	2.1.3 3.1	PL-1 PM-2	LMH
2.28	The CISO shall recommend approval or denial of Security Authorizations (SAs).	2.1.3	PL-1 PM-2	LMH
2.29	The CISO shall serve as Security Control Assessor (SCA) when no other person has been officially designated.	2.1.3	PL-1 PM-2	LMH

4.3 System Owner

The SO is the Government security official responsible for the security posture of an assigned set of information systems or locations, per the direction of the AO. For SOs and ISSOs, the term "system" is synonymous with "application" and "software", and the expectation for adherence is the same.

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
3.1	SO shall designate an ISSO in writing for each information system.	2.2.9.b	PL-1 PM-1	LMH
3.2	The SO shall be responsible for the overall procurement, development, integration, modification, operation, and maintenance of an information system.	2.2.9	PL-1 PM-1	LMH
3.3	The SO shall ensure that security requirements are included in the acquisition process and considered throughout the lifecycle of the information system.	2.2.9	PL-1 PM-1	LMH
3.4	The SO shall ensure the development and maintenance of the SP, which documents compliance with TSA and DHS IA policy.	2.2.9	PL-1 PM-1	LMH
3.5	The SO shall ensure the system is deployed and operated according to the security requirements in the SP and information security policy.	2.2.9.a	PL-1 PM-1	LMH
3.6	The SO shall develop ISAs and MOU as documenting the provisions for interconnecting with other systems and the rules for such interconnections and data sharing.	2.2.9	PL-1 PM-1	LMH
3.7	The SO shall notify the CISO of any changes to the information system SELC status or when new information systems are in development.	2.2.9	PL-1 PM-1	LMH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
3.8	The SO shall inform the SCA or CIO of the need to conduct a security authorization or update of the information system.	2.2.9	PL-1 PM-1	LMH
3.9	The SO shall ensure that adequate resources are available to ensure information security during all system life-cycle phases.	2.2.9	PL-1 PM-1	LMH
3.10	The SO shall take appropriate steps, including ensuring adequate funding, to reduce or eliminate vulnerabilities.	2.2.9	PL-1 PM-1	LMH
3.11	The SO shall ensure the successful operation and hold ultimate accountability for the security of the information systems and programs under their control.	2.2.9	PL-1 PM-1	LMH
3.12	The SO shall work with the SSI Program Office to develop the SSI TA and obtain SSI IA approval from the SSI Program Office for all SSI systems.	2.2.9	PL-1 PM-1	LMH
3.13	The SO shall understand, document and manage accepted and known security risks.	2.2.9	PL-1 PM-1	LMH
3.14	The SO shall determine the appropriate levels of security and periodically test and evaluate security controls and techniques to ensure that they are cost effective and do not substantially impede business operations.	2.2.9	PL-1 PM-1	LMH
3.15	The SO shall generate and oversee, through mitigation, POA&Ms for identified information security risks, routing the POA&Ms through the SCA and AO for approval, and ensuring that points of contact and resources are identified.	2.2.9	PL-1 PM-1	LMH
3.16	The SO shall prioritize security weaknesses for mitigation and ensure mitigation funding is made available based on material weaknesses, external audits, and program assessments.	2.2.9	PL-1 PM-1	LMH
3.17	The SO shall report Privacy and Computer Security incidents, in coordination with the CISO and Program Manager.	2.2.9	PL-1 PM-1	LMH
3.18	The SO shall work with the TSA Privacy Office to develop Privacy Impact Assessment(s) and obtaining Privacy Impact Assessment approvals from the DHS Privacy Office for all privacy systems.	2.2.9	PL-1 PM-1	LMH
3.19	The SO shall establish procedures to allow cleared users access to their systems.	2.2.9	PL-1 PM-1	LMH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
3.20	The SO shall authorize privileged access to their systems.	2.2.9	PL-1 PM-1	LMH
3.21	The SO shall ensure Personally Identifiable Information (PII)-identified systems implement all necessary NIST SP 800-53 controls as identified in OMB M-06-16.	2.2.9	PL-1 PM-1	LMH
3.22	The SO shall implement and maintain safeguards to ensure that protection is provided for all information systems and networks that collect, process, transmit, store and/or disseminate TSA information.	2.2.9	PL-1 PM-1	LMH
3.23	The SO shall ensure compliance with all applicable Federal statutes and regulations governing IA, including DHS Directive System 140-01 *Information Technology Security Program*, and DHS Policy Directives (PD) 4300A *Sensitive Systems Policy* and DHS PD 4300B *National Security Systems Handbook*.	2.2.9	PL-1 PM-1	LMH
3.24	The SO shall ensure the accountability, Confidentiality, Integrity, and Availability of information, data, and source codes. See **OMB Memo M-16-21** regarding open source software code. Also, see **DHS PD 142-04** DHS Reusable and Open Source Software (OSS) Framework; and **Open Source Software (OSS) Policy Guidance.**	2.2.9	PL-1 PM-1	LMH
3.25	The SO shall prohibit the opportunity to create unauthorized links to other systems, bypass authentication mechanisms, circumvent data access control procedures, or otherwise jeopardize the security of any or all components within TSA systems, networks or data.	2.2.9	PL-1 PM-1	LMH
3.26	The SO shall ensure any information systems processing sensitive or classified information have developed encryption plans prior to authorization.	2.2.9	PL-1 PM-1	LMH
3.27	SO shall ensure personnel implementing encryption requirements are technically qualified and adequately trained in encryption technologies and ensure that specific methodologies are employed.	2.2.9	PL-1 PM-1	LMH
3.28	The SO shall ensure that each information system is deployed and operated in compliance with this policy document.	2.2.9.a	PL-1	LMH
3.29	The SO shall ensure that an ISSO is designated, in writing, for each information system under their purview.	2.2.9.b	PL-1	LMH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
3.30	Only one SO shall be designated for each TSA system.	2.2.9.c	PL-1	LMH
3.31	The SO shall ensure that any hardware or software develops a full lifecycle plan based on the vendor's established life expectancy of the product and total cost of ownership. Any new or existing product that shall reach end-of-life (EOL)* within three (3) years and is part of a TSA FISMA IT System shall require development of a remediation, upgrade, replacement and funding plan to remove the EOL item(s) from the TSA environment completely within that time frame. A POA&M shall be submitted for risk acceptance to the TSA CISO and AO in order to track remediation milestones appropriately. *EOL- End of Life is defined as production and/or development, technical support, spare parts and security patches which are no longer available from the vendor."	2.2.9.j	PL-1 SA-1	LMH
3.32	The SO shall follow all TSA policy and directives.	2.2.9.b	PL-1 PM-1	LMH
3.33	The SO shall review and update, as necessary the system security controls, the Federal Information Processing Standard (FIPS) 199 Security Categorization, PTA, PIA, and Security Plan (SP).	2.2.9	PL-1 PM-1	LMH
3.34	The SO shall execute Steps 1, 2, 3, and 6 of the RMF.	2.2.9	PL-1 PM-1	LMH
3.35	The SO shall ensure the confidentiality, integrity and availability (CIA) of all aspects of the information system including, but not limited to data, information and source code. Information on **Open Source Code (OSS)** may be found **here**.	2.2.9	PL-1 PM-1	LMH
3.36	The SO shall participate in and actively support (as with the ISSO) system assessments.	2.2.9.a	PL-1 PM-1	LMH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
3.37	The SO shall designate a TPoC or designee in order to support the system assessments; the TPoC is the main point of contact for questions regarding the system that may arise during the assessment; during testing, the designee shall be responsible for approving or escalating all events and deviations from testing to the program management.	2.2.9	PL-1 PM-1	LMH
3.38	The SO shall grant approval in writing for testing to be conducted in an appropriate Integrated Test Environment (ITE)/User Acceptance Test (UAT) environment.	2.2.9	PL-1 PM-1	LMH
3.39	The SO shall formally identify this test environment in a Scanning Authorization Letter, and provide that environment to the assessment team as an exact replica of the production environment.	2.2.9	PL-1 PM-1	LMH
3.40	The SO shall ensure that selective scanning results obtained in the ITE/UAT environment are verified in the production environment.	2.2.9	PL-1 PM-1	LMH
3.41	The SO shall authorize in writing that testing may be conducted in the production environment should an adequate ITE/UAT environment not be available for security testing purposes, or if initial testing indicates that the ITE and production environments are not exact replicas.	2.2.9	PL-1 PM-1	LMH
3.42	The SO shall ensure that current backups are available for restoration purposes and that a separate duplicative database is available for testing purposes.	2.2.9	PL-1 PM-1	LMH
3.43	The SO shall follow additional requirements in the appropriate RoE.	2.2.9	PL-1 PM-1	LMH
3.44	The SO shall provide a TPoC for the privileged account management process and audit.	2.2.9	PL-1 PM-1	LMH
3.45	The SO shall approve, in advance, any scans performed by the assessment team using a signed Scanning Letter.	2.2.9	PL-1 PM-1	LMH
3.46	The SO shall approve all privileged users, training and account for the information system.	2.2.9	PL-1 PM-1	LMH

4.4 Information Owner

The Information Owner (IO) is the TSA Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing,

dissemination, and disposal. For SOs and ISSOs, the term "system" is synonymous with "application" and "software", and the expectation for adherence is the same.
NOTE: With some systems, the IO may also be the Program Manager, Business Owner, or SO.

