Homeland Security

DHS National Security Systems:
Control Guidance

Department of Homeland Security
DHS Directives System

Instruction Number: 4300B.102

Version Number: 10.1

Issue Date: 11/21/2018

Chip Fulghum
Deputy Under Secretary for Management

11/21/18
Date

This page intentionally left blank.

Table of Contents

1.0 Purpose 4

2.0 Scope 4

3.0 References 4

4.0 Definitions 4

5.0 Responsibilities 4

6.0 Processes and Procedures 5

7.0 DHS National Security Systems: Control Guidance 7

8.0 Abbreviations and Acronyms 169

1.0 Purpose

This Instruction provides the Department of Homeland Security (DHS) requirements regarding the selection and implementation of the security controls for managing and safeguarding DHS National Security Systems (NSS).

2.0 Scope

This Instruction applies to all DHS elements, employees, contractors, detailees, and others working on behalf of DHS, and users of DHS NSS (referred to collectively in this instruction as the "DHS Components") that collect, generate, process, store, display, transmit, or receive Unclassified, Confidential, Secret, Top Secret, and Special Access Program (SAP) National Security Information (NSI). These NSS include networks, information systems, standalone systems, and applications for which DHS is responsible and has authority, regardless of the physical location.

All DHS NSS and the information they process must be categorized based upon the guidance in Committee on National Security Systems Instruction (CNSSI) 1253, *Security Categorization and Control Selection for National Security Systems*. Using the NSS's categorization, select the appropriate security controls, which identifies the initial security control sets (baselines) for NSS and identifies their applicability by security category value (e.g., Low, Moderate, or High).

3.0 References

For a listing of references that apply to DHS NSS, refer to DHS NSS Policy Standard 4300B.101-2, *National Security System References*.

4.0 Definitions

Definitions specific to NSS are defined in CNSSI 4009*, National Information Assurance Glossary*. The terms, as defined in CNSSI 4009, "safeguarding," "information security," and "information assurance" may be used interchangeably throughout this policy.

5.0 Responsibilities

Refer to National Security Cyber (NSC) Policy Directive 4300B.100, *DHS National Security Cyber Policy*.

6.0 Processes and Procedures

6.1 This Instruction includes the high-level text of each security control from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

6.2 CNSS-defined values for organizationally-defined parameters defined by CNSSI-1253 are shown in bold italics and are identified with the tag "[CNSS]".

6.3 DHS defined values for organizationally-defined parameters defined by DHS are shown in bold italics and are identified with the tag "[DHS]".

6.4 Whenever the parameters for organizationally defined values do not contain DHS or CNSS values, then it is incumbent upon the appropriate Chief Information Security Officer (CISO) or Information System Security Manager (ISSM) to define those values based on mission/business needs.

6.5 The DHS NSS 4300B Policy Series, along with the proper application and documentation of all relevant "-1" baseline controls, CNSS, and DHS defined values, supplemental guidance, and any inheritable network or enterprise controls provide the basis for satisfying all "-1".

6.6 Within the table, there are nine columns for the three security objectives (e.g., confidentiality, integrity, and availability) and three for the possible values (e.g., high, moderate, or low).

- An "X" within one of these columns signifies the security control allocated to that security objective and at what value(s).

- A blank column signifies that a security control is not allocated.

6.7 A security control may be:

(1) Common – Inherited from the organization, environment, or infrastructure where the system is intended to operate;

(2) System Specific – The responsibility of the Information System Owner (ISO)/Program Manager (PM); or

(3) Hybrid – A portion of the control is Common and a portion is System Specific.

6.8 Security control designations must be reviewed for each information system as the environment of operation may vary from system to system. A control that may be Common for one information system may be System Specific for another, or may not apply.

Security controls shall be documented in the Security Control Traceability Matrix (SCTM), which can be created from the table below by deleting those rows associated with impact values that do not apply to the NSS. This provides the baseline set of security controls applicable to the NSS which may require additional tailoring and/or supplementing based on other factors such as the information system usage, information owner requirements, or the environment. This is especially true for tactical systems, stand-alone systems, embedded systems, and others.

Security controls that did not have NSS-assigned impact value were removed from this baseline set of controls. However, if necessary, all controls can be tailored back in with justification.

If a security control identified in the baseline set of controls is tailored out, an explanation must be provided in the SCTM, describing the rationale as to why the control does not apply or how it is satisfied by other mitigating factors. This can be accomplished by adding a "Comments" column to the SCTM. The SCTM can be included as an appendix to an NSS System Security Plan (SSP).[1]

6.10 To enhance cybersecurity, the security control baseline includes the Framework Core from the NIST Cybersecurity Framework. This inclusion stems from Executive Order No. 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (April 16, 2018). Executive Order 13800 requires the Federal Government to implement the NIST *Framework for Improving Critical Infrastructure Cybersecurity*, also known as the *Cybersecurity Framework* or the *NIST Framework*.

The Framework enables organizations to apply the principles and best practices of risk management to improve security and resilience. The Framework Core is a set of cybersecurity activities, desired outcomes, and applicable references. The Core presents industry standards, guidelines, and practices, in a manner that allows for communication of cybersecurity activities and outcomes across the organization from the executive level to the implementation/operations level. The Framework Core consists of five concurrent and continuous Functions: (1) Identify, (2) Protect, (3) Detect, (4) Respond, and (5) Recover. These Functions provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk.

[1] For guidance on SSPs for DHS NSS, refer to NSS Policy Standard 4300B.103-1, *Template for System Security Plans*.

The Cybersecurity Framework controls are highlighted in the color purple and also have an asterisk by the Cybersecurity Framework Subcategory/Control ID in the Systems Control Guidance table below. These cybersecurity controls are applicable for all security categorization values and must be included in the baseline.

6.11 In addition to the security controls documented in the SCTM, as stated in 4300B, overlays derived from CNSS, NIST, and the Joint Special Access Program (SAP) Cybersecurity (JSCS) Implementation Guide have been provided on the NSCD SharePoint site for further security control enhancement. The available overlay address; Classified, Standalone, Cross Domain Solution (CDS), Isolated Local Area Network (LAN), Privacy and Industrial Control Systems (ICS).

6.12 Any changes to the baseline security control selections or designation must be addressed in the SCTM, and must be approved by the assigned Authorizing Official (AO), Information System Owner (ISO), Information System Security Manager (ISSM), Information System Security Officer (ISSO), the Risk Executive Function (REF), and the assigned Security Control Assessor (SCA).

6.13 The DHS Privacy Office (PRIV) reviews and approves all privacy controls which should not be confused with the Privacy Overlay, which are additional controls to be applied to applicable security controls that are not privacy related.

7.0 DHS National Security Systems: Control Guidance

See table below

DHS National Security Systems: Control Guidance

Access Control (AC)

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
AC 1 Protect Function: PR.AC 1, PR.AC 3, PR.AC 4, PR.AC 6*	Access Control Policy and Procedures	X	X	X	X	X	X	X	X	X	The organization: a. Develops, documents, and disseminates *to **all personnel*** **[DHS]**: 1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the access control policy and associated access controls; and b. Reviews and updates the current: 1. Access control *policy* ***at least annually if not otherwise defined in formal organizational policy*** **[CNSS]**; and 2. Access control procedures ***at least annually if not otherwise defined in formal organizational policy*** **[CNSS]**.	The DHS NSS 4300B Policy, along with the proper application and documentation of all relevant (AC) baseline controls, CNSS and DHS defined values, supplemental guidance, and any inheritable network or enterprise controls provide the basis for satisfying AC 1. However, the ISO is ultimately responsible for addressing any and all (AC) policy and procedures within the SSP. References: DHS NSS General User and Privileged User Agreement Templates.
AC 2 Protect Function: PR.AC 1, PR.AC 4, PR.AC 6* Detect Function; DE.CM 1, DE.CM 3*	Account Management	X	X	X	X	X	X				The organization: a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: ***e.g. individual, group, system, application, guest/anonymous, and temporary*** **[DHS]**; b. Assigns account managers for information system accounts; c. Establishes conditions for group and role membership; d. Specifies authorized users of the information system, group and role membership, and access authorizations (e.g., privileges) and other attributes (as required) for each account; e. Requires approvals by ***Supervisors*** **[DHS]** for requests to create information system accounts; f. Creates, enables, modifies, disables, and removes information system accounts in accordance with ***organization/component defined procedures or conditions*** **[DHS]**; g. Monitors the use of information system accounts; h. Notifies account managers: 1. When accounts are no longer required;	**Account Creation:** Individual user identifiers (USERIDs) are used on DHS NSS information systems. The CISO/ISSM or designee is the official authorized to issue the initial USERID and password to each user of the system. Documented supervisor approval must be obtained for each individual requiring Information System (IS) access prior to account creation. The supervisor must ensure all individual access requests are valid and access is work related. Prior to granting access to any information system, the CISO/ISSM or System Administrator responsible for account creation and/or changes to access permissions shall verify the user to whom access is being granted is appropriately cleared and indoctrinated to all levels of information that will be accessible, and are in compliance with personnel security requirements. This verification shall be done via the local Security Manager, Special Security Officer (SSO), or SAP/Security Assessment Report (SAR) PM as applicable. In addition, the CISO/ISSM or SA responsible for account creation shall ensure that only accesses and privileges validated by the requestor's supervisor are granted **Group Accounts** In general, group accounts are prohibited. Authorizing Official(s) shall avoid situations in which the group account/authenticator is effectively the sole access control mechanism for the system.

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
											2. When users are terminated or transferred; and 3. When individual information system usage or need to know changes; i. Authorizes access to the information system based on: 1. A valid access authorization; 2. Intended system usage; and 3. Other attributes as required by the organization or associated missions/business functions; j. Reviews accounts for compliance with account management requirements ***at least annually*** **[DHS]**; and k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.	However, use of group accounts/authenticators for broader access after the use of a unique authenticator for initial identification and authentication carries much less risk. The use of group accounts/authenticators shall be explicitly authorized by the AO or designated representative and shall be documented in the SSP. **System Accounts** System accounts shall not be added to any general user groups and shall not have general user rights assigned to them. **User Account Disabling/Deletion** All password accessible accounts must be disabled when information system users are terminated, transferred, or no longer require access to the information resource in the performance of their assigned duties. Accounts that are inactive for forty five (45) days shall be disabled automatically by the IS. Accounts where the user has lost their security clearance will be disabled immediately. Each password accessible account shall be archived when a user no longer has an authorized need to use the account or has not accessed it for one hundred eighty (180) days. Exceptions to this policy may be granted by the CISO and/or ISSM on a case by case basis when a user is away for an extended period of time, but is expected to return. Examples include, but are not limited to, medical leave, personnel deployments and reserve duty assignments. Organizations must ensure that information deemed to be of value is retained before the user s accounts are deleted. **User Access Agreement** The User Access Agreement shall be retained by the CISO/ISSM/SA for a minimum of one (1) year after access is removed
AC-2(1)	Automated System Account Management	X	X		X	X					The organization employs automated mechanisms to support the management of information system accounts.	
AC-2(2)	Account Management Removal of Temporary / Emergency Accounts	X	X		X	X					The information system automatically disables temporary and emergency accounts after ***not to exceed 72 hours*** **[CNSS]**.	**Temporary/Emergency Accounts** The CISO and/or ISSM must approve the creation of temporary or emergency accounts. Temporary and emergency accounts may be for one-time use or for a very limited time period. The ISSO/SA must be notified when temporary or emergency accounts are no longer needed. Temporary and emergency accounts shall be used for no more than 72 hours, and shall be automatically terminated.

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
												Exceptions to this must be approved by the AO or designee for certain situations such as blue/red team assessments, exercises, and test systems.
AC-2(3)	Account Management Disable Inactive Accounts	X	X		X	X					The information system automatically disables inactive accounts after ***not to exceed forty-five (45) days*** **[DHS].**	
AC-2(4)	Automated Audit Actions	X	X	X	X	X	X				The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and ***notifies the ISSO/ISSM*** **[DHS]**.	
AC-2(5)	Account Management Inactivity Logout	X	X	X	X	X	X	X	X	X	The organization: a. Requires that users log out ***at the end of the users standard work period unless otherwise defined in formal component level policy*** **[CNSS]**.	
AC-2(7)	Account Management Role-Based Schemes	X	X	X	X	X	X				The organization: a. Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles; and b. Monitors privileged role assignments. c. ***Disables (or revokes) privileged user accounts*** **[CNSS]** when privileged role assignments are no longer appropriate. d. Implement ***Role Based Access Control (RBAC) to restrict users to the data they are authorized to access and manage*** **[CNSS]** ***(CNSSD 504 Annex A Section 2)***.	
AC-2(9)	Account Management Restrictions On Use Of Shared / Group Accounts	X	X	X	X	X	X				The organization only permits the use of shared/group accounts that meet: ***DHS Policy does not permit shared group accounts. However, if required based on an***	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
											organization's mission, a documented justification must be referenced in the SSP **[DHS]**.	
AC-2(10)	Account Management Group Account Credential Termination	X	X	X	X	X	X				The information system terminates shared/group account credentials when members leave the group.	
AC-2(11)	Account Management Usage Conditions	X			X						The information system enforces Organizational/Component mission specific conditions or circumstances under which information system accounts can be used, for example, by restricting usage to certain days of the week, time of day, or specific durations of time.	
AC-2(12)	Account Management Account Monitoring / Atypical Usage	X	X	X	X	X	X				The organization: a. Monitors information system accounts for ***atypical usage*** **[DHS]**; and b. Reports atypical usage of information system accounts to ***Component or DHS Headquarters Security Office pursuant to DHS Instruction 262-05-002*** **[DHS]**.	
AC-2(13)	Account Management Disable Accounts For High-Risk Individuals	X	X	X	X	X	X				The organization disables accounts of users posing a significant risk within ***30 minutes unless otherwise defined in formal organizational policy*** **[CNSS]** of discovery of the risk.	
AC 3 Protect Function: PR.AC 4,	Access Enforcement	X	X	X	X	X	X				The information system enforces approved authorizations for logical access to the system in accordance with applicable access control policies.	

					I						Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
PR.AC 6, PR.PT 3*												
AC-3(4)	Access Enforcement Discretionary Access Control	X	X	X	X	X	X				The information system enforces ***organization-defined discretionary access control guidance*** **[DHS]** over defined subjects and objects where the guidance specifies whether a subject has been granted access to information can do one or more of the following: a. Pass the information to any other subjects or objects; b. Grant its privileges to other subjects; c. Change security attributes on subjects, objects, the information system, or the information system's components; d. Choose the security attributes to be associated with newly created or revised objects; or e. Change the rules governing access control.	
AC 4 Protect Function: PR.AC 5, PR.DS 5, PR.PT 4* Detect Function: DE.AE 1* Identify	Information Flow Enforcement	X	X		X	X					The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on the ***DHS Information And Data Flow Guidelines Version 2.0*** **[DHS]**.	

					I						Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
Function: ID.AM 3*												
AC 5 Protect Function: PR.AC 4, PR.DS 5*	Separation of Duties	X	X	X	X	X	X				The organization: a. Separates duties ***of individuals as necessary, to prevent malicious activity e.g., system management, systems programming, configuration management, quality assurance and testing, database management, and network security)*** **[DHS]**; b. Documents separation of duties of individuals; and c. Defines information system access authorizations to support separation of duties.	Components shall separate duties of individuals with information system access to prevent malicious activity; document separation of duties; and implement separation of duties through assigned information system access authorizations. Examples of separation of duties include, but are not limited to: •Mission functions and distinct information system support functions are divided among different individuals/roles. •Different individuals perform information system support functions. •Different administrator accounts for different roles, e.g., system administration, security administration, database administration. At a minimum, System Administrators shall not also perform security audit administration functions. Exceptions to the requirement for separation of duties must be documented in the SSP and approved by the AO or designee. Refer to National Information Assurance Partnership (NIAP), mandated by Committee on National Security Systems Policy (CNSSP) Number 11
AC 6 Protect Function: PR.AC 4, PR.DS 5*	Least Privilege	X	X	X	X	X	X				The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
AC-6(1)	Least Privilege Authorize Access To Security Functions	X	X	X	X	X	X				The organization explicitly authorizes access to ***privileged functions (e.g., System Administrator, Security Administrator, Database Administrator (DBA))*** **[DHS]**.	
AC-6(2)	Least Privilege Non-Privileged Access For Non-Security Functions	X	X	X	X	X	X				The organization requires that users of information system accounts, or roles, with access to ***privileged functions*** **[CNSS]** use non-privileged accounts, or roles, when accessing non privileged functions.	
AC-6(3)	Least Privilege Network Access To Privileged Commands	X			X						The organization authorizes network access to ***organization/component-defined privileged commands only for defined compelling operational needs pursuant to the DHS Integrating Identity Management into Systems and Applications Appendix version 1.0*** **[DHS]** and documents the rationale for such access in the security plan for the information system.	
AC-6(5)	Least Privilege Privileged Accounts	X	X	X	X	X	X				The organization restricts privileged accounts on the information system to [***organization-defined personnel or roles***].	***4300B.106 NSS Privileged User Template***
AC-6(7)	Least Privilege Review Of User Privileges	X	X	X	X	X	X				The organization: a. Reviews ***at least annually*** **[DHS]** the privileges assigned to ***any user with elevated privileges*** **[DHS]** to validate the need for such privileges; and b. Reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs.	
AC-6(8)	Least Privilege Privilege Levels For Code Execution	X	X	X	X	X	X				The information system prevents ***All*** **[CNSS]** software from executing at higher privilege levels than users executing the software.	
AC-6(9)	Auditing Use Of Privileged Functions	X	X	X	X	X	X				The information system audits the execution of privileged functions.	
AC-6(10)	Least Privilege	X	X	X	X	X	X				The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
	Prohibit Non-Privileged Users From Executing Privileged Functions										altering implemented security safeguards/countermeasures.	
AC 7 Protect Function: PR.AC 7*	Unsuccessful Login Attempts	X	X	X	X	X	X	X	X	X	The information system: a. Enforces a limit of ***a maximum of three (3)*** **[CNSS]** consecutive invalid login attempts by a user during a ***fifteen (15) minute*** **[CNSS]** time period; and b. Automatically ***locks the account/node for at least fifteen (15) minutes, or until unlocked by an administrator*** **[CNSS]** when the maximum number of unsuccessful attempts is exceeded.	
AC 8 Protect Function: PR.AC 7*	System Use Notification	X	X	X	X	X	X				The information system: a. Displays to users [*Assignment: organization defined system use notification message or banner*] before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders (EO), directives, policies, regulations, standards, and guidance and states that: 1. Users are accessing a U.S. Government (USG) information system; 2. Information system usage may be monitored, recorded, and subject to audit; 3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and 4. Use of the information system indicates consent to monitoring and recording; b. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and c. For publicly accessible systems: 1. Displays system use information [*Assignment: organization defined conditions*], before granting further access; 2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and	Use DHS Office of the General Counsel (OGC) Mandated Consent Banner applicable to the level of classification of system access. Authorized Banners: http://dhsconnect.dhs.gov/org/comp/mgmt/ocio/ciso/Pages/SecurityPubs.aspx For authorized use and limited personal use guidance, refer to: • DHS Management Directive (MD) 4600.1, *Personal Use of Government Office Equipment* • DHS MD 4900, *Individual Use and Operation of DHS Information Systems/Computers* • DHS Directive 142 03, *Electronic Mail Usage and Maintenance* • DHS Directive 262 04, *DHS Web (Internet and Extranet Information)*