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
4.1	The IO shall establish the rules for appropriate use and protection of the subject information (to include rules of behavior). The IO retains this responsibility even when the information is shared with other organizations.	2.2.9, 4.3.2	PL-1 MP-1	LMH
4.2	The IO shall oversee the implementation of the rules for appropriate use in all TSA information systems, including Minor Applications (MiA). See MiA definition for additional information.	2.2.9, 4.3.2	PL-1 MP-1	LMH
4.3	The IO shall ensure all information is restricted on a need to know basis with annual reviews of the access list.	2.2.9, 4.3.2	PL-1 MP-1	LMH
4.4	The IO shall designate in writing the use of and restrictions to access to SSI, PII and FOUO information.	2.2.9, 4.3.2	PL-1 MP-1	LMH
4.5	The IO shall establish the controls for data generation, collection, processing, dissemination, and disposal.	2.2.9, 4.3.2	PL-1 MP-1	LMH
4.6	The IO shall ensure the protection of information and the information systems that store, process, or transmit TSA information.	2.2.9, 4.3.2	PL-1 MP-1	LMH
4.7	The IO shall direct the security categorization process in conjunction with the SO and Risk Executive.	2.2.9, 4.3.2	PL-1 MP-1	LMH
4.8	The IO shall create the system description,	2.2.9, 4.3.2	PL-1 MP-1	LMH
4.9	The IO shall participate in security control selection and continuous monitoring.	2.2.9, 4.3.2	PL-1 MP-1	LMH

4.5 Information Systems Security Officer

The Information System Security Officer (ISSO) is the security official, either government or contractor, responsible for the security posture of an assigned set of information systems or locations per the direction of the SO. The ISSO shall coordinate and inform the Governance, Risk and Compliance (GRC) Portfolio Manager on all general ISSO-related activities including issues concerning TSA IT systems and/or equipment. For SOs and ISSOs, the term "system" is synonymous with "application" and "software", and the expectation for adherence is the same.

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
5.1	The ISSO shall serve as the principal point of contact for all IT security aspects pertaining to the systems under their responsibility in support of the SO.	2.1.8 Attch C	PL-1	LMH
5.2	The ISSO shall work closely with the SO, CISO, and IAD staff to interpret and apply IA policies and implement procedures.	2.1.8 Attch C	PL-1	LMH
5.3	The ISSO shall serve as liaison between the SO and the TSA CISO.	2.1.8 Attch C	PL-1	LMH
5.4	The ISSO shall work with the SO to document weaknesses in POA&Ms and initiate corrective action.	2.1.8 Attch C	PL-1	LMH
5.5	The ISSO shall employ automated tools as directed by IAD.	2.1.8 Attch C	PL-1	LMH
5.6	The ISSO shall compile an inventory of allocated information systems and providing a copy of the inventory on an annual basis to the TSA CISO or upon request.	2.1.8 Attch C	PL-1	LMH
5.7	The ISSO shall perform duties as required in the DHS Performance Plan, as directed by IAD.	2.1.8 Attch C	PL-1	LMH
5.8	The ISSO shall develop IT security plans by using the security controls specified in the Computer Security Act of 1987, OMB Circular A-130, DHS regulations, NIST guidance, and other statutory and regulatory policies and guidance.	2.1.8 Attch C	PL-1	LMH
5.9	The ISSO shall conduct risk assessments that address vulnerabilities, threats, risk management, operational and technical security controls, and levels of risk acceptance.	2.1.8 Attch C	PL-1	LMH
5.10	The ISSO shall perform other ISSO specific tasking as defined in the DHS “ISSO Guide to the DHS Information Security Program" and the specific TSA ISSO appointment letter.	2.1.8 Attch C	PL-1	LMH
5.11	The ISSO shall ensure the accountability, Confidentiality, Integrity, and Availability of information, data, and source codes.	2.1.8 4.6.2 Attch C	PL-1	LMH
5.12	The ISSO shall ensure the protection of information and the information systems that store, process, or transmit TSA information.	2.1.8 Attch C	PL-1	LMH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
5.13	An ISSO shall be designated in writing by the CISO for every information system and serve as the POC for all security matters related to that system.	2.1.8.a Attch C	PL-1	LMH
5.14	An ISSO shall ensure the implementation and maintenance of security controls in compliance with the SP and DHS policy.	2.1.8.b Attch C	PL-1	LMH
5.15	The ISSO shall be a DHS employee or a contractor.	2.1.8.c Attch C	PL-1	LMH
5.16	The ISSO shall be permitted to be assigned to more than one system.	2.1.8.d Attch C	PL-1	LMH
5.17	ISSO duties shall not be assigned as collateral duties unless approved by the CISO.	2.1.8.e Attch C	PL-1	LMH
5.18	The ISSO shall be granted a clearance and access greater than or equal to the highest level of information contained on the system. It is strongly encouraged that ISSOs be cleared to the Secret level in order to facilitate intelligence sharing among information security professionals.	2.1.8.f Attch C	PL-1	LMH
5.19	The ISSO shall ensure that timely responses are provided to SCCB change request packages.	2.1.8.g Attch C	PL-1	LMH
5.20	The ISSO shall serve as the POC for all security matters related to that system.	3.1.d Attch C	PL-1	LMH
5.21	The ISSO shall support Steps 1, 2, 3, and 6 of the RMF.	2.1.8 Attch C	PL-1	LMH
5.22	The ISSO shall ensure code developers adhere to US-CERT coding practices.	2.1.8 Attch C	PL-1	LMH
5.23	The ISSO shall also ensure the confidentiality, integrity, and availability (CIA) of all aspects of the information system including, but not limited to, data, information, and source code.	2.1.8 Attch C	PL-1	LMH
5.24	The ISSO shall participate in system assessments, including HVA system assessments (HVASAs). Additional information on HVA and related overlays per OMB M-17-09 can be found **here.** BODs can be found **here**.	2.1.8 Attch C	PL-1	LMH
5.25	The ISSO shall support systems undergoing assessments, including HVA systems.	2.1.8 Attch C	PL-1	LMH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
5.26	The ISSO shall maintain inventory of privileged users and ensure annual training.	2.1.8 Attch C	PL-1	LMH
5.27	The ISSO, as with the SO, may designate a TPoC in order to support system assessment and is the main contact for any questions regarding the system that may arise during the system assessment. During testing, the designee will be responsible for approving or escalating all events and deviations from testing to the program management.	2.1.8 Attch C	PL-1	LMH
5.28	The ISSO shall ensure that prior to commencing the activities and connecting to the target system, the TSA scanning laptops are scanned and verified to be up-to-date and clean of viruses and malware.	2.1.8 Attch C	PL-1	LMH
5.29	The ISSO shall, together with the TSA team, determine physical requirements, such as network and electrical connectivity, during assessment entrance brief.	2.1.8 Attch C	PL-1	LMH
5.30	The ISSO shall ensure credentials, access level, and accounts anticipated for the system are addressed during the entrance brief; any deviation from this formula will be addressed by the SA team, the ISSO (or designee), and the on-site technical POCs; deviations shall follow standard Rules of Engagement (RoE).	2.1.8 Attch C	PL-1	LMH
5.31	The ISSO shall coordinate with SA team to determine if scanning laptops can be added to the target network domain in order to facilitate system assessments (request shall be sent via email to the ISSO from the TSA PA and the ISSO shall follow procedures to evaluate and approve the request. Request shall be acknowledged and approved in writing by the ISSO prior to allowing any TSA laptop to be added to the target network domain).	2.1.8 Attch C	PL-1	LMH
5.32	The ISSO shall coordinate with the SA team for the creation of scanning privileged accounts in the target system in order to facilitate a system assessment (requests shall be sent via email to the ISSO from the PA; follow procedures to evaluate and approve the request. Requests shall be acknowledged and approved in writing by the ISSO prior to the creation of accounts in the target system).	2.1.8 Attch C	PL-1	LMH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
5.33	The ISSO shall ensure system audit logs are reviewed monthly and issues are appropriately remediated, and verify audit logs are capturing necessary information for the system. The respective system ISSO shall ensure that, for example privileged user activities are logged and regularly reviewed. Note: The IAD Security Operations Center (SOC) does reviews logs from an enterprise perspective and is engaged when there's an issue or incident, however, the SOC cannot perform this function for every system. (If the SOC reviews security logs, including application logs, then the ISSO can conduct a "spot audit" to ensure abnormal events are not occurring. If not all logs are sent to the SOC, the ISSO is responsible for audit log reviews until the SOC captures all logs. Even then, "spot audits" are required).	2.1.8 Attch C	PL-1	LMH

4.6 Authorizing Official

The Authorizing Official is the senior management official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to TSA operations (including mission, functions, image, or reputation), IT assets, and individuals.

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
6.1	The AO shall ensure that funding for implementation of IT security is included in project life cycle planning.	2.2.2.a	PL-1 PM-1	LMH
6.2	The AO shall evaluate the Security Authorization (SA) Package findings and assess vulnerabilities and residual risks.	2.1.6.e	PL-1 PM-1	LMH
6.3	The AO shall approve corrective action and ensure its implementation.	Not Defined	PL-1 PM-1	LMH
6.4	The AO shall accept the system's residual risks, as described in the Statement of Residual Risk in the Security Assessment Report (SAR).	4.5.4.a	PL-1 PM-9	LMH
6.5	The AO shall sign the Authorization Memorandum that documents the Authorization decision determined by the adequacy of system safeguards providing the ATO.	3.9.h	PL-1 PM-10	LMH
6.6	The AO shall determine the period of Authorization, not to exceed three years.	3.9.h	PL-1 PM-10	LMH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
6.7	The AO shall oversee compliance with security life cycle and risk management processes.	2.1.6	PL-1 PM-1	LMH
6.8	The AO shall grant an Authorization with conditions based on the acceptability of system safeguards and the risks of operating in conditional status, approval of proposed corrective action, and approval of the schedule to accomplish proposed corrective action.	2.1.6	PL-1 PM-1	LMH
6.9	The AO shall deny Authorization if the system's vulnerabilities permit potential breaches to the system or application.	Not Defined	PL-1 PM-1	LMH
6.10	The AO shall ensure that if a major change to the system or operating environment is implemented, or a breach of security has occurred, that the information system is reauthorized prior to it being placed back into operation.	3.9.g	PL-1 PM-1	LMH
6.11	The AO shall review Notices of Findings and Recommendations and POA&Ms.	3.9.o	PL-1 PM-1	LMH
6.12	The AO shall approve the implementation and use of the key management plan at acceptable risk levels.	Not Defined	PL-1 PM-1	LMH
6.13	The AO shall ensure appropriate and effective security measures are included in the key management plan.	Not Defined	PL-1 PM-1	LMH
6.14	The AO shall ensure appropriate and effective security measures are included in the SP.	2.2.10.e	PL-1 PM-1 PM-4	LMH
6.15	The AO shall receive immediate notification when any security features are disabled in response to time-sensitive, mission-critical incidents.	4.6.3.a	CM-3	LMH F
6.16	Reserve			
6.17	The AO shall review, approve, and sign the ISAs.	5.4.3.c 5.4.3.f	CA-3	LMH F
6.18	The AO shall ensure TSA information systems processing sensitive or classified information have developed encryption plans prior to Authorization.	5.5.1.b	IA-7 SC-13 PL-1 PM-1	LMH
6.19	The AO shall ensure the TSA SA Program is established and working in accordance with FISMA and DHS procedures.	2.1.6	PL-1 PM-1	LMH

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
6.20	The AO shall ensure the SA process is executed properly for each TSA information system, in operation or development.	2.1.6	PL-1 PM-1	LMH
6.21	The AO shall ensure security authorization requirements are defined.	2.1.6	PL-1 PM-1	LMH
6.22	The AO shall obtain a threat assessment for the system.	2.1.6	PL-1 PM-1	LMH
6.23	The AO shall support the SA tailoring and level of effort determination.	2.1.6	PL-1 PM-1	LMH
6.24	The AO shall make the determination to authorize, reauthorize, or terminate system operations.	2.1.6	PL-1 PM-1	LMH
6.25	The AO shall monitor SA integrity and oversee compliance validation.	2.1.6	PL-1 PM-1	LMH

4.7 Security Control Assessor

The SCA is the individual who ensures that appropriate security measures are in place for a given system, and recommends whether or not the system should be authorized based on documented residual risk.

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
7.1	The SCA shall ensure that a security control assessment is performed for the information system to identify security risks, determine risk magnitude, and identify what areas need safeguards.	2.1.7	PL-1 CA-1	LMH F
7.2	The SCA shall ensure that required authorization activities are completed and that the results are documented and updated annually.	2.1.7	PL-1 CA-1	LMH F
7.3	The SCA shall ensure that Rules of Behavior and security procedures and guides are developed for each information system.	2.1.7	PL-1 CA-1	LMH F
7.4	The SCA shall ensure that a contingency plan is prepared and tested annually for each information system.	2.1.7	PL-1 CA-1	LMH F

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
7.5	The SCA shall ensure open POA&Ms are documents and tracked through mitigation or risk acceptance.	2.1.7	PL-1 CA-1	LMH F
7.6	The SCA shall ensure that the authorization documentation is recorded as directed by DHS.	2.1.7	PL-1 CA-1	LMH F
7.7	The SCA shall prepare a Security Assessment Report on the status of the security control assessment results and recommending to the AO whether or not the system should be authorized based on documented residual risk.	2.1.7	PL-1 CA-1	LMH F
7.8	The SCA, previously the Certifying Official, is a senior management official who certifies the results of the security control assessment and shall be a Federal Government employee.	2.1.7	PL-1 CA-1	LMH F

4.8 Outsourcing Contractors

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
8.1	TSA Outsourcing Contractors shall ensure TSA information is defined and executed as defined in the security specific clauses of their contract.	2.2.11	PL-1 PL-4	LMH

4.9 Information System Users

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
9.1	Users of TSA information systems shall follow the prescribed rules of behavior for the information system and abide by TSA and DHS security policy.	2.2.11	PL-1 PL-4	LMH

4.10 TSA Administrator

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
10.1	The TSA Administrator shall ensure that information systems and their data are sufficiently protected and shall designate the CIO.	2.2.2.a	PL-1	LMH

4.11 TSA Chief Privacy Officer

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
11.1	The TSA Chief Privacy Officer shall review program and system Privacy Threshold Analyses (PTA), Privacy Impact Assessments (PIA), and System of Records Notices (SORN), providing approval as appropriate.	2.2.6.a	PL-1 PL-5	LMH

4.12 Portfolio Manager

Policy ID	Policy Statements	DHS 4300A	NIST SP 800-53	Category
12.1	The Portfolio Manager shall possess complete understanding of FISMA 214.	Not Defined	Not Defined	LMH
12.2	The Portfolio Manager shall be a Subject Matter Expert in all steps of the Risk Management Framework and execute all steps of that framework as outlined in OMB, NIST, DHS, and TSA guidance.	Not Defined	Not Defined	LMH
12.3	The Portfolio Manager shall ensure PAs are assigned to conduct vulnerability assessments, risk assessments, and privileged account audits.	Not Defined	Not Defined	LMH
12.4	The Portfolio Manager shall provide training to System Owners.	Not Defined	Not Defined	LMH

5. Definitions

Unless otherwise provided, all terms used in this handbook have the meanings provided in the Public Laws, Regulations, and Executive Orders referenced in Section 3 of the TSA MD 1400.3 Information Technology Security.

This list contains definitions for terms used in TSA Policy, including the TSA Information Assurance Handbook and Technical Standards. Additional definitions may be located in the NIST Glossary of Key Information Security Terms and shall be used as a baseline for reference purposes.

A. Administrator – TSA agency head with responsibility and accountability for all actions taken by the agency and for compliance with all constraints placed upon the agency.

B. Application Programming Interface (API) – An application is a software program hosted by an information system that performs a specific function directly for a user and can be executed without access to system control, monitoring, or administrative privileges. An API is source code-based and specifies how some software components interact with one another through means such as accessing databases, hardware, disk drives, video cards, or graphical

user interfaces (GUI). An API comes in the form of a library that may include specifications for functions or routines, programming languages, data structures, object classes, and variables to accomplish a specific task or who are allowed to interact with a specific software component.

C. Authorizing Official (AO) – A senior management official or executive within a Federal Government agency empowered to grant and oversee approval for a system to operate. The AO formally assumes responsibility for operating an information system at an acceptable level of risk to organizational operations including mission, functions, assets, individuals, image, or reputation. The AO shall also assign the Security Control Assessor for the system.

D. Certificate Authority (CA) – A trusted third party that issues certificates and verifies the identity of the holder of the digital certificate.

E. Classified National Security Information – Information that has been determined, pursuant to Executive Order 13526, *Classified National Security Information*, to require protection against unauthorized disclosure and is marked to indicate its classified status.

F. Clear – To use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file (to include file allocation table) but may also include all addressable locations. (See NIST SP 800-88, Guidelines for Media Sanitization).

G. Cloud Computing – A model for enabling on-demand and secured network access to a shared pool of configurable IT capabilities and resources to include networks, servers, storage, applications, and services that can be rapidly provisioned and released with minimal management effort or service provider interaction. It allows users to access technology-based services from the network cloud without knowledge of, expertise with, or control over the technology infrastructure that supports them. This cloud model is composed of five essential characteristics and include: on-demand self-service, ubiquitous network access, location independent resource pooling, rapid elasticity, and measured service. It also includes three service delivery models such as: Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS), and Cloud Infrastructure as a Service (IaaS). Lastly, it also includes four models for enterprise access: Private cloud, Community cloud, Public cloud and Hybrid cloud. (See National Security Systems Glossary, 2010). See Cloud Computing Security Handbook.

H. Cloud Service Provider (CSP) – A FedRAMP-approved entity responsible for providing cloud computing services. A CSP may be comprised of multiple entities, such as a primary, customer-facing organization, which utilizes the products, services, and support of other multiple sub-contracted organizations.

I. Component – A DHS Component is any of the entities within DHS, including all DHS offices and independent agencies.

J. Computer Readable Extracts – “any Federal record or collection of records containing sensitive PII that is retrieved from a DHS-owned database, through a query, reporting tool, extract generation tool, or other means that is then saved into removable media and/or a separate computer-readable device or application such as another database, a spreadsheet, or a text file." (Attachment S1 *Managing CREs Containing SPII, DHS 4300A Sensitive Systems Handbook*).

K. Continuity of Operations – Internal organizational efforts to ensure that a viable capability exists to continue essential functions across a wide range of potential emergencies, through plans and procedures that:

- Delineate essential functions and supporting information systems
- Specify succession to office and the emergency delegation of authority
- Provide for the safekeeping of vital records and databases
- Identify alternate operating facilities
- Provide for interoperable communications
- Validate the capability through tests, training, and exercises

L. Continuity of Operations Plan – A plan that provides for the continuity of essential functions of an organization in the event that an emergency prevents occupancy of its primary facility. It provides the organization with an operational framework for continuing its essential functions when normal operations are disrupted or otherwise cannot be conducted from its primary facility.

M. Controlled Access Area (CAA) – Physical area (e.g., building, room, etc.) to which only authorized personnel are granted unrestricted access. All other personnel are either escorted by authorized personnel or are under continuous surveillance. (See NIST Glossary of Key Information Security Terms).

N. Controlled Unclassified Information (CUI) – Upon implementation of 32 CFR 2002, which will require use of the term CUI, the terms *sensitive information*, as well as others such as "*For Official Use Only (FOUO)"* and "*Sensitive but Unclassified (SBU)"*, will no longer be used. Established by **Executive Order 13556,** the CUI program standardizes the way the Executive branch handles unclassified information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies. The **CUI Registry** is the authoritative source for guidance regarding CUI policies and practices.

O. Cybersecurity – The ability to protect or defend the use of cyberspace from cyber attacks (See NIST Glossary of Key Information Security Terms).

P. Cyberspace – A global domain within the information environment consisting of an interdependent network of information systems infrastructures including the: Internet, telecommunications networks, computer systems, and embedded processors and controllers (See NIST Glossary of Key Information Security Terms).

Q. Degauss – Remove data from certain media by manipulating magnetic properties. Degaussing typically applies to hard disks (including but not limited to IDE, ATA, and SCSI). Also called demagnetizing. (NIST SP 800-88, Guidelines for Media Sanitization)

R. Demilitarized Zone (DMZ) – A network segment that resides between a trusted internal network and an un-trusted external network.

S. Destroy – The result of actions taken to ensure that media cannot be reused as originally intended and that information is virtually impossible to recover or prohibitively expensive to recover (NIST SP 800-88, Guidelines for Media Sanitization).