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
											3. Includes a description of the authorized uses of the system.	
AC 9 Protect Function: PR.AC 7*	Previous Logon (Access) Notification	X	X	X	X	X	X	X	X	X	The information system notifies the user, upon successful logon (access) to the system, of the date and time of the last logon (access).	This control is applicable to logons to information systems via human user interfaces and logons to systems that occur in other types of architectures (e.g., service oriented architectures). Framework for Improving Critical Infrastructure Cybersecurity ("Cybersecurity Framework), Version 1.1, April 16, 2018.
AC 10 Protect Function: PR.AC 5*	Concurrent Session Control	X	X		X	X		X	X		The information system limits the number of concurrent sessions for each ***system account*** to ***a maximum of three (3) sessions*** **[CNSS]**.	
AC 11 Protect Function: PR.AC 7*	Session Lock	X	X	X	X	X	X				The information system: a. Prevents further access to the system by initiating a session lock ***within twenty (20) minutes of user inactivity*** **[DHS]**; and b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.	DHS Components shall also apply AC 2(5) and Configuration Management (CM) 6 in addition to this baseline requirement.
AC-11(1)	Session Lock Pattern-Hiding Displays	X	X	X							The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.	
AC 12 Protect Function: PR.AC 7*	Session Termination	X	X		X	X					The information system automatically terminates a user session after [*Assignment: organization defined conditions or trigger events requiring session disconnect*].	
/	Session Termination User-initiated Logouts / Message Displays	X	X		X	X					The information system: a. Provides a logout capability for user-initiated communications sessions whenever authentication is used to gain access to ***all*** **[CNSS]** resources; and b. Displays an explicit logout message to users indicating the reliable termination of authenticated communications sessions.	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
AC 14 Protect Function: PR.AC 4, PR.AC 7*	Permitted Actions Without Identification Or Authentication	X	X	X	X	X	X				The organization: a. Identifies ***No user actions*** **[CNSS]** that can be performed on the information system without identification or authentication consistent with organizational missions/business functions; and b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.	
AC 16 Protect Function: PR.AC 4, PR.AC 6*	Security Attributes	X	X		X	X					The organization: a. Provides the means to associate [*Assignment: organization defined types of security attributes*] having [*Assignment: organization defined security attribute values*] with information in storage, in process, and/or in transmission; b. Ensures that the security attribute associations are made and retained with the information; c. Establishes the permitted [*Assignment: organization defined security attributes*] for [*Assignment: organization defined information systems*]; and d. Determines the permitted [*Assignment: organization defined values or ranges*] for each of the established security attributes.	
AC-16(6)	Security Attributes Maintenance Of Attribute Association By Organization	X	X		X	X					The organization allows personnel to associate, and maintain the association of [*Assignment: organization-defined security attributes*] with [*Assignment: organization-defined subjects and objects*] in accordance with [*Assignment: organization-defined security policies*].	
AC 17 Protect Function: PR.PT 4, PR.AC 3*	Remote Access	X	X	X	X	X	X				The organization: a. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and b. Authorizes remote access to the information system prior to allowing such connections.	Components shall centrally manage all remote access and dial in connections to their systems and shall ensure that remote access and approved dial in capabilities provide strong authentication, two factor authentication, audit capabilities, and protection for sensitive information throughout transmission. DHS has an immediate goal that remote access shall only be allowed with two factor authentication where one of the factors is provided by a device separate from the computer gaining access. Any two factor authentication shall be based on Department controlled certificates or hardware tokens issued directly to each authorized user. Remote access solutions shall comply with the encryption requirements of

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
												Federal Information Processing Standards (FIPS) 140 2, *Security Requirements for Cryptographic Modules.* See Privacy Controls Section for additional requirements involving remote access of PII. DHS Components shall also apply AC 4 in addition to this baseline control.
AC-17(1)	Remote Access Automated Monitoring / Control	X	X	X	X	X	X				The information system monitors and controls remote access methods.	
AC-17(2)	Remote Access Protection Of Confidentiality / Integrity Using Encryption	X	X	X	X	X	X				The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.	
AC-17(3)	Remote Access Managed Access Control Points	X	X	X	X	X	X				The information system routes all remote accesses through [*Assignment: organization-defined number*] managed network access control points.	
AC-17(4)	Remote Access Privileged Commands / Access	X	X	X	X	X	X				The organization: a. Authorizes the execution of privileged commands and access to security-relevant information via remote access only for [*Assignment: organization-defined needs*]; and b. Documents the rationale for such access in the security plan for the information system.	
AC-17(6)	Remote Access Protection of Information	X	X	X							The organization ensures that users protect information about remote access mechanisms from unauthorized use and disclosure.	
AC-17(9)	Remote Access Disconnect / Disable Access	X	X	X	X	X	X				The organization provides the capability to expeditiously disconnect or disable remote access to the information system within ***Low confidentiality or integrity impact: 30 minutes; Moderate confidentiality or integrity impact: 20; minutes; High***	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
											confidentiality or integrity impact: 10 minutes **[CNSS]**.	
AC 18 Protect Function; PR.PT 4*	Wireless Access	X	X	X	X	X	X				The organization: a. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and b. Authorizes wireless access to the information system prior to allowing such connections.	
AC-18(1)	Wireless Access Authentication And Encryption	X	X	X	X	X	X				The information system protects wireless access to the system using authentication of ***both users and devices as appropriate*** **[CNSS]** and encryption.	
AC-18(3)	Wireless Access Disable Wireless Networking	X	X	X	X	X	X				The organization disables, when not intended for use, wireless networking capabilities internally embedded within information system components prior to issuance and deployment.	
AC-18(4)	Wireless Access Restrict Configurations By Users	X	X	X	X	X	X				The organization identifies and explicitly authorizes users allowed to independently configure wireless networking capabilities.	
AC-18(5)	Wireless Access Antennas / Transmission Power Levels	X			X						The organization selects radio antennas and calibrates transmission power levels to reduce the probability that usable signals can be received outside of organization-controlled boundaries.	
AC 19 Protect Function: PR.AC 3, PR.AC 6*	Access Control For Mobile Devices	X	X	X	X	X	X				The organization: a. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization controlled mobile devices; and b. Authorizes the connection of mobile devices to organizational information systems.	Wireless Portable Electronic Devices (PED) shall not be used to store, process, or transmit combinations, personal identification numbers (PIN), or sensitive information in unencrypted formats. Wireless PEDs shall not be used to store, process, or transmit combinations, personal identification numbers (PIN), or sensitive information in unencrypted formats. Laptop computers shall be powered down when not in use (due to volatile memory vulnerabilities). Refer to DHS Instruction 121 01 011, The Department of Homeland Security Administrative Security Program.

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
												DHS Components shall also apply IA 5, IA 7, PL 4, SC 8, SC 9, and SC 13 in addition to this baseline control.
AC-19(5)	Access Control For Mobile Devices Full Device / Container-Based Encryption	X	X		X	X					The organization employs [*Selection: full-device encryption; container encryption*] to protect the confidentiality and integrity of information on ***all mobile devices authorized to connect to the organizations IS*** **[CNSS]**.	
AC 20 Identify Function: ID.AM 4, PR.AC 3*	Use of External Information Systems	X	X	X	X	X	X				The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to: a. Access the information system from the external information systems; and b. Process, store, or transmit organization controlled information using external information systems.	
AC-20(1)	Use of External Information Systems Limits On Authorized Use	X	X	X	X	X	X				The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization: a. Verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or b. Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.	
AC-20(2)	Use of External Information Systems Portable Storage Devices	X	X	X							The organization [*Selection: restricts; prohibits*] the use of organization-controlled portable storage devices by authorized individuals on external information systems.	
AC-20(3)	Use of External Information Systems	X	X	X	X	X	X				The organization ***restricts*** **[CNSS]** the use of non-organizationally owned information systems, system components, or devices to	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
	Non-Organizationally Owned Systems / Components / Devices										process, store, or transmit organizational information.	
AC 21 Protect Function: PR.IP 8*	Information Sharing	X	X								The organization: a. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for [*Assignment: organization defined information sharing circumstances where user discretion is required*]; and b. Employs [*Assignment: list of organization defined information sharing circumstances and automated mechanisms or manual processes required*] to assist users in making information sharing/collaboration decisions.	
AC-22	Publicly Accessible Content	X	X	X							The organization: a. Designates individuals authorized to post information onto an organizational information system that is publicly accessible; b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information; c. Reviews the proposed content of publicly accessible information for nonpublic information prior to posting onto the organizational information system; and d. Reviews the content on the publicly accessible information system for nonpublic information ***quarterly or as new information is posted*** **[CNSS]** and removes such information, if discovered.	
AC-23	Data Mining Protection	X	X								The organization employs [*Assignment: organization-defined data mining prevention and detection techniques*] for [*Assignment: organization-defined data storage objects*] to adequately detect and protect against data mining.	
AC 24 Protect Function:	Access Control Decisions	X	X	X	X	X	X	X	X	X	The organization establishes procedures to ensure [Assignment: organization defined access control decisions] are applied to each access request prior to access enforcement.	Access control decisions occur when authorization information is applied to specific accesses. In contrast, access enforcement occurs when information systems enforce access control decisions. While it is very common to have access control decisions and access

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
PR.AC 4, PR.AC 6*												enforcement implemented by the same entity, it is not required and it is not always an optimal implementation choice. For some architectures and distributed information systems, different entities may perform access control decisions and access enforcement. Refer to *Cybersecurity Framework*, Version 1.1, April 16, 2018.
AC 25 Detect Function: DE.DP 2*	Reference Monitor	X	X	X	X	X	X	X	X	X	The information system implements a reference monitor for [Assignment: organization defined access control policies] that is tamperproof, always invoked, and small enough to be subject to analysis and testing, the completeness of which can be assured.	Information is represented internally within information systems using abstractions known as data structures. Internal data structures can represent different types of entities, both active and passive. Active entities, also known as subjects, are typically associated with individuals, devices, or processes acting on behalf of individuals. Passive entities, also known as objects, are typically associated with data structures such as records, buffers, tables, files, inter process pipes, and communications ports. Reference monitors typically enforce mandatory access control policies a type of access control that restricts access to objects based on the identity of subjects or groups to which the subjects belong. The access controls are mandatory because subjects with certain privileges (e.g., access permissions) are restricted from passing those privileges on to any other subjects, either directly or indirectly that is, the information system strictly enforces the access control policy based on the rule set established by the policy. The tamperproof property of the reference monitor prevents adversaries from compromising the functioning of the mechanism. The always invoked property prevents adversaries from bypassing the mechanism and hence violating the security policy. The smallness property helps to ensure the completeness in the analysis and testing of the mechanism to detect weaknesses or deficiencies (e.g., latent flaws) that would prevent the enforcement of the security policy. Refer to *Cybersecurity Framework*, Version 1.1, April 16, 2018.