T. DHS System – A DHS system is any information system that transmits, stores, or processes data or information and is (1) owned, leased, or operated by any DHS Component, (2) operated by a contractor on behalf of DHS, or (3) operated by another Federal, state, or local

Government agency on behalf of DHS. DHS systems include general support systems and major applications. If a system is not owned or operated by DHS, and the data on that system is not owned or controlled by DHS, DHS is not responsible for ensuring that an authorization to operate is in force on that system.

U. Disintegration – A physically destructive method of sanitizing media; the act of separating into component parts. (NIST SP 800-88, Guidelines for Media Sanitization)

V. Domain Name System (DNS) Zone – The name allocated for a particular server. A zone file maintains instructions for resolving specified Internet domain names to the appropriate number form of an Internet Protocol address (an IP address). (See Search Networking, 2004).

W. Essential Functions – Functions that enable Federal Executive Branch agencies to provide vital services, exercise civil authority, maintain the safety and well-being of the general populace, and sustain the industrial and economic base during an emergency.

X. Federal Information Security Modernization Act – The Federal Information Security Modernization Act of 2014 (FISMA) requires each agency to develop, document, and implement an agency-wide information security program to provide a high-level of security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

Y. Foreign Intelligence Information – This type of information relates to the capabilities, intentions, and activities of foreign powers, organizations, or persons, but does not include counterintelligence except for information on international terrorist activities.

Z. General Support System (GSS) – A general support system (GSS) is an interconnected set of information resources under the same direct management control that share common functionality. A GSS normally includes hardware, software, information, applications, communications, data, and users. Examples of a GSS include a local area network (LAN), including smart terminals that support a branch office, a Department-wide backbone, a communications network, or a Departmental data processing center including its operating system and utilities. Note: Security for GSS in use at DHS Headquarters shall be under the oversight of the DHS CIO, with support from the DHS Enterprise Security Operations Center (ESOC). All other GSS shall be under the direct oversight of the respective Component CISOs, with support from the appropriate Component Security Operations Center (SOC). All GSS must have one or more Information Systems Security Officers (ISSO) assigned.

AA. High Value Assets (HVA) – Those assets; systems, information, information systems, and data, for which unauthorized disclosure or loss of control could cause exceptionally grave harm to the United States (U.S.). These IT resources may contain sensitive controls, instructions, data used in critical Federal operations, or unique collections of data (by size or content), or support an agency's mission essential functions, making them of specific value to criminal, politically motivated, or state-sponsored actors for either direct exploitation or to cause a loss of confidence in the U.S. Government. HVA BOD 16-01 can be found **here**.

BB. Hypervisor – See "Virtual Management Monitor (VMM)".

CC. Incineration – A physically destructive method of sanitizing media; the act of burning completely to ashes. (NIST SP 800-88, Guidelines for Media Sanitization)

DD. Information Owner (IO) – Official with statutory or operational authority for specified information and responsibility to establish controls for its generation, collection, processing, dissemination, and disposal.

EE. Information System – Any information technology that is (1) owned, leased, or operated by any TSA Office, (2) operated by a contractor on behalf of TSA, or (3) operated by another Federal, state, or local Government agency on behalf of TSA. Information systems include general support systems and major applications (MA).

FF. Information System Security Officer (ISSO) – Individual with assigned responsibilities for maintaining the appropriate operational security posture for an information system or program. The ISSO is a Government employee or contractor who implements and/or monitors security for a particular system. There is only one ISSO designated to a system, but multiple Alternate ISSOs may be designated to assist the ISSO.

GG. Information Technology (IT) – The Clinger-Cohen Act defines information technology (IT) as any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an Executive agency. For purposes of the preceding definition, "equipment" refers to that used by any DHS Component or contractor, if the contractor requires the use of such equipment in the performance of a service or the furnishing of a product in support of DHS. The term "information technology" includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources. The term "information system," as used within this policy document, is equivalent to the term "IT system."

HH. Insider Threat – One or more individuals with access and/or insider knowledge that allows them to exploit vulnerabilities of the Nation's transportation systems with intent to cause harm. This includes direct risks associated with TSA's security programs and operations, as well as the indirect risks that may compromise our critical infrastructure. For purposes of the TSA *Insider Threat Program*, insiders are, or present themselves to be, current or former transportation sector employees, contractors, or partners who have or have had authorized access to transportation sector facilities, operations, systems, and information.

II. IT Asset – Any IT component owned and operated by the TSA, including assets located at non-TSA facilities and non-TSA owned assets hosting TSA data. TSA IT Assets include, but are not limited to: workstations, laptop computers, infrastructure devices (switches, routers, firewalls, etc.), software (individual and enterprise), firmware, peripheral Devices (USB drives, USB microphones, keyboards, etc.), wireless mobile device, and MEM.

JJ. Inter-zone communication – The flow of information which occurs between two or more zones. Inter-zone communication may include adjacent or non-adjacent zones.

KK. Intra-zone communication – Communication that occurs between two or more nodes (or hosts) within the same zone.

LL. Land Mobile Radio (LMR) – A wireless communications system intended for use by terrestrial users in vehicles or on foot. LMRs can be part of independent systems, primarily using radio frequency (RF) or interconnected using a public switched telephone network or cellular network.

MM. Major Application (MA) – A MA is an automated information system (AIS) that OMB Circular A-130 defines as requiring "…special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application." All Federal applications require some level of

protection. Certain applications, because of the information they contain, however, require special management oversight and classification as MAs. An MA is distinguishable from a GSS by the fact that it is a discrete application, whereas a GSS may support multiple applications. Each MA is under the direct oversight of a Component CISO or an ISSM and has an ISSO assigned.

NN. Media Disposition – Final stage of the SELC; the steps taken to determine whether or how data should be destroyed or maintained for residual value.

OO. Melt – A physically destructive method of sanitizing media; to be changed from a solid to a liquid state generally by the application of heat. (NIST SP 800-88, Guidelines for Media Sanitization)

PP. Metadata – Data that provides information about other data.

QQ. Minor Application (MiA)- An application, other than a major application, that requires attention to security due to the risk and magnitude resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Must be certified and accredited separately. The factors in determining if an application is a minor one on a particular GSS or within a MA are the following: Percentage of controls inherited from GSS or MA: If over 80% of the Low, Moderate, or High baseline security controls (including enhancements) of a software application and associated database(s) are deemed to be inherited or partially inherited (this is known as Hybrid controls), the application is deemed to be minor. The minor application takes advantage of common controls from the hosting system where applicable. As stated in NIST SP 800-37 Rev 1 regarding software applications; additional application-level security controls are provided by the respective software applications as needed. Application owners coordinate with system owners to ensure that information security and risk management activities are carried out as seamlessly as possible among applications and hosting systems. At a minimum, data owners shall state in the security plan if the hosting system has the security controls in the following control families implemented at the application and database levels: AC, AU, IA, SI, RA, SC, CM, AT, IR. Tailoring by data owners and the respective ISSOs may occur, as deemed necessary, including leveraging assurance controls in Appendix E of NIST SP 800-53 Rev. 1 (page E-3). See *Security Authorization (SA)* document for additional details.

RR. Mission Essential System (MES) -- an information system (as defined in the Clinger–Cohen Act) that a Component Head or designee determines is necessary to perform one or more of its Mission Essential Functions.

SS. Mobile Electronic Media (MEM) – A type of IT asset with electronic media with persistent memory that can be used to store electronic representations of information/data other than that which is structurally internal to typical computational platforms (wireless mobile device, laptops, workstations, or other device with persistent memory).

TT. Multi-homed/Dual-Homed – Any device (server, workstation, firewall, IDS/IPS, network connected copier, scanner, etc.), that is configured with more than one Internet Protocol (IP) address and/or multiple network interface cards (NICs). In other words, a device that is connected to two or more networks or having two or more network addresses.

UU. Multi-homing – A device or host with two or more active IP (v4 or v6) data links or connections. These links may be separate physical connections or linked through a single physical connection with two or more logical connections. Loopback interfaces using

127.0.0.0/24 or: 1 addresses do not represent an interface with regard to multi-homing as they are not associated with a physical interface.

VV. National Intelligence Information – The following definition is provided in *Public Law 108-458, Intelligence Reform and Terrorism Prevention Act of 2004*, December 17, 2004, "The terms 'national intelligence' and 'intelligence related to national security' refer to all intelligence, regardless of the source from which derived and including information gathered within or outside the United States, that – "(A) pertains, as determined consistent with any guidance issued by the President, to more than one United States Government agency; and (B) that involves – (i) threats to the United States, its people, property, or interests; (ii) the development, proliferation, or use of weapons of mass destruction; or (iii) any other matter bearing on United States national or homeland security."

WW. National Security Information – Information that has been determined, pursuant to Executive Order 13526, *Classified National Security Information*, or any predecessor order, to require protection against unauthorized disclosure.

XX. Network Address Translation (NAT) – The process of modifying network address information in datagram (IP) packet headers while in transit across a traffic routing device for the purpose of remapping one IP address space into another. For example, IP traffic originating from a computer using a private IP address of 10.0.0.1 can be translated to appear to be a different, public IP address to allow connectivity to the internet.

YY. Network Interface Card (NICs) – A physical component attached to a computing device that provides a physical interface allowing network connectivity. NICs can be simulated in virtual environments and are referred to as "virtual NICs." Also known as network adapter.

ZZ. Network Zone – A segment of a network which is isolated and protected from all other network segments by physical security devices, physical and logical access controls, and/or other measures to protect and control the flow of data

AAA. Operational Data – Operational data is information used in the execution of any DHS mission.

BBB. Personally Identifiable Information (PII) – PII is any information that permits the identity of an individual to be directly or indirectly inferred, including any information which is linked or linkable to that individual regardless of whether the individual is a U.S. Citizen, lawful permanent resident, a visitor to the U.S., or employee or contractor to the Department.

CCC. Policy Enforcement Point (PEP) – A Trust Zone policy enforcement point (PEP) is the edge of trust boundary in which all policy decisions are made with regard to connections to and from the TSA Trust Zone. Examples of the types of policies and protections a Component requires at a Trust Zone include email, Web applications, and system applications. At a minimum the PEP shall evaluate traffic and permit inbound & outbound IP netblocks, specific Internet protocol (IP) addresses, and ports based on a set of rules established by TSA.

DDD. Port Address Translation (PAT) – Translation of TCP or UDP communications made between hosts on a private network and hosts on a public network. PAT allows a single public IP address to be used by multiple hosts on a private network.

EEE. Pristine – The state of data on a medium being free from change, compromise, or any other alteration relative to its original state. Pristine data (often installation media and files) is

logically identical to the state it was in when it was published by a vendor, certified as authorized for use, or otherwise formally approved for use or installation.

FFF. Privacy Sensitive System – A Privacy Sensitive System is any system that collects, uses, disseminates, or maintains PII or Sensitive PII.

GGG. Proxy - An application that "breaks" the connection between client and server. The proxy accepts certain types of traffic entering or leaving a network and processes it and forwards it.

HHH. Public Information – This type of information can be disclosed to the public without restriction but requires protection against erroneous manipulation or alteration (e.g. Public Web sites).

III. Pulverize – A physically destructive method of sanitizing media; the act of grinding to a powder or dust. (NIST SP 800-88, Guidelines for Media Sanitization)

JJJ. Purge – A sanitization type that removes all data and any remnants of the data so thoroughly that recovering the data with sophisticated tools in a laboratory setting (Laboratory Attack) would not be possible. (NIST SP 800-88, Guidelines for Media Sanitization)

KKK. Restricted Zone – An internal zone that is protected from un-trusted zones by a minimum of one semi-trusted zone and one trusted zone. The restricted zone is designed to house systems

LLL. Sanitization – Process to remove information from media such that data recovery is not possible. It includes removing all classified labels, markings, and activity logs.

MMM. Sanitization Method – The specific process and steps by which a type of sanitization is carried out. Melting is a type of destruction. Writing bits of data multiple times across the same media is a form a clearing.

NNN. Sanitization Type – A category or grouping of information removal methods, which end in the same result. The three sanitization types, in order of effectiveness from least to greatest are: Clearing, Purging, and Destruction.

OOO. Security Categorization – The process of determining the security category for information or an information system based on an assessment of the potential impact that a loss of Confidentiality, Integrity, or Availability of such information or information system would have on organizational operations, organizational assets, or individuals. Security categorization methodologies are described in FIPS 199 for other than national security systems.

PPP. Security Control Assessor – A senior management official who certifies the results of the security control assessment. He or she must be a Federal Government employee.

QQQ. Semi-Trusted Zone – A semi-trusted zone, also a form of DMZ, resides between an un-trusted zone or zones and a trusted zone or zones. Un-trusted (commonly internet) facing services such as web services, VPN services, and proxy servers reside in this zone.

RRR. Sensitive Information – Sensitive information is information not otherwise categorized by statute or regulation that if disclosed could have an adverse impact on the welfare or privacy of individuals or on the welfare or conduct of federal programs or other programs or operations essential to the national interest. Examples of sensitive information include personal data such as Social Security Numbers; trade secrets; system vulnerability

information; pre-solicitation procurement documents, such as statements of work; and law enforcement investigative methods; similarly, detailed reports related to computer security deficiencies in internal controls are also sensitive information because of the potential damage that could be caused by the misuse of this information. System vulnerability information about a financial system shall be considered Sensitive Financial Information. All sensitive information must be protected from loss, misuse, modification, and unauthorized access. With the exception of certain types of information protected by statute (e.g. Sensitive Security Information, Critical Infrastructure Information), there are no specific Federal criteria and no standard terminology for designating types of sensitive information. Such designations are left to the discretion of each individual Federal agency. "For Official Use Only" (FOUO) is the term used within DHS to identify unclassified information of a sensitive nature that is not otherwise categorized by statute or regulation. DHS shall be adopting the term "Controlled Unclassified Information (CUI)" at a later date.

SSS. Sensitive Personally Identifiable Information (SPII) – Sensitive PII is PII which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Examples of Sensitive PII include Social Security Numbers, alien number (A-number), criminal history information, and medical information. Sensitive PII requires stricter handling guidelines due to the sensitivity of the information.

TTT. Shred – A method of sanitizing media; the act of cutting or tearing into small particles. (NIST SP 800-88, Guidelines for Media Sanitization)

UUU. Strong Authentication – Strong authentication is a layered authentication approach relying on two or more authenticators to establish the identity of an originator or receiver of information. Typically, strong authentication requires authenticators that are resistant to replay attacks and employ multifactor authentication. Strong authenticators include, for example, PKI where certificates are stored on a token protected by a passcode, passphrase, or biometric.

VVV. Supply Chain - A system's supply chain is composed of the organizations, people, activities, information, resources, and facilities for designing, creating and moving a product or service from suppliers through to the integrated system (including its sub-components), and into service by the original acquirer.

WWW. System Owner (SO) – Agency official or program manager responsible for the overall procurement, development, integration, modification, operation, maintenance and/or final disposition of an information system, software and/or applications who use information technology to help achieve the mission needs within their program area of responsibility. The SO is responsible and accountable for the successful operation and security of the information system and programs within their program area. All systems require a System Owner designated in writing for proper administration of security.

XXX. Trusted Internet Connection (TIC) - Boundary protection zone between DHS and external networks, which is implemented by firewalls at the TIC and other approved direct system inter-connections. DHS TIC are provided by OneNet and monitored by the DHS ESOC. Component SOCs may protect DHS-internal boundaries across Trust Zones. The TIC is a DHS entity entrusted in providing a more centrally managed Semi-Trusted and DMZ

environment. The TIC optimizes and standardizes the security of individual external network connections (extranet services) currently in use by Components and other agencies.

YYY. Trusted Zone (Trust Zone) – A trusted zone resides behind a semi-trusted zone and is separated by layers physical and logical access controls from the un-trusted networks. A trusted zone is designed to provide front-end services (restricted, trusted, semi-trusted zones only) for clients and servers on different zones. The trusted zone often hosts intranet services such as intranet websites and applications.

ZZZ. Two-Factor Authentication – Authentication can involve something the user knows to include: a passcode, something the user has like a smart card, or something the user "is" to include a fingerprint or voice pattern. Single-factor authentication uses only one of the three forms of authentication, while two-factor authentication uses any two of the three forms. Three-factor authentication uses all three forms.

AAAA. Un-trusted Zone – A zone over which the TSA does not have administrative authority or technical control and/or does not have a contractual, binding agreement in place such as an Intersystem Security Agreement (ISA).

BBBB. Virtual Guest Operating System (OS) – A single instance of an OS and its applications. Guest OSs may be client or server operating systems such as Windows- and Unix-based platforms. Also known as "Guest OS."

CCCC. Virtual Host – The hardware which runs the hypervisor and/or virtual management monitors (VMM) and provides virtualization services. In some cases, a hypervisor runs on top of another operating system and is known as the "host" operating system. In the context of virtualization, it is referred to only as the "host."

DDDD. Virtual Management Monitor (VMM) – Also known as a hypervisor: it controls the flow of instruction between guest OSs and the physical hardware, such as CPU, disk storage, and memory.

EEEE. Virtual Private Network – Protected information system links utilizing tunneling, security controls, and endpoint address translation giving the impression of a dedicated line.

FFFF. Virtualization – The simulation of the software and/or hardware upon which other software runs (as defined by the NIST). A common implementation is described as a process by which a physical server and its components are shared with multiple heterogeneous operating systems.

GGGG. Vital Records – Electronic and hardcopy documents, references, records, databases, and information systems needed to support essential functions under the full spectrum of emergencies. Categories of these types of records may include:

1. *Emergency operating records* – emergency plans and directive(s), orders of succession, delegations of authority, staffing assignments, selected program records needed to continue the most critical agency operations, as well as related policy or procedural records.
2. *Legal and financial rights* records – protect the legal and financial rights of the government and of the individuals directly affected by its activities. Examples include accounts receivable records, social security records, payroll records, retirement records, and insurance records. These records were formerly defined as "rights-and-interests" records.

3. *Records used to perform national security preparedness functions and activities (E.O. 12656).*

HHHH. Waivers – Temporary dispensation of a policy requirement, granted to a Component to operate a system while working toward compliance.

IIII. Zone – A physical or logical area of administration separated or apportioned into sections. Zones typically are a set of objects that a subject is allowed to access. All objects and subjects within this area share a common security policy and procedures and are controlled by the same management domain.

6. Abbreviations

Abbreviations	Full Terminology
AC (FAMILY)	Access Control
ACL	Access Control List
AO	Authorizing Official
AOI	Alerts of Interest
API	Application Programming Interface
AT (FAMILY)	Awareness and Training
ATM	Asynchronous Transfer Mode
ATO	Authorization to Operate
AU (FAMILY)	Audit and Accountability
C&A	Certification and Accreditation
CA (FAMILY)	Assessment, Authorization and Monitoring
CAA	Controlled Access Area
CAA	TSA Form 1403 Computer and Personal Electronic Device Access Agreement
CCE	Common Configuration Enumeration
CD	Compact Disk
CD-R	Compact Disk-Recordable
CD-ROM	Compact Disk-Read Only Memory
CD-RW	Compact Disk-Rewriteable
CFO	Chief Financial Officer
C.F.R.	Code of Federal Regulation
CI	Configuration Item
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CM (FAMILY)	Configuration Management
CMP	Configuration Management Plan
CO	Certifying Official
COMSEC	Communications Security
CONOPS	Concept of Operations
CONUS	Continental United States
COOP	Continuity of Operations Plan
COR	Contracting Officer Representative
COTS	Commercial-Off-The-Shelf
CP	Contingency Plan