Awareness and Training (AT)

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
AT-1	Security Awareness And Training Policy And Procedures	X	X	X	X	X	X	X	X	X	The organization: a. Develops, documents, and disseminates ***to all personnel*** **[CNSS]**: 1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and b. Reviews and updates the current: 1. Security awareness and training policy [***at least annually if not otherwise defined in formal organizational policy*** **[CNSS]**; and 2. Security awareness and training procedures ***at least annually if not otherwise defined in formal organizational policy*** **[CNSS]**.	The DHS NSS 4300B Policy, along with the proper application and documentation of all relevant (AT) baseline controls, CNSS and DHS defined values, supplemental guidance, and any inheritable network or enterprise controls provide the basis for satisfying AT-1. However, the ISO is ultimately responsible for addressing any and all (AT) policy and procedures within the SSP.
AT 2 Protect Function: PR.AT 1*	Security Awareness	X	X	X	X	X	X	X	X	X	The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors): a. As part of initial training for new users; b. When required by information system changes; and c. ***At least annually if not otherwise defined in formal organization*** **[CNSS]** thereafter.	During in processing. Site specific information will be provided based on local operating environment and job specific duties. Refer to DHS Instruction 121 01 011, *The Department of Homeland Security Administrative Security Program*, for derivative classification requirements. If Classified/NSS, all users must take the current *Cyber Awareness Challenge* training (Intelligence Community Version), provide certificate of completion to component ISSM, and sign a Standard Form (SF) 312. https://iatraining.disa.mil/eta/disa_cac2018/launchPage.htm
AT-2(2)	Security Awareness Practical Exercises	X	X	X	X	X	X	X	X	X	The organization includes security awareness training on recognizing and reporting potential indicators of insider threat.	
AT 3 Protect	Role Based Security Training	X	X	X	X	X	X	X	X	X	The organization provides role based security training to personnel with assigned security roles and responsibilities:	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
Function: PR.AT 2, PR.AT 4, PR.AT 5*											a. Before authorizing access to the information system or performing assigned duties; b. When required by information system changes; and c. ***At least annually if not otherwise defined in formal organization*** **[CNSS]** thereafter.	
AT-3(2)	Role-Based Security Training Practical Exercises	X	X	X	X	X	X	X	X	X	The organization provides [Assignment: organization-defined personnel or roles] with initial and ***at least annually if not otherwise defined in formal organizational policy or when sufficient changes are made to physical security systems*** **[CNSS]** training in the employment and operation of physical security controls.	Refer to DHS Instruction 121-01-011, *The Department of Homeland Security Administrative Security Program*, Chapter 4.
AT-3(4)	Role-Based Security Training Suspicious Communications and Anomalous System Behavior	X	X	X	X	X	X	X	X	X	The organization provides training to its personnel on ***Minimally but not limited to indicators of potentially malicious code in suspicious email*** **[CNSS]** to recognize suspicious communications and anomalous behavior in organizational information systems.	
AT-4	Security Training Records	X	X	X	X	X	X	X	X	X	The organization: a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and b. Retains individual training records for ***a minimum of two (2) years*** **[DHS]**.	At a minimum training records shall identify user name, name of training, and date of training (initial and refresher) Reference: DHS Records Retention Program

Audit and Accountability (AU)

					I						Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H		**L**	**H**	**M**	**L**	**H**		**L**	4300B.102	
AU-1	Audit And Accountability Policy And Procedures	X	X	X	X	X	X	X	X	X	The organization: a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]: 1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and b. Reviews and updates the current: 1. Audit and accountability policy ***at least annually if not otherwise defined in formal organizational policy*** **[CNSS]**; and 2. Audit and accountability procedures ***at least annually if not otherwise defined in formal organizational policy*** **[CNSS]**.	The DHS NSS 4300B Policy, along with the proper application and documentation of all relevant (AU) baseline controls, CNSS and DHS defined values, supplemental guidance, and any inheritable network or enterprise controls provide the basis for satisfying AU-1. However, the ISO is ultimately responsible for addressing any and all (AU) policy and procedures within the SSP.
AU 2 Identify Function: ID.SC 4*	Audit Events	X	X	X	X	X	X				The organization: a. Determines, based on a risk assessment and mission/business needs, that the information system must be capable of auditing the following events: 1. Authentication events: (1) Logons (Success/Failure) (2) Logoffs (Success) 2. File and Objects events: (1) Create (Success/Failure) (2) Access (Success/Failure) (3) Delete (Success/Failure) (4) Modify (Success/Failure) (5) Permission Modification (Success/Failure) (6) Ownership Modification (Success/Failure) 3. Writes/downloads to external devices/media (e.g., A Drive, CD/DVD devices/printers) (Success/Failure) 4. Uploads from external devices (e.g., CD/DVD drives) (Success/Failure) 5. User and Group Management events:	(1) Systems with unique security considerations such as CDSs and Community of Interest (COI) may require the following additional events to be recorded. Successful and unsuccessful: • Changes of user's formal access permissions • Information downgrades and overrides • Access to objects or data whose labels are inconsistent with user privileges • Changes to security label. • Counterintelligence requirements (2) Components shall consider the types of auditing to be performed by an information system and the audit processing requirements when allocating audit storage capacity.

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
											(1) User add, delete, modify, suspend, lock (Success/Failure) (2) Group/Role add, delete, modify (Success/Failure) 6. Use of Privileged/Special Rights events: (1) Security or audit policy changes (Success/Failure) (2) Configuration changes (Success/Failure) 7. Admin or root level access (Success/Failure) 8. Privilege/Role escalation (Success/Failure) 9. Audit and log data accesses (Success/Failure) 10. System reboot, restart and shutdown (Success/Failure) 11. Print to a device (Success/Failure) 12. Print to a file (e.g., pdf format) (Success/Failure) 13. Application (e.g., Firefox, Internet Explorer, Microsoft (MS) Office Suite, etc.) initialization (Success/Failure) 14. Export of information (Success/Failure) include (e.g., to CDRW, thumb drives, or remote systems) 15. Import of information (Success/Failure) include (e.g., from CDRW, thumb drives, or remote systems) **[CNSS]**; b. Coordinates the security audit function with other organizational entities requiring audit related information to enhance mutual support and to help guide the selection of auditable events; c. Provides a rationale for why the auditable events are deemed to be adequate to support after the fact investigations of security incidents; and d. Determines that the following events are to be audited within the information system: ***Refer to a. above*** **[DHS]**.	
AU-2(3)	Audit Events Privileged Functions	X	X	X	X	X	X				The organization reviews and updates the audited events ***at least annually if not otherwise defined in formal organizational policy*** **[CNSS]**.	
AU-3	Content of Audit Records	X	X	X	X	X	X				The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source	(1) If manual audit collection is approved by the AO, the audit records shall contain, at a minimum the following content: • Date

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
											of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.	• Identification of the user • Time the user logs on and off the system • Function(s) performed (2) Manual audit logs will be used to record the transmission of any data over a FAX connected to a secure voice (e.g., Secure Telephone Equipment (STE)). These logs will be maintained for one year and must include the following information: • Sender's name, organization and telephone number • Date and time of FAX transmission • Classification level of the information • Recipient's name, organization and telephone number (3) Audit data shall be centrally managed to the maximum extent possible.
AU-3(1)	Content of Audit Records Additional Audit Information	X	X	X	X	X	X				The information system generates audit records containing the following additional information: [*Assignment: organization-defined additional, more detailed information*].	
AU-3(2)	Content of Audit Records Centralized Management of Planned Audit Record Content	X			X						The information system provides centralized management and configuration of the content to be captured in audit records generated by ***all information systems to the maximum extent possible*** **[DHS]**.	
AU 4 Protect Function: PR.DS 4*	Audit Storage Capacity							X	X	X	The organization allocates audit record storage capacity in accordance with [*Assignment: organization defined audit record storage requirements*].	Components shall consider the types of auditing to be performed by an information system and the audit processing requirements when allocating audit storage capacity.
AU-4(1)	Audit Storage Capacity Transfer to Alternate Storage	X	X	X	X	X	X	X	X	X	The information system off-loads audit records [*Assignment: organization-defined frequency*] onto a different system or media than the system being audited.	
AU-5	Response To Audit Processing Failures							X	X	X	The information system: a. Alerts at a minimum, the ISSO and ISSM in the event of an audit processing failure; and b. Takes the following additional actions: ***record any audit processing failure in the audit log*** **[DHS]**.	
AU-5(1)	Response To Audit Processing Failures Audit Storage Capacity							X	X	X	The information system provides a warning to [*Assignment: organization-defined personnel, roles, and/or locations*] within [*Assignment:*	