CP (FAMILY)	Contingency Planning
CPE	Common Platform Enumeration
DDOS	Distributed Denial of Service
DHS	Department of Homeland Security
DMZ	Demilitarized Zone
DNS	Domain Name Server
DNSSEC	DNS Security Extensions
DOS	Denial of Service
DSL	Digital Subscriber Line
DVD	Digital Versatile Disc
EAP	Extensible Authentication Protocol
E.O.	Executive Order
EOI	Event of Interest
ESOC	Enterprise Security Operations Center
FAM	Foreign Affairs Manual (State Department)
FDCC	Federal Desktop Core Configuration
FedRAMP	Federal Risk and Authorization Management Program
FICAM	Federal Identity, Credential and Access Management (US CIO)
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
FOIA	Freedom Of Information Act
FOUO	For Official Use Only
GFE	Government Furnished Equipment
GMT	Greenwich Mean Time
GOTS	Government Off the Shelf
GPO	Group Policy Object
GSS	General Support System
HIDS	Host-based Intrusion Detection System
HIPS	Host-based Intrusion Prevention System
HSAR	Department of Homeland Security (DHS) Acquisition Regulation
HVA	High Value Asset
IA	Information Assurance
IA (FAMILY)	Identification and Authentication
IACS	Information Assurance Compliance System
IAD	Information Assurance and Cybersecurity Division

IATO	Interim Authorization to Operate
ID	Identification
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IG	Inspector General
INFOSEC	Information Security
IO	Information Owner
IOS	Internetworking Operating System
IP (FAMILY)	Individual Participation
IP	Internet Protocol
IPSec	Internet Protocol Security
IPS	Intrusion Prevention Systems
IR	Incident Response
IR (FAMILY)	Incident Response
IS	Information System
ISA	Interconnection Security Agreement
ISDN	Integrated Services Digital Network
ISOO	Information Security Oversight Office
ISP	Internet Service Provider
ISRA	Information Security Restricted Area
ISSO	Information System Security Officer
ISVM	Information Security Vulnerability Management
IT	Information Technology
ITAR	Information Technology Acquisition Review
ITSP	Information Technology Security Policy
L2TP	Layer Two Tunneling Protocol
LAN	Local Area Network
LE	Local Element
MA	Major Application
MA (FAMILY)	Maintenance
MAC	Media Access Control
MAM	Mobile Applications Management
MBI	Moderate Risk Background Investigation
MD	Management Directive
MDM	Mobile Device Management

MEM	Mobile Electronic Media
MES	Mission Essential System
MEO	(TSA) Microsoft Engineering and Operations
MiA	Minor Application
MO disks	Magneto Optical disks
MP (FAMILY)	Media Protection
NARA	National Archives and Records Administration
NDA	Non-Disclosure Agreement
NIAP	National Information Assurance Partnership
NIDS	Network Intrusion Detection System
NISPOM	National Industrial Security Program Operating Manual
NIST	National Institute of Standards and Technology
NIST SP	NIST Special Publication
NOC	Network Operations Center
NPE	Non-Person Entity
NSA	National Security Agency
OA	Ongoing Authorization
OCA	Original Classification Authority
OMB	Office of Management and Budget
OPSEC	Operations Security
OTA	Over-the-Air
OWASP	Open Web Application Security Project
PA (FAMILY)	Privacy Authorization
PBX	Private Branch Exchange
PE (FAMILY)	Physical and Environmental Protection
PEP	Policy Enforcement Point
PHI	Protected Health Information
PI	Potential Incident
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PL (FAMILY)	Planning
PM (FAMILY)	Program Management
POA&M	Plan of Action and Milestones

PS (FAMILY)	Personnel Security
PSTN	Public Switched Telephone Network
PTA	Privacy Threshold Analysis
RA (FAMILY)	Risk Assessment
RDS	Records Disposition Schedules
RFC	Request for Change
RFID	Radio Frequency Identification
RFP	Request for Proposal
RMS	Remote Management System
ROB	Rules of Behavior
ROM	Read-Only Memory
SA	Security Authorization
SA (FAMILY)	System and Services Acquisition
SAR	Security Assessment Report
SC (FAMILY)	System and Communications Protection
SCCB	Systems Change Control Board
SCRM	Supply Chain Risk Management
SELC	Systems Engineering Life Cycle
SI (FAMILY)	System and Information Integrity
SMG	Software Management Group
SNMP	Simple Network Management Protocol
SO	System Owner
SOC	Security Operations Center
SOC CONOPS	Security Operations Center Concept of Operations
SOP	Standard Operating Procedure
SOW	Statement of Work
SP	Security Plan (Previously System Security Plan or SSP)
SPOC	Single Point of Contact
SSH	Secure Shell
SSI	Sensitive Security Information
SSI IA	SSI Impact Analysis
SSI TA	SSI Threshold Analysis
SSN	Social Security Number
SSR	Significant Security Responsibility
ST&E	Security Testing and Evaluation

STIG	Security Technical Implementation Guide
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TDF	Technical Discussion Forum
TechSP	Technology Solutions Portfolio
TIC	Trusted Internet Connection
TLS	Transport Layer Security
TOC	TSA Operations Center
TRM	(DHS) Technical Reference Model
TS	Technical Standard
TSA	Transportation Security Administration
UCMJ	Uniform Code of Military Justice
U.S.C.	United States Code
URL	Uniform Resource Locator
USB	Universal Serial Bus
US-CERT	United States Computer Emergency Readiness Team
VoIP	Voice over Internet Protocol
VMM	Virtual Machine Monitor
VPN	Virtual Private Network
WAN	Wide Area Network
WCM	Web Content Manager
WMO	(DHS) Wireless Management Office

7. Acknowledgements

This Handbook was developed, updated and maintained by the Information Assurance (IA) Policy team within the Governance, Risk, and Compliance (GRC) Branch under IAD. Much thanks and acknowledgements go out to our IAD Senior Leadership Team; contributing staff members from the GRC, Cybersecurity Awareness and Operational Support (CAOS), Computer Network Defense (CND), Focused Operations (FO), Secure Infrastructure & Vulnerability Management (SIVM), and the Security Operations Center (SOC) teams whose dedicated efforts contributed significantly to this publication.

Special thanks go to IAD Policy team members to include: Carl Shirley, Dan Henry, Sean Fitzgerald and editor Joseph House for leading discussions and working groups on changes, additions, editing and other contributions.

8. Authorities

Authority	Document ID	Document of External Origin? Y/N	Authority Type
E-Government Act of 2002, Public Law 107-347, 116 Stat. 2899, 44 U.S.C. 101	P.L. 107-347	Yes	Mandated
Federal Information Security Modernization Act of 2014, 44 USC, CH 35, Pub L 113-283, 128 Stat 3073	P.L. 113-283	Yes	Mandated
Cybersecurity Information Sharing Act of 2015	P L. 114-113	Yes	Mandated
Presidential Policy Directive 40, "National Continuity Programs"	(PPD-40)	Yes	Mandated
Office of Management and Budget (OMB) Circular A-130, "*Managing Information as a Strategic Resource*," July 27, 2016	OMB A-130	Yes	Mandated
National Archives and Records Administration (NARA) General Records Schedule (GRS) 18	NARA GRS 18	Yes	Mandated
National Institute of Standards and Technology (NIST) Federal Information Processing Standard FIPS 200, "*Minimum Security Requirements for Federal Information and Information Systems*," March 2006	FIPS 200	Yes	Mandated
NIST Special Publications (SP) 800-53 "*Security and Privacy Controls for Federal Information Systems*"	SP 800-53 Rev 4	Yes	Mandated
NIST SP 800-124 "*Guidelines for Managing the Security of Mobile Devices in the Enterprise*"	SP 800-124 Rev 1	Yes	Mandated
DHS 4300A Sensitive System Handbook, Attachment Q1 "*Wireless Systems*"	DHS 4300A Attachment Q1	Yes	Directed
DHS 4300A Handbook, Attachment Q2 "*Mobile Devices*"	DHS 4300A Attachment Q2	Yes	Directed
DHS 4300A handbook, Attachment Q6 "*Bluetooth Security*"	DHS 4300A Attachment Q6	Yes	Directed
DHS Security Architecture Framework, Appendix on Secure *Cloud Computing Guidance*	DHS SAF App SCCG v1	Yes	Directed

DHS Instruction 102-01-103, Systems Engineering Life Cycle.”.	DHS Instruction 102-01-103	Yes	Directed
DHS Directive System MD 140-01, “*Information Technology Security Program*,” May 5, 2017	DHS MD 140-01	Yes	Directed
DHS Sensitive Systems Policy Directive 4300A	DHS 4300A PD	Yes	Directed
DHS Sensitive Systems Policy Handbook 4300A	DHS 4300A Handbook	Yes	Directed
DHS National Security Systems Policy Directive 4300B	DHS 4300B PD	Yes	Directed
Homeland Security Presidential Directive-12 (HSPD-12) PIV	HSPD-12 PIV	Yes	Mandated
TSA MD 1400.3 *Information Technology Security*	TSA MD 1400.3	No	Directed
TSA IT Cloud Computing Security Handbook	TSA IT CCSH	No	Directed

9. Document Change History

Effective	Ver	Summary of Changes	By
06/22/2010	7.0.1	Updated per NIST SP 800-53 R3 and DHS 4300 v7.0 Reformatted	C. Rodriguez
10/25/2011	8.1	Updated per DHS 4300 v.8.0 and DHS TIC/PEP Initiative Reformatted/Additions	A. Deane
12/21/2011	9.0	Updated per DHS 4300 v.9.0 Modified Computer Access Agreement policies to support OLC integration	A. Deane
9/21/2012	9.1	Updated per DHS 4300 v9.1 Updated security controls; Modified the Computer and Personal Electronic Device (PED) Access Agreement policies to support OLC integration; Conducted other updates to include: technical standard references, SOP references, regulatory citations, and added definitions; see matrix (in binder) for general added updates.	C. Rodriguez
02/25/2014	9.2	Added: general content, technical standards, SOPs, abbreviations, removed old reference information, signature block, TSA cloud data via the TIC, clarified non-routine foreign travel, connect TSA laptops to non-GFE peripherals, remove ISSO review of audit logs, move audit log review to the SOC, add requirement of Moderate or higher for Integrity on SSI systems to be in line with SSI Policies and Procedures and SSI/IAD prior agreement.	C. Rodriguez
03/18/2014	9.2.1	Conducted a number of updated to include: general content, technical standards, SOPs, FedRAMP, NIST 800-53 Rev 4 controls, mobile policy, mobile applications, ongoing authorizations (OA), continuous diagnostic and mitigation (CDM), abbreviations and remove old reference information.	C. Rodriguez
05/12/2014	9.2.2	Updated password complexity and other minor administrative updates.	S. Jurado
09/29/2015	9.2.3	Incorporated records disposition schedule (RDS) policy reference in the cover page; addressed password/PIN/PIV and username updates; updated references and authorities; conducted general edits; incorporated several new security controls; and updated the signature block. See “Summary Page” for details.	S. Jurado
07/27/2018	14.0	See Summary of Changes (may be provided upon request).	GRC, Policy Team

10. Document Control Information

Doc ID	Doc Owner	Change Approval Authority	Stored	Review	Disposition
TSA IA Handbook	GRC	TSA CISO	Main Site	Annual	RDS Policy Records Code and Item #: 2000.4.1 PERMANENT: Cut off at end of calendar year in which superseded or obsolete. Transfer to NARA 10 years after cut off. [Authority N1-560-04-10, Item 5b]

11. Effective Date and Implementation

Upon signature, this Handbook becomes effective on the date indicated below.