					I					Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	**M**	**L**	**H**	**M**	**L**	**H**	**M**	**L**	4300B.102	
											organization-defined time period] when allocated audit record storage volume reaches a ***maximum of 75%*** **[CNSS]** of repository maximum audit record storage capacity.	
AU-5(2)	Response to Audit Processing Failures Real-Time Alerts							X			The information system provides an alert in [*Assignment: organization-defined real-time period*] to [*Assignment: organization-defined personnel, roles, and/or locations*] when the following audit failure events occur: ***Minimally but not limited to: auditing software/hardware errors; failures in the audit capturing mechanisms; and audit storage capacity being reached or exceeded*** **[CNSS]**.	
AU 6 Identify Function: ID.SC 4* Detect Function: DE.AE 2, DE.AE 3, DE.DP 4* Respond Function; RS.CO 2, RS.AN 1*	Audit Review, Analysis, And Reporting	X	X	X	X	X	X				The organization: a. Reviews and analyzes information system audit records ***on at least on a weekly basis*** **[CNSS]** for indications of [*Assignment: organization defined inappropriate or unusual activity*]; and b. Reports findings to [*Assignment: organization defined personnel or roles*].	Audit records for financial systems or for systems hosting or processing PII shall be reviewed by the System Administrator monthly. Unusual activity or unexplained access attempts shall be reported to the ISO and Component CISO and/or ISSM.
AU-6(1)	Audit Review, Analysis, And Reporting Process Integration	X	X	X	X	X	X				The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.	
AU-6(3)	Audit Review, Analysis, And Reporting Correlate Audit Repositories	X	X	X	X	X	X				The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
AU-6(4)	Audit Review, Analysis, And Reporting Central Review and Analysis	X	X	X	X	X	X				The information system provides the capability to centrally review and analyze audit records from multiple components within the system.	
AU-6(5)	Audit Review, Analysis, And Reporting Integration / Scanning and Monitoring Capabilities	X			X						The organization integrates analysis of audit records with analysis of [*Selection (one or more): vulnerability scanning information; performance data; information system monitoring information; [Assignment: organization-defined data/information collected from other sources]*] to further enhance the ability to identify inappropriate or unusual activity.	
AU-6(6)	Audit Review, Analysis, And Reporting Correlation With Physical Monitoring	X			X						The organization correlates information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.	
AU-6(10)	Audit Review, Analysis, And Reporting Audit Level Adjustment	X	X	X	X	X	X				The organization adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.	
AU 7 Respond Function: RS.AN 3*	Audit Reduction And Report Generation	X	X		X	X					The information system provides an audit reduction and report generation capability that: a. Supports on demand audit review, analysis, and reporting requirements and after the fact investigations of security incidents; and b. Does not alter the original content or time ordering of audit records.	
AU-7(1)	Audit Reduction And Report Generation Automatic Processing	X	X		X	X					The information system provides the capability to process audit records for events of interest based on [*Assignment: organization-defined audit fields within audit records*].	
AU-8	Time Stamps				X	X	X				The information system: a. Uses internal system clocks to generate time stamps for audit records; and b. Records time stamps for audit records that can be mapped to Universal Time Coordinated (UTC) or Greenwich Mean Time (GMT) and meets [*Assignment: organization-defined granularity of time measurement*].	
AU-8(1)	Time Stamps Authoritative Time Source				X	X	X				The information system:	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
											a. Compares the internal information system clocks ***At least every 24 hours*** **[CNSS]** with ***ntp.sgov.gov*** **[DHS]**; b. Synchronizes the internal system clocks to the authoritative time source when the time difference is greater than ***the organizationally defined granularity in AU-8*** **[CNSS]**.	
AU-9	Protection of Audit Information	X	X	X	X	X	X	X	X	X	The information system protects audit information and audit tools from unauthorized access, modification, and deletion.	Audit information shall be handled and protected at the same security level from which it originated, until reviewed and determination is made on the actual classification. Access to audit functionality shall be restricted by distinguishing between privileged users with audit-related privileges and privileged users without audit-related privileges to improve audit integrity.
AU-9(2)	Protection of Audit Information Backup on Separate Physical Systems/Components							X			The information system backs up audit records ***at least weekly*** **[CNSS]** onto a physically different system or system component than the system or component being audited.	
AU-9(3)	Protection of Audit Information Cryptographic Protection				X						The information system implements cryptographic mechanisms to protect the integrity of audit information and audit tools.	
AU-9(4)	Protection of Audit Information Access by Subset of Privileged Users	X	X	X	X	X	X				The organization authorizes access to management of audit functionality to only [*Assignment: organization-defined subset of privileged users*].	
AU-10	Non-Repudiation				X	X					The information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed a [*Assignment: organization-defined actions to be covered by non-repudiation*].	
AU-11	Audit Record Retention							X	X	X	The organization retains audit records for a ***minimum of 1 year for all information (Unclassified through Collateral Top Secret)*** **[CNSS]** to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.	
AU-11(1)	Audit Record Retention							X	X	X	The organization employs ***a retention of technology to access audit records for the***	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
	Long-Term Retrieval Capability										***duration of the required retention period*** **[CNSS]** to ensure that long-term audit records generated by the information system can be retrieved.	
AU 12 Identify Function: ID.SC 4* Detect Function: DE.CM 1, DE.CM 3, DE.CM 7*	Audit Generation	X	X	X	X	X	X				The information system: a. Provides audit record generation capability for the auditable events defined in AU 2 a. for ***all information system and network components***; **[CNSS]**; b. Allows [*Assignment: organization defined personnel or roles*] to select which auditable events are to be audited by specific components of the information system; and c. Generates audit records for the events defined in AU 2 d. with the content defined in AU 3.	
AU-12(1)	Audit Generation System-Wide / Time-Correlated Audit Trail				X	X	X				The information system compiles audit records from ***all information system components*** **[DHS]** into a system-wide (logical or physical) audit trail that is time-correlated to within ***the tolerance defined in AU-8*** **[CNSS]**.	
AU-12(3)	Audit Generation Changes by Authorized Individuals	X	X	X	X	X	X				The information system provides the capability for [*Assignment: organization-defined individuals or roles*] to change the auditing to be performed on [*Assignment: organization-defined information system components*] based on [*Assignment: organization-defined selectable event criteria*] within [*Assignment: organization-defined time thresholds*].	
AU 13 Detect Function: DE.CM 3*	Monitoring for Information Disclosure	X	X	X	X	X	X	X	X	X	The organization monitors [Assignment: organization defined open source information and/or information sites] [Assignment: organization defined frequency] for evidence of unauthorized disclosure of organizational information.	Open source information includes, for example, social networking sites. Refer to *Cybersecurity Framework*, Version 1.1, April 16, 2018.
AU-14	Session Audit	X	X	X	X	X	X				The information system provides the capability for authorized users to select a user session to capture/record or view/hear.	
AU-14(1)	Session Audit System Start-Up	X	X	X	X	X	X				The information system initiates session audits at system start-up.	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
AU-14(2)	Session Audit Capture/Record and Log Content	X	X	X	X	X	X				The information system provides the capability for authorized users to capture/record and log content related to a user session.	
AU-14(3)	Session Audit Remote Viewing / Listening	X	X	X							The information system provides the capability for authorized users to remotely view/hear all content related to an established user session in real time.	
AU 16 Identify Function: ID.SC 4*	Cross Organizational Auditing	X	X	X	X	X	X	X	X	X	The organization employs [Assignment: organization defined methods] for coordinating [Assignment: organization defined audit information] among external organizations when audit information is transmitted across organizational boundaries.	When organizations use information systems and/or services of external organizations, the auditing capability necessitates a coordinated approach across organizations. For example, maintaining the identity of individuals that requested particular services across organizational boundaries may often be very difficult, and doing so may prove to have significant performance ramifications. Therefore, it is often the case that cross organizational auditing (e.g., the type of auditing capability provided by service oriented architectures) simply captures the identity of individuals issuing requests at the initial information system, and subsequent systems record that the requests emanated from authorized individuals. Refer to *Cybersecurity Framework*, Version 1.1, April 16, 2018.

Security Assessment and Authorization (CA)

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
CA-1	Security Assessment and Authorization Policies and Procedures	X	X	X	X	X	X	X	X	X	The organization a. Develops, documents, and disseminates to ***all personnel*** **[CNSS]**: 1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and b. Reviews and updates the current: 1. Security assessment and authorization policy ***at least annually if not otherwise defined in formal organizational policy*** **[CNSS]**; and 2. Security assessment and authorization procedures a***t least annually if not otherwise defined in formal organizational policy*** **[CNSS]**.	The DHS NSS 4300B Policy, along with the proper application and documentation of all relevant (CA) baseline controls, CNSS and DHS defined values, supplemental guidance, and any inheritable network or enterprise controls provide the basis for satisfying CA-1. However, the ISO is ultimately responsible for addressing any and all (CA) policy and procedures within the SSP. Supporting References: DHS templates for the following artifacts: • System Security Plan (SSP) • Risk Assessment Report (RAR) • Security Assessment Report (SAR) • Plan of Action and Milestones (POA&M) All of the above documentation shall be maintained in the Classified Information Assurance Compliance System (CIACS).
CA 2 Identify Function: ID.RA 1* Protect Function: PR.IP 7* Detect Function: DE.DP 1, DE.DP 2, DE.DP 3, DE.DP 4, DE.DP 5* Respond Function: RS.CO 3*	Security Assessments	X	X	X	X	X	X	X	X	X	The organization: a. Develops a security assessment plan that describes the scope of the assessment including: Security controls and control enhancements under assessment; Assessment procedures to be used to determine security control effectiveness; and Assessment environment, assessment team, and assessment roles and responsibilities; b. Assesses the security controls in the information system and its environment of operation ***at least annually, or as stipulated in the organization's continuous monitoring program*** **[CNSS]** to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements; c. Produces a security assessment report that documents the results of the assessment; and d. Provides the results of the security control assessment to the ***Information System Security Officer, Information System Security Manager, Information System Owner, and Authorizing Official*** **[DHS]**.	The DHS CISO shall conduct critical control reviews and site assistance visits across the Department in order to monitor the effectiveness of Component security programs.
CA-2(1)	Security Assessments	X	X	X	X	X	X	X	X	X	The organization employs assessors or assessment teams with ***Authorizing Officials***	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
	Independent Assessor										***determine the required level of independence based on the security categories of information systems and/or the ultimate risk to organizational operations, organizational assets, or individuals*** **[DHS]** to conduct security control assessments.	
CA-2(2)	Security Assessments Specialized Assessments	X			X			X			The organization includes as part of security control assessments, ***as required by the Authorizing Official, announced or unannounced, malicious user testing, penetration testing, and/or red team exercises conducted for information systems with a Confidentiality, Integrity, or Availability impact level of High or as required by the Authorizing Official*** **[DHS]**.	
CA 3 Identify Function: ID.AM 3* Detect Function: DE.AE 1*	System Interconnections	X	X	X	X	X	X				The organization: a. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements; b. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and c. Reviews and updates Interconnection Security Agreements ***at least annually*** **[CNSS]**.	DHS Components shall: a. Ensure appropriate identification and authentication controls, audit logging, and integrity controls are implemented on every network component. b. Interconnections between DHS systems and systems not controlled by DHS shall be established only through controlled interfaces. The controlled interfaces shall be authorized at the highest security level of the information on the network. c. Components shall document interconnections with other external networks with an Interconnection Security Agreement (ISA). d. ISAs shall be reissued every three years, whenever there are significant changes that may impact the ISA, and/or as established in the signed ISA. e. ISAs shall be signed by the appropriate Authorizing Official for the involved parties, or their designated representatives. f. ISAs shall be reviewed annually by DHS Components. g. Interconnections must be documented in the System Security Plan (SSP). h. If required, Components shall establish Memorandum of Agreements (MOA) that is supported by the associated ISA. i. Authorizing Officials may determine the need for an ISA for interconnections within and across DHS organizational boundaries. j. Components shall apply ISAs or other documentation required/agreed to between the agencies/departments/components involved. References:

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
												Office of Management and Budget (OMB) Circular A 130, Appendix III NIST SP 800 47, *Security Guide for Interconnecting Information Technology Systems*
CA-3(1)	System Interconnections Unclassified National Security System Connections	X	X	X							The organization prohibits the direct connection of ***all unclassified NSS*** **[CNSS]** to an external network without the use of [*Assignment: organization-defined boundary protection device*] (e.g., Router, firewall, CDS).	
CA-3(5)	System Interconnections Restrictions on External Network Connections	X	X	X	X	X	X				The organization employs ***deny-all, permit-by-exception for all systems*** **[CNSS]** policy for allowing ***all NSS*** **[DHS]** to connect to external information systems	
CA-5	Plan of Action and Milestones	X	X	X	X	X	X	X	X	X	The organization: a. Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and b. Updates existing plan of action and milestones ***at least quarterly*** **[CNSS]** based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.	Milestone completion dates must be addressed according to their criticality (e.g., 30 days for High/Critical, 60 days for Moderate, and 90 days for Low).
CA-6	Security Authorization	X	X	X	X	X	X	X	X	X	The organization: a. Assigns a senior-level executive or manager as the authorizing official for the information system; b. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and c. Updates the security authorization ***if the organization and/or system is adequately covered by a continuous monitoring program the Security Authorization may be continuously updated: If not; at least every three (3) years, when significant security breaches occur, whenever there is a significant change to the system, or to the environment in which the system operates*** **[CNSS]** or when there is a significant change to the system.	CFO Designated System Authorization to Operate (ATO) shall be rescinded if Information System Owners fail to comply with testing and reporting requirements established within this policy.

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
CA 7 Identify Function: ID.RA 1* Protect Function: PR.IP 7, PR.IP 8* Detect Function: DE.AE 2, DE.AE 3, DE.CM 1, DE.CM 2, DE.CM 3, DE.CM 6, DE.CM 7, DE.DP 1, DE.DP 2, DE.DP 3, DE.DP 4, DE.DP 5* Respond Function: RS.CO 3, RS.AN 1, RS.MI 3*	Continuous Monitoring	X	X	X	X	X	X	X	X	X	The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [*Assignment: organization defined metrics*] to be monitored; b. Establishment of [*Assignment: organization defined frequencies*] for monitoring and [*Assignment: organization defined frequencies*] for assessments supporting such monitoring; c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; d. Ongoing security status monitoring of organization defined metrics in accordance with the organizational continuous monitoring strategy; e. Correlation and analysis of security related information generated by assessments and monitoring; f. Response actions to address results of the analysis of security related information; and g. Reporting the security status of organization and the information system to [*Assignment: organization defined personnel or roles*] [*Assignment: organization defined frequency*].	***The DHS NSS Cybersecurity Performance Plan (CPP) should be referenced for Information System Continuous Monitoring.*** Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework), Version 1.1, April 16, 2018.
CA-7(1)	Continuous Monitoring Independent Assessment	X	X		X	X		X	X		The organization employs assessors or assessment teams with ***Authorizing Officials determining the required level of independence based on the security categories of information systems and/or the ultimate risk to organizational operations, organizational assets, or individuals*** **[DHS]** to monitor the security controls in the information system on an ongoing basis.	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
CA 8 Identify Function: ID.RA 1*	Penetration Testing				X						The organization conducts penetration testing at least once during the security authorization lifecycle on high integrity systems.	
CA 9 Identify Function: ID.AM 3*	Internal System Connections	X	X	X	X	X	X				The organization: a. Authorizes internal connections of: ***organization defined information system components or classes of components within the authorization boundary*** **[DHS]** to the information system; and b. Documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.	

Configuration Management (CM)

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
CM-1	Configuration Management Policy and Procedures	X	X	X	X	X	X				The organization: a. Develops, documents, and disseminates to personnel with ***configuration management responsibilities*** **[DHS]**: 1. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; and b. Reviews and updates the current: 1. Configuration management policy ***at least annually if not otherwise defined in formal organizational policy*** **[CNSS]**; and 2. Configuration management procedures ***at least annually if not otherwise defined in formal organizational policy*** **[CNSS]**.	The DHS NSS 4300B Policy, along with the proper application and documentation of all relevant (CM) baseline controls, CNSS and DHS defined values, supplemental guidance, and any inheritable network or enterprise controls provide the basis for satisfying CM-1. However, the ISO is ultimately responsible for addressing any and all (CM) policy and procedures within the SSP. Refer to NIAP, mandated by Committee on National Security Systems Policy Number 11
CM 2 Protect Function: PR.DS 7, PR.IP 1* Detect Function: DE.AE 1, DE.CM 2*	Baseline Configuration				X	X	X				The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.	Information System Owners shall develop and maintain a Configuration Management Plan (CMP) for each information system as part of its SSP. All DHS systems shall be under the oversight of a Configuration Management Board (CMB). Users shall report known or suspected implementations of unauthorized classified Information Technology (IT) changes to their appropriate governing CMB (e.g., For Homeland Secure Data Network (HSDN), the ISSO shall ensure that timely responses are provided to the Classified Infrastructure Change Control Board (C ICCB) for change request packages.) The baseline configuration shall describe the approved configuration of an information system including all hardware (manufacturer, model and serial number), software (name and version number), and firmware components (name and version number), how the components are interconnected, and the physical and logical locations of each. Components shall maintain a baseline configuration for development and test environments that is managed separately from the operational baseline configuration.

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
												Modifying, relocating, or reconfiguring the hardware of any computer system must be approved by the appropriate organizational Configuration Control Board (CCB) for each system. Hardware will not be connected to any system/network without the express written consent of the ISSO/ISSM/CISO and when appropriate the CCB. See CM 6 for system configuration guidance. Refer to NIAP, mandated by CNSSP Number 11
CM-2(1)	Baseline Configuration Reviews and Updates				X	X	X				The organization reviews and updates the baseline configuration of the information system: a. ***at least annually*** **[CNSS]**; b. When required due to ***significant or security relevant changes or security incidents*** **[CNSS]**; and c. As an integral part of information system component installations and upgrades.	
CM-2(2)	Baseline Configuration Automation Support For Accuracy / Currency				X						The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.	
CM-2(3)	Baseline Configuration Retention of Previous Configurations				X	X					The organization retains ***at least two (2) previous versions of baseline configurations of the information system*** **[CNSS]** to support rollback.	
CM-2(7)	Baseline Configuration Configure Systems, Components, or Devices for High-Risk Areas				X	X					The organization: a. Issues ***mobile devices*** **[DHS]** with ***approved security configurations*** **[DHS]** to individuals traveling to locations that the organization deems to be of significant risk; and b. Applies ***specific security safeguards (e.g., examining the device for signs of physical tampering and purging/reimaging the hard disk drive.)*** **[DHS]** to the devices when the individuals return.	
CM 3 Protect Function: PR.IP 1,	Configuration Change Control				X	X	X				The organization: a. Determines the types of changes to the information system that are configuration controlled;	Refer to NIAP, mandated by CNSSP Number 11

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
PR.IP 3* Detect Function: DE.CM 1, DE.CM 3, DE.CM 7*											b. Reviews proposed configuration controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses; c. Documents configuration change decisions associated with the information system; d. Implements approved configuration controlled changes to the information system; e. Retains records of configuration controlled changes to the information system for ***one (1) year or two change cycles of baseline configurations as defined in CM 2(3), whichever is longer*** **[CNSS]**; f. Audits and reviews activities associated with configuration controlled changes to the information system; and g. Coordinates and provides oversight for configuration change control activities through a ***Configuration Control Board*** that ***convenes as required*** **[DHS]**.	
CM-3(1)	Configuration Change Control Automated Document / Notification / Prohibition of Changes				X						The organization employs automated mechanisms to: a. Document proposed changes to the information system; b. Notify [*Assignment: organized-defined approval authorities*] of proposed changes to the information system and request change approval; c. Highlight proposed changes to the information system that have not been approved or disapproved ***within 90 days*** **[CNSS]**; d. Prohibit changes to the information system until designated approvals are received; e. Document all changes to the information system; and f. Notify [*Assignment: organization-defined personnel*] when approved changes to the information system are completed.	
CM-3(2)	Configuration Change Control				X	X					The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
	Test / Validate / Document Changes											
CM-3(4)	Configuration Change Control | Security Representative				X	X	X				The organization requires an information security representative to be a member of the ***the configuration change control element defined in CM-3 g.*** **[CNSS]**.	
CM-3(5)	Configuration Change Control Automated Security Response				X						The information system implements ***automated security responses to appropriate personnel*** **[DHS]** automatically if baseline configurations are changed in an unauthorized manner.	
CM-3(6)	Configuration Change Control Cryptography Management				X	X	X				The organization ensures that ***cryptographic mechanisms used to provide all security safeguards that rely on cryptography*** **[CNSS]** are under configuration management.	
CM 4 Protect Function: PR.IP 1, PR.IP 3* Detect Function: DE.CM 4*	Security Impact Analysis				X	X	X				The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.	Refer to NIAP, mandated by CNSSP Number 11
CM-4(1)	Security Impact Analysis Separate Test Environments				X	X					The organization analyzes changes to the information system in a separate test environment before implementation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.	
CM 5 Protect Function: PR.IP 1*	Access Restrictions for Change				X	X	X				The organization defines documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.	Refer to NIAP, mandated by CNSSP Number 11