/// Signature on File /// **July 27, 2018**

_____ _____

Paul D. Morris
Executive Director
Chief Information Security Officer
Information Assurance and Cybersecurity Division
Information Technology

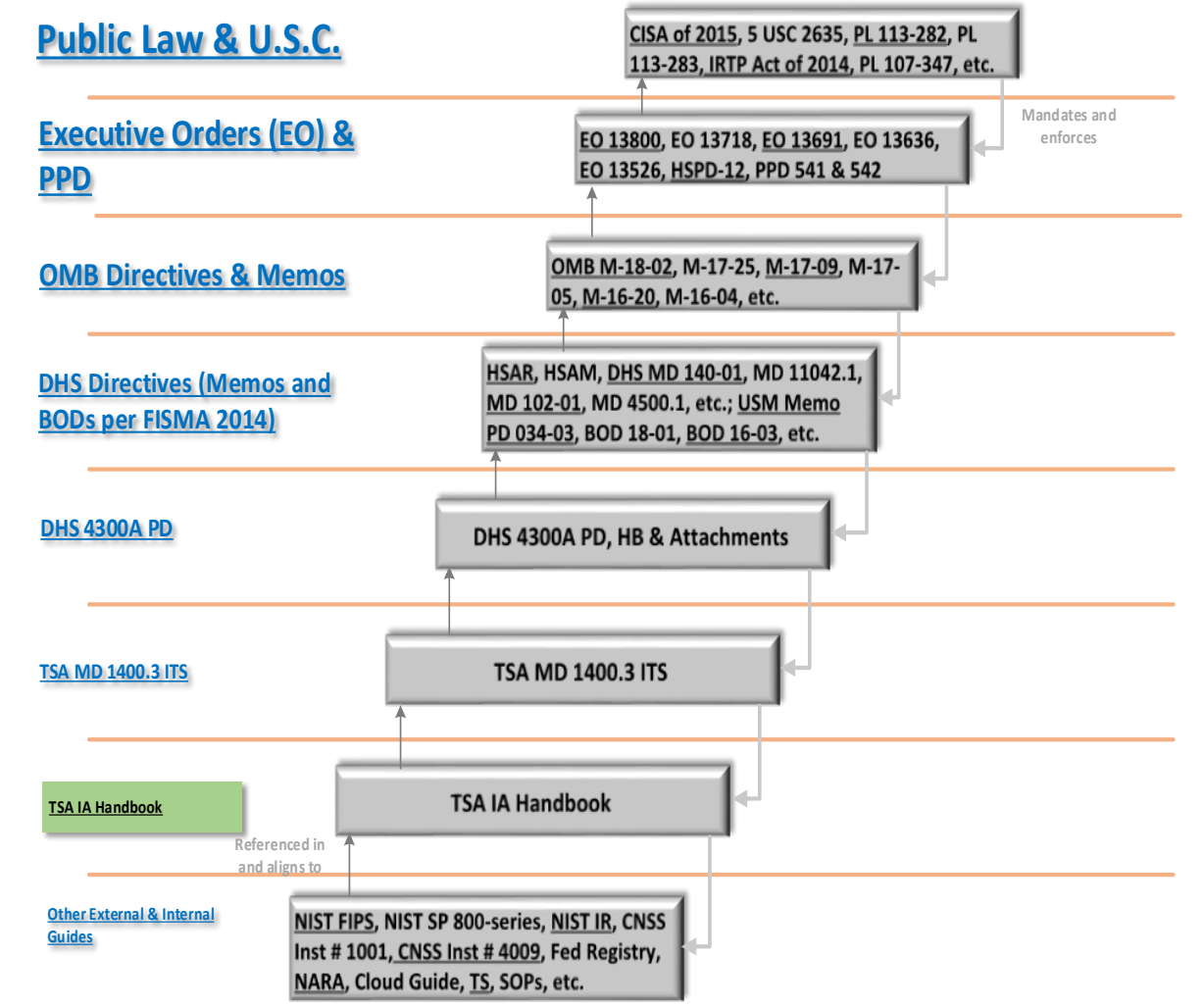
Date

Distribution: TSA Employees, Contractors, and Contracts
Point of Contact: IAD Policy, TSAIADPolicy@tsa.dhs.gov

12. Appendix A - References (Federal Information Assurance (IA) Policy Mandate -- Top-Down Alignment Diagram and Detailed Authorities):

- Public Laws & United States Code (U.S.C.)
- Executive Orders & Presidential Memoranda or Presidential Policy Directives (PPD)
- OMB Directives and Memorandums
- DHS Directives (including USM Memorandums and Binding Operational Directives (BOD) pursuant to FISMA 2014)
- DHS 4300A PD
- TSA MD 1400.3 ITS
- TSA Information Assurance (IA) Handbook
- Other External and Internal Guidance

Figure 1: Cybersecurity Related IA Policy Directive Flowchart (See Appendix A for details)



Detailed Federal Mandates: In order of approval (top-down), our TSA IT IAD Information Assurance (IA) Policy Program and related IA Handbook is derived or aligns with:

- **Public Laws & United States Code (U.S.C.):** After the President signs a bill into law, it is delivered to the Office of the Federal Register (OFR), where editors: assign a *Public Law* Number, prepare it for publication and include it in the next edition of the United States Statutes. *U.S. Code*: The Code of Laws of the United States of America (variously abbreviated as: Code of Laws of the United States, United States Code, U.S. Code, U.S.C., or USC) is the official compilation and codification of the general and permanent federal statutes of the United States. It contains 53 titles (Titles 1-54, except Title 53 is reserved). The main edition is published every six years by the Office of the Law Revision Counsel of the House of Representatives, and cumulative supplements are published annually. The official version of those laws not codified in the United States Code can be found in United States Statutes.
- **Executive Orders, Presidential Memoranda or Presidential Policy Directives (PPD):** The United States president issues directives or executive orders to help officers and agencies of the executive branch manage the operations within the federal government itself. *Presidential memoranda* are closely related and, like executive orders, have the force of law on the Executive Branch, but are generally considered less prestigious. *Presidential memoranda* do not have an established process for issuance or publication and are not numbered - unlike executive orders, which are numbered. *Presidential Policy Directives (PPD)* sets forth principles governing the Federal Government's response to any cyber related incident, whether involving government or private sector entities. For significant cyber incidents, certain PPDs also establishes lead Federal agencies and an architecture for coordinating the broader Federal Government response.
- **OMB Directives and Memorandums**: These directives issue government-wide guidelines to "provide policy and procedural guidance to Federal agencies for ensuring and maximizing the quality, objectivity, utility, and integrity of information (including statistical information) disseminated by Federal agencies." By October 1, 2002, agencies must issue their own implementing guidelines that include "administrative mechanisms allowing affected persons to seek and obtain correction of information maintained and disseminated by the agency" that does not comply with the OMB guidelines.
- **DHS Directives (including USM Memorandums and Binding Operational Directives (BOD) pursuant to FISMA 2014):** *Directives* establishes DHS policy to all DHS organizational elements and is governed by numerous Public Laws, Executive Orders (E.O.), regulations, Presidential Decision Directives (PDD), agency manuals, and Office of Management and Budget (OMB) circulars. DHS *BODs* serves as compulsory directives to federal, executive branch, civilian departments and agencies for purposes of safeguarding federal information and information systems by using proper "cyber hygiene" requirements. DHS develops and oversees the implementation of BODs pursuant to FISMA of 2014. Federal agencies are required to comply with these DHS-developed directives. USM *Memorandums* are used to notify executives, as well as document requirements for heads of executive departments and agencies. The USM directs efforts to, in this case, provide security for information technology and communications systems Department-wide.

- **DHS 4300A PD**: Serves as the official document that articulate Departmental policies, standards, and guidelines in accordance with DHS Directive System 140-01, "Information Technology Security Program. Namely, it articulates the DHS Information Security Program policies for sensitive systems. Procedures for implementing these policies are outlined in a companion publication, DHS 4300A Sensitive Systems Handbook. This Policy Directive and the Handbook serve as the foundation on which Components are to develop and implement their own information security programs.
- **TSA MD 1400.3 ITS**: Provides TSA policy and procedures for the secure use, development, and maintenance of TSA information systems including prototypes and telecommunications. This directive and the TSA Information Assurance Handbook apply to all TSA employees and contractors, as well as TSA-owned or TSA-controlled information systems that collect, generates, process, store, display, transmit, or receive TSA data. This includes prototypes, telecommunications systems, and all systems in all phases of the System Engineering Life Cycle (SELC).
- **TSA IA Handbook**: This handbook implements the policies and requirements of the above mentioned TSA Management Directive (MD) 1400.3, Information Technology Security by establishing guidance applicable to the use, development, and maintenance of TSA Information Technology (IT) assets, networks and systems. The guidance contained herein are designed to ensure the Confidentiality, Integrity, Availability, and overall assurance of TSA information. This handbook is supplemented by published extension documents, TSA Technical Standards (TSs) and Standard Operating Procedures (SOPs). This document is used to identify responsibilities by educating and increasing awareness of TSA information assurance (IA) policy. References to the specific areas and authorities to enable successful execution of tasks and job requirements are identified in the Handbook.
- **Other External and Internal Guidance**: Guidance as provided by internal and outside entities and organizations such as: NIST FIPS, NIST SP, NIST IR, CNSS Instructions, Federal Register and Federal Archives.