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
CM-5(1)	Access Restrictions for Change Automated Access Enforcement / Auditing				X	X					The information system enforces access restrictions and supports auditing of the enforcement actions.	
CM-5(2)	Access Restrictions for Change Review System Changes				X	X					The organization reviews information system changes ***every 90 days or more frequently as the organization defines for high integrity systems AND at least annually or more frequently as the organization defines for low integrity and moderate integrity systems*** **[CNSS]** and ***when there is an incident or when planned changes have been performed*** **[CNSS]** to determine whether unauthorized changes have occurred.	
CM-5(3)	Access Restrictions for Change Signed Components				X						The information system prevents the installation of ***all digitally signed software and firmware products*** **[CNSS]** without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.	
CM-5(5)	Access Restrictions for Change Limit Production / Operational Privileges				X	X	X				The organization: a. Limits privileges to change information system components and system-related information within a production or operational environment; and b. Reviews and reevaluates privileges ***at least annually*** **[CNSS]**.	
CM-5(6)	Access Restrictions for Change Limit Library Privileges				X	X	X				The organization limits privileges to change software resident within software libraries.	
CM 6 Protect Function: PR.IP 1*	Configuration Settings				X	X	X				The organization: a. Establishes and documents configuration settings for information technology products employed within the information system using ***DHS approved configuration guides. Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) and/or National Security Agency (NSA) guides may also be applied if DHS Guides do not apply to the system(s) to be configured***	Information systems shall be configured in accordance with guidance from at least one of the following: United States Government Configuration Baseline (USGCB), Department of Defense (DoD) STIGs, or (NSA) Security Configuration Guides. https://csrc.nist.gov/Projects/United_States_Government_Configuration_Baseline/USGCB_Content

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
											[DHS] that reflect the most restrictive mode consistent with operational requirements; b. Implements the configuration settings; c. Identifies, documents, and approves any deviations from established configuration settings for ***all configurable information system components*** **[CNSS]** based on [*Assignment: organization defined operational requirements*]; and d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.	https://iase.disa.mil/stigs/Pages/az.aspx?Paged=TRUE&p_Title=Microsoft%20Exchange%202010%20STIG%20Release%20Memo%20&p_ID=24&PageFirstRow=301&&View={25A09AF8-178B-447B-B42B-8839EBD71CAD} https://www.nsa.gov/resources/everyone/media-destruction/ Refer to NIAP, mandated by CNSSP Number 11
CM-6(1)	Configuration Settings				X	X					The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings for [*Assignment: organization-defined information system components*]	
CM-6(2)	Configuration Settings Respond to Unauthorized Changes				X						The organization employs [*Assignment: organization-defined security safeguards*] to respond to unauthorized changes to ***security sub-system configuration settings*** **[DHS]**.	
CM 7 Protect Function: PR.IP 1, PR.PT 3*	Least Functionality	X	X	X	X	X	X				The organization: a. Configures the information system to provide only essential capabilities; and b. Prohibits or restricts the use of the following functions, ports, protocols, and/or services: [*Assignment: organization defined prohibited or restricted functions, ports, protocols, and/or services*].	Department guidance on this subject is provided in DHS Hardening Guides (e.g., USGCB and DoD STIGs). Refer to NIAP, mandated by CNSSP Number 11
CM-7(1)	Least Functionality Periodic Review	X	X	X	X	X	X				The organization: a. Reviews the information system ***at least annually*** **[CNSS]** to identify unnecessary and/or non-secure functions, ports, protocols, and services; and b. ***Disables all functions, ports, protocols, and services within the information system deemed to be unnecessary and/or nonsecure*** **[CNSS]**.	
CM-7(2)	Least Functionality Prevent Program Execution	X	X	X	X	X	X				The information system prevents program execution in accordance with [*Selection (one or more): [Assignment: organization-defined policies regarding software program usage and restrictions]; rules authorizing the terms and conditions of software program usage*].	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
CM-7(3)	Least Functionality Registration Compliance	X	X	X	X	X	X				The organization ensures compliance ***with the latest ports, protocols and services guidance*** **[DHS]**.	
CM-7(5)	Least Functionality Authorized Software / Whitelisting	X	X	X	X	X	X				The organization: a. Identifies [*Assignment: organization-defined software programs authorized to execute on the information system*]; b. Employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system; and c. Reviews and updates the list of authorized software programs ***at least annually*** **[CNSS]**.	
CM 8 Identify Function: ID.AM 1, ID.AM 2* Protect Function: PR.DS 3* Detect Function: DE.CM 7*	Information System Component Inventory				X	X	X				The organization: a. Develops and documents an inventory of information system components that: 1. Accurately reflects the current information system; 2. Includes all components within the authorization boundary of the information system; 3. Is at the level of granularity deemed necessary for tracking and reporting; and 4. Includes minimally but not limited to: ***hardware specifications (manufacturer, type, model, serial number, physical location), software and software license information, information system/component owner, and for a networked component/device, the machine name*** **[CNSS]**; and b. Reviews and updates the information system component inventory ***at least annually*** **[CNSS]**	Refer to DHS Instruction 121 01 011, *The Department of Homeland Security Administrative Security Program*, for guidance on inventory of classified laptops. Refer to NIAP, mandated by CNSSP Number 11
CM-8(1)	Information System Component Inventory Updates During Installations / Removals				X	X					The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
CM-8(2)	Information System Component Inventory Automated Maintenance				X	X	X				The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.	
CM-8(3)	Information System Component Inventory Automated Unauthorized Component Detection				X	X	X				The organization: a. Employs automated mechanisms ***continuously*** **[DHS]** to detect the presence of unauthorized hardware, software, and firmware components within the information system; and b. Takes the following actions when unauthorized components are detected: ***Disables network access by such components/devices or notifies designated organizational officials*** **[DHS]**.	
CM-8(4)	Information System Component Inventory Accountability Information	X			X						The organization includes in the information system component inventory information, a means for identifying by Minimally ***position or role*** **[CNSS]**, individuals responsible/accountable for administering those components.	
CM-8(5)	Information System Component Inventory No Duplicate Accounting of Components				X	X					The organization verifies that all components within the authorization boundary of the information system are not duplicated in other information system component inventories.	
CM 9 Protect Function: PR.IP 1*	Configuration Management Plan				X	X	X				The organization develops, documents, and implements a configuration management plan for the information system that: a. Addresses roles, responsibilities, and configuration management processes and procedures; b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items; c. Defines the configuration items for the information system and places the configuration items under configuration management; and Protects the configuration management plan from unauthorized disclosure and modification.	Refer to NIAP, mandated by CNSSP Number 11
CM 10	Software Usage Restrictions				X	X	X				The organization:	Refer to NIAP, mandated by CNSSP Number 11

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
Detect Function: DE.CM 3*											a. Uses software and associated documentation in accordance with contract agreements and copyright laws; b. Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and c. Controls and documents the use of peer to peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.	
CM-10(1)	Software Usage Restrictions Source Software				X	X	X				The organization establishes the following restrictions on the use of open source software: [*Assignment: organization-defined restrictions*].	
CM 11 Detect Function: DE.CM 3*	User Installed Software	X	X	X	X	X	X				The organization: a. Establishes [*Assignment: organization defined policies*] governing the installation of software by users; b. Enforces software installation policies through [*Assignment: organization defined methods*]; and c. Monitors policy compliance ***continuously*** **[CNSS]**.	Refer to NIAP, mandated by CNSSP Number 11
CM-11(1)	User-Installed Software Alerts For Unauthorized Installations	X			X						The information system alerts [*Assignment: organization-defined personnel or roles*] when the unauthorized installation of software is detected.	
CM-11(2)	User-Installed Software Prohibit Installation without Privileged Status	X	X	X	X	X	X				The information system prohibits user installation of software without explicit privileged status.	

Contingency Planning (CP)

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
CP-1	Contingency Planning Policy and Procedures	X	X	X	X	X	X	X	X	X	The organization: a. Develops, documents, and disseminates to ***personnel with contingency planning responsibilities*** **[DHS]**: 1. A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls; and b. Reviews and updates the current: 1. Contingency planning policy ***at least annually if not otherwise defined in formal organizational policy*** **[CNSS]**; and 2. Contingency planning procedures ***at least annually if not otherwise defined in formal organizational policy*** **[CNSS]**.	The DHS NSS 4300B Policy, along with the proper application and documentation of all relevant (CP) baseline controls, CNSS and DHS defined values, supplemental guidance, and any inheritable network or enterprise controls provide the basis for satisfying CP-1. However, the ISO is ultimately responsible for addressing any and all (CP) policy and procedures within the SSP. References: NIST SP 800- 34, *Contingency Planning Guide for Federal Information Systems*
CP 2 Protect Function: PR.IP 7, PR.IP 9* Detect Function: DE.AE 4* Respond Function: RS.RP 1, RS.CO 1, RS.CO 3, RS.CO 4, RS.AN 2, RS.AN 4, RS.IM 1,	Contingency Plan							X	X	X	The organization: a. Develops a contingency plan for the information system that: 1. Identifies essential missions and business functions and associated contingency requirements; 2. Provides recovery objectives, restoration priorities, and metrics; 3. Addresses contingency roles, responsibilities, assigned individuals with contact information; 4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; 5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and 6. Is reviewed and approved by the ***Information System Owner*** **[DHS]**; b. Distributes copies of the contingency plan to ***key personnel or roles and organizational elements identified in the contingency plan*** **[CNSS]**;	ISOs shall ensure that contingency plans are created for all Chief Financial Officer (CFO) Designated Systems requiring high availability and that each plan is tested annually. ISOs shall refer to NIST SP 800 34, *Contingency Planning Guide for Federal Information Systems*, for the development of a Contingency Plan.