List of Relevant Mandates and Links

Public Laws and U.S. Code

- 5 Code of Federal Regulations (CFR) §2635, Office of Government Ethics, "Standards of Ethical Conduct for Employees of the Executive Branch"
- Cybersecurity Information Sharing Act of 2015 (S. 2588)
- Public Law 113-282, National Cybersecurity Protection Act of 2014, Dec 18, 2014
- Public Law 113-283, Federal Information Security Modernization Act of 2014 (FISMA), 128 Stat 3087
- Intelligence Reform and Terrorism Prevention Act of 2004, 118 Stat. 363
- Public Law 93-579, Freedom of Information Act of 2002, as amended, 5 U.S.C 552
- Public Law 107–347, E-Government Act of 2002, 116 Stat. 2899, 44 U.S.C. 101
- Public Law 104-106, *Clinger-Cohen Act* of 1996

- Public Law 100-235, Computer Security Act of 1987, as amended, codified at 40 U.S.C. 759
- Public Law 93-579, Privacy Act of 1974, As Amended. 5 U.S.C 552a, Wash, DC, July 14, 1987

Executive Orders & Presidential Memorandums or Presidential Policy Directives (PPD)

- Presidential Executive Order (EO) 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, May 11, 2017
- Executive Order 13718, "Commission on Enhancing National Cybersecurity", February 9, 2016
- Executive Order 13691, "Promoting Private Sector Cybersecurity Information Sharing", Feb 13, 2015
- Executive Order 13636, "Improving Critical Infrastructure Cybersecurity", February 12, 2013
- Executive Order 13526, "Classified National Security Information," December 29, 2009
- Homeland Security Presidential Directive 12, "Policy for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004
- PPD 541 & 542 – United States Cyber Incident Coordination, July 26, 2016

Office of Management and Budget (OMB) Directives and Memorandums

- OMB Circular A-130, "Management of Federal Information Resources, Transmittal Letter No. 4," 2010
- OMB M-18-12, "Implementation of the Modernizing Government Technology Act", February 27, 2018
- OMB M-18-02, "FY17-18 Guidance on Federal Information Security and Privacy Management Requirements", October 16, 2017
- OMB M-17-27, Assessment and Enforcement of Domestic Preferences in Accordance with Buy American Laws
- OMB M-17-25, "Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure", May 19, 2017
- OMB M-17-09, "Management of Federal High Value Assets", December 9, 2016
- OMB M-17-05, "FY 2016 - 2017 Guidance On Federal Information Security and Privacy Management Requirements", Nov 4, 2016
- OMB M-16-20, "Category Management Policy 16-3: Improving the Acquisition and Management of Common Information Technology: Mobile Devices and Services", August 4, 2016
- OMB M-16-17, OMB Circular No. A-123, "Management's Responsibility for Enterprise Risk Management and Internal Control", July 15, 2016
- OMB M-16-15, "Federal Cybersecurity Workforce Strategy", July 12, 2016

- OMB M-16-12, "Category Management Policy 16-1: Improving the Acquisition and Management of Common Information Technology: Software Licensing", June 2, 2016
- OMB M-16-04, "Cybersecurity Strategy and Implementation Plan (CSIP)", October 30, 2015
- OMB M-15-13, "Policy to Require Secure Connections across Federal Websites and Web Services", June 8, 2015
- OMB M-12-20, "FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," September 27, 2012
- OMB M-10-28, "Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (DHS)," July 6, 2010
- OMB M-09-02, "Information Technology Management Structure and Governance Framework," October 21, 2008
- OMB M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," May 22, 2007
- OMB M-06-16, "Protection of Sensitive Agency Information," June 23, 2006
- OMB M-06-15, "Safeguarding Personally Identifiable Information," May 22, 2006
- OMB M-04-04, "E-Authentication Guidance for Federal Agencies," December 16, 2003
- OMB Bulletin 06-03, "Audit Requirements for Federal Financial Statements," August 23, 2003

DHS Directives (including USM Memorandums and Binding Operational Directives (BOD) pursuant to FISMA 2014)

- Department of Homeland Security Acquisition Regulation (HSAR)
- Homeland Security Acquisition Manual (HSAM)
- DHS Management Directives (MD):
  - MD 140-01, "Information Technology Security Program", May 05, 2017
  - MD 11042.1, "Safeguarding Sensitive but Unclassified (For Official Use Only) Information," January 6, 2005
  - MD 102-01, "Acquisition Management Directive", Amendment 1, Feb 13, 2012
  - MD 1030, "Corrective Action Plans," May 15, 2006
  - MD 4500.1, "DHS Email Usage," March 1, 2003
  - MD 4600.1," Personal Use of Government Office Equipment," April 14, 2003
  - MD 4900, "Individual Use and Operation of DHS Information Systems/Computers"
- DHS USM, OCPO and **BOD Memorandums:**
  - USM Memo PD 034-03, "Continuous Improvement of Department of Homeland Security Cyber Defenses", January 13, 2016
  - USM Memo PD # TBD, "Strengthening DHS Cyber Defenses", July 22, 2015
  - **DHS Office of the Chief Procurement Officer (OCPO) Memo, *Training for Homeland Security Acquisition Regulation Class Deviation 15-01, Safeguarding of Sensitive Information",* HSAR Class Deviation 15-01, Safeguarding of Sensitive**

Information, also known as "Cyber Hygiene." HSAR Class Deviation 15-01, dated March 9, 2015

- BOD Memo 18-01, "Enhance Email and Web Security"
- BOD Memo 17-01, "Removal of Kaspersky Branded Products", Sept 13, 2017
- BOD Memo 16-03, "2016 Agency Cybersecurity Reporting Requirements", October 17, 2016
- BOD Memo 16-02, "Threat to Network Infrastructure Devices", September 27, 2016
- BOD Memo 16-01, "Securing High-Value Assets", June 16, 2016
- BOD Memo 15-01, "Critical Vulnerability Mitigation Requirement for Federal Civilian Executive Branch Departments' and Agencies' Internet-Accessible Systems", July 22, 2015

DHS 4300A Sensitive Systems Policy, v13.1, July 27, 2017 and related Attachments

TSA MD 1400.3 Information Technology Security, April 8, 2014

TSA IT Cloud Computing Handbook v1, September 2017

Other External and Internal Guidance

- National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS), including:
  - NIST FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems," February 2004
  - NIST FIPS 200, "Minimum Security Requirements for Federal Information and Information Systems," March 2006
- NIST Information Technology Security Special Publications (SP) 800 series, including:
  - NIST SP 800-16, "Information Technology Security Training Requirements: A Role- and Performance-Based Model," April 1998
  - NIST SP 800-34, Rev 1, "Contingency Planning Guide for Information Technology Systems," May, 1010, updated November 11, 2010
  - NIST SP 800-37, Rev 1, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach," Feb 2010, updated June 5, 2014
  - NIST SP 800-39, "Integrated Enterprise-Wide Risk Management: Organization, Mission, and Information System View," March 2011
  - NIST SP 800-50, "Building an Information Technology Security Awareness and Training Program," October 2003

- NIST SP 800-52, Rev 1, “Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations,” April 2014
- NIST SP 800-53, Rev 4, “Security and Privacy Controls for Federal Information Systems and Organizations,” April 2013, updated January 22, 2015
- NIST SP 800-53A, Rev 4, “Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans,” December 2014, updated December 18, 2014
- NIST SP 800-60, Rev 1, “Guide for Mapping Types of Information and Information Systems to Security Categories: (2 Volumes) - Vol 1: Guide Volume 2: Appendices,” Aug 2008
- NIST SP 800-63-2, “Electronic Authentication Guideline,” August 2013
- NIST SP 800-65, “Integrating IT Security into the Capital Planning and Investment Control Process (CPIC),” January 2005
- NIST SP 800-88 Rev 1, “Guidelines for Media Sanitization,” December 2014
- NIST SP 800-92, “Guide to Computer Security Log Management,” September 2006
- NIST SP 800-94, “Guide to Intrusion Detection and Prevention Systems (IDPS),” February 2007
- NIST SP 800-95, “Guide to Secure Web Services,” August 2007
- NIST SP 800-100, “Information Security Handbook: A Guide for Manager,” October 2006 (Including updates as of 03-07-2007)
- NIST SP 800-115, “Tech Guide to Info Security Testing & Assessment,” Sep 2008
- NIST SP 800-122, “Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),” April 2010
- NIST SP 800-123, “Guide to General Server Security,” July 2008
- NIST SP 800-124, Rev 1, “Guidelines for Managing the Security of Mobile Devices in the Enterprise,” June 2013
- NIST SP 800-128, “Guide for Security-Focused CM of Info Systems,” August 2011
- NIST SP 800-137, “Information Security Continuous Monitoring for Federal Information Systems and Organizations,” September 2011
- NIST SP 800-160, “Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems,” November 2016
- NIST SP 800-161, “Supply Chain Risk Management Practices for Federal Information Systems and Organizations,” April 2015

- NIST IR 7298 Rev 2, “Glossary of Key Information Security Terms,” May 2013
- CNSS Instruction No. 1001, “Nat’l Instruction on Classified Information Spillage,” Feb 2008
- CNSS Instruction No. 4009 (Revised), “National Information Assurance Glossary,” April 2015
- Federal Register and Federal Archives: National Archives and Records Administration (NARA) General Records Schedule (GRS) 18

- TSA IT Cloud Computing Handbook v1, September 2017
- Internal: Technical Standards (TSs) and Standard Operating Procedures (SOPs)