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
RS.IM 2* Recover Function: RC.IM 1, RC.IM 2, RC.CO 3*											c. Coordinates contingency planning activities with incident handling activities; d. Reviews the contingency plan for the information system ***at least annually unless otherwise defined in organizational policy*** **[CNSS]**; e. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; f. Communicates contingency plan changes to ***key personnel and organizational elements identified in the contingency plan*** **[CNSS]**; and g. Protects the contingency plan from unauthorized disclosure and modification.	
CP-2(1)	Contingency Plan Coordinate with Related Plans							X	X		The organization coordinates contingency plan development with organizational elements responsible for related plans.	
CP-2(2)	Contingency Plan Capacity Planning							X			The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.	
CP-2(3)	Contingency Plan Resume Essential Missions / Business Functions							X	X		The organization plans for the resumption of essential missions and business functions within ***a time period as defined in the contingency plan*** **[CNSS]** of contingency plan activation.	
CP-2(4)	Contingency Plan Resume All Missions / Business Functions							X			The organization plans for the resumption of all missions and business functions within ***a time period as defined in the contingency plan*** **[CNSS]** of contingency plan activation.	
CP-2(5)	Contingency Plan							X			The organization plans for the continuance of essential missions and business functions with little or no loss of operational continuity and sustains that continuity until full information	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
	Continue Essential Missions / Business Functions										system restoration at primary processing and/or storage sites.	
CP-2(8)	Contingency Plan Identify Critical Assets							X	X		The organization identifies critical information system assets supporting essential missions and business functions.	
CP 3 Respond Function: RS.CO 1*	Contingency Training							X	X	X	The organization provides contingency training to information system users consistent with assigned roles and responsibilities: a. Within ***10 working days*** **[CNSS]** of assuming a contingency role or responsibility; b. When required by information system changes; and c. ***at least annually or as defined in the contingency plan*** **[CNSS]** thereafter.	
CP-3(1)	Contingency Training Simulated Events							X			The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.	
CP 4 Identify Function: ID.SC 5* Protect Function: PR.IP 4, PR.IP 10*	Contingency Plan Testing							X	X	X	The organization: a. Tests the contingency plan for the information system ***at a frequency as defined in the contingency plan*** **[CNSS]** using ***organization defined tests and/or exercises*** **[DHS]** to determine the effectiveness of the plan and the organizational readiness to execute the plan; b. Reviews the contingency plan test results; and c. Initiates corrective actions, if needed.	For systems with a High availability, components shall provide simulated annual testing for system recovery roles, responsibilities, procedures.
CP-4(1)	Contingency Plan Testing Coordinate With Related Plans							X	X		The organization coordinates contingency plan testing with organizational elements responsible for related plans.	
CP-4(2)	Contingency Plan Testing							X			The organization tests the contingency plan at the alternate processing site:	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
	Alternate Processing Site										a. To familiarize contingency personnel with the facility and available resources; and b. To evaluate the capabilities of the alternate processing site to support contingency operations.	
CP 6 Protect Function: PR.IP 4*	Alternate Storage Site							X	X		The organization: a. Establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information; and b. Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.	
CP-6(1)	Alternate Storage Site Separation From Primary Site							X	X		The organization identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.	
CP-6(2)	Alternate Storage Site Recovery Time / Point Objectives							X			The organization configures the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.	
CP-6(3)	Alternate Storage Site Accessibility							X	X		The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.	
CP 7 Protect Function: PR.IP 9, PR.PT 5*	Alternate Processing Site	X	X		X	X		X	X		The organization: a. Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of ***information system operations as defined in the contingency plan*** **[CNSS]** for essential missions/business functions within ***a time period as defined in the contingency plan*** **[CNSS]** when the primary processing capabilities are unavailable; and b. Ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the	

					I						Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
											site within the organization defined time period for transfer/resumption; and c. Ensures that the alternate processing site provides information security safeguards equivalent to those of the primary site.	
CP-7(1)	Alternate Processing Site Separation From Primary Site							X	X		The organization identifies an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats	
CP-7(2)	Alternate Processing Site Accessibility							X	X		The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.	
CP-7(3)	Alternate Processing Site Priority of Service							X	X		The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives).	
CP-7(4)	Alternate Processing Site Preparation For Use							X			The organization prepares the alternate processing site so that the site is ready to be used as the operational site supporting essential missions and business functions.	
CP 8 Identify Function; ID.BE 4* Protect Function: PR.PT 4, PR.PT 5*	Telecommunications Services							X	X		The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of ***Information system operations as defined in the contingency plan*** **[CNSS]** for essential missions and business functions within ***A time period as defined in the contingency plan*** **[CNSS]** when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
CP-8(1)	Telecommunications Services Priority of Service Provisions							X	X		The organization: a. Develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives); and b. Requests 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.	
CP-8(2)	Telecommunications Services Single Points of Failure							X	X		The organization obtains alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.	
CP-8(3)	Telecommunications Services Separation Of Primary / Alternate Providers							X			The organization obtains alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.	
CP-8(4)	Telecommunications Services Provider Contingency Plan							X			The organization: a. Requires primary and alternate telecommunications service providers to have contingency plans; b. Reviews provider contingency plans to ensure that the plans meet organizational contingency requirements; and c. Obtains evidence of contingency testing/training by providers [*Assignment: organization-defined frequency*].	
CP-8(5)	Telecommunications Services Alternate Telecommunication Service Testing							X			The organization tests alternate telecommunication services [*Assignment: organization-defined frequency*].	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
CP 9 Protect Function: PR.IP 4*	Information System Backup	X	X	X	X	X	X	X	X	X	The organization: a. Conducts backups of user level information contained in the information system ***at least weekly or as defined in the contingency plan*** **[CNSS]**; b. Conducts backups of system level information contained in the information system ***at least weekly or as defined in the contingency plan*** **[CNSS]**; c. Conducts backups of information system documentation including security related documentation ***when created, received, updated, or as defined in the contingency plan*** **[CNSS]**; and d. Protects the confidentiality, integrity, and availability of backup information at storage locations	
CP-9(1)	Information System Backup Testing For Reliability / Integrity				X	X		X	X		The organization tests backup information ***at least monthly or as defined in the contingency plan*** **[CNSS]** to verify media reliability and information integrity.	
CP-9(2)	Information System Backup Test Restoration Using Sampling							X			The organization uses a sample of backup information in the restoration of selected information system functions as part of contingency plan testing.	
CP-9(3)	Information System Backup Separate Storage For Critical Information							X			The organization stores backup copies of [*Assignment: organization-defined critical information system software and other security-related information*] in a separate facility or in a fire-rated container that is not collocated with the operational system.	
CP-9(5)	Information System Backup							X	X		The organization transfers information system backup information to the alternate storage site ***in accordance with the site backup policy and procedures*** **[DHS]**.	

					I						Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H		**L**	**H**	**M**	**L**	**H**		**L**	4300B.102	
	Transfer To Alternate Storage Site											
CP 10 Respond Function: RS.RP 1* Recover Function: RC.RP 1*	Information System Recovery and Reconstitution							X	X	X	The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.	
CP-10(2)	Information System Recovery and Reconstitution Transaction Recovery				X	X		X	X		The information system implements transaction recovery for systems that are transaction-based.	
CP-10(4)	Information System Recovery and Reconstitution Restore Within Time Period				X			X			The organization provides the capability to restore information system components within [*Assignment: organization-defined restoration time-periods*] from configuration-controlled and integrity-protected information representing a known, operational state for the components.	
CP 11 Identify Function: ID.BE 5* Protect Function: PR.PT 5*	Alternate Communications Protocols	X	X	X	X	X	X	X	X	X	The information system provides the capability to employ [Assignment: organization defined alternative communications protocols] in support of maintaining continuity of operations.	Contingency plans and the associated training and testing for those plans, incorporate an alternate communications protocol capability as part of increasing the resilience of organizational information systems. Alternate communications protocols include, for example, switching from Transmission Control Protocol/Internet Protocol (TCP/IP) Version 4 to TCP/IP Version 6. Switching communications protocols may affect software applications and therefore, the potential side effects of introducing alternate communications protocols are analyzed prior to implementation.

					I						Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
												Refer to *Cybersecurity Framework*, Version 1.1, April 16, 2018.
CP 12 Protect Function: PR.IP 9*	Safe Mode	X	X	X	X	X	X	X	X	X	The information system, when [Assignment: organization defined conditions] are detected, enters a safe mode of operation with [Assignment: organization defined restrictions of safe model of operation].	For information systems supporting critical missions/business functions including, for example, military operations and weapons systems, civilian space operations, nuclear power plant operations, and air traffic control operations (especially real time operational environments), organizations may choose to identify certain conditions under which those systems revert to a predefined safe mode of operation. The safe mode of operation, which can be activated automatically or manually, restricts the types of activities or operations information systems could execute when those conditions are encountered. Restriction includes, for example, allowing only certain functions that could be carried out under limited power or with reduced communications bandwidth. Refer to *Cybersecurity Framework*, Version 1.1, April 16, 2018.
CP 13 Protect Function: PR.PT 5, PR.IP 9*	Alternative Security Mechanisms	X	X	X	X	X	X	X	X	X	The organization employs [Assignment: organization defined alternative or supplemental security mechanisms] for satisfying [Assignment: organization defined security functions] when the primary means of implementing the security functions is unavailable or compromised.	This control supports information systems resiliency and contingency planning/continuity of operations. To ensure mission/business continuity, organizations can implement alternative or supplemental security mechanisms. These mechanisms may be less effective than the primary mechanisms (e.g., not as easy to use, not as scalable, or not as secure). However, having the capability to readily employ these alternative/supplemental mechanisms enhances overall mission/business continuity that might otherwise be adversely impacted if organizational operations had to be curtailed until the primary means of implementing the functions was restored. Given the cost and level of effort required to provide such alternative capabilities, this control would typically be applied only to critical security capabilities provided by information systems, system components, or information system services. For example, an organization may issue to senior executives and System Administrators one time pads in case multifactor tokens, the organization s standard means for secure remote authentication is compromised. Refer to *Cybersecurity Framework*, Version 1.1, April 16, 2018.

Identification and Authentication (IA)

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
IA 1 Protect Function: PR.AC 1, PR.AC 6, PR.AC 7*	Identification and Authentication Policy and Procedures	X	X	X	X	X	X				The organization: a. Develops, documents, and disseminates to ***all personnel*** **[CNSS]**: 1. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls; and b. Reviews and updates the current: 1. Identification and authentication ***policy at least annually if not otherwise defined in formal organizational policy*** **[CNSS]**; and 2. Identification and authentication procedures ***at least annually if not otherwise defined in formal organizational policy*** **[CNSS]**.	The DHS NSS 4300B Policy, along with the proper application and documentation of all relevant (IA) baseline controls, CNSS and DHS defined values, supplemental guidance, and any inheritable network or enterprise controls provide the basis for satisfying IA 1. However, the ISO is ultimately responsible for addressing any and all (IA) policy and procedures within the SSP.
IA 2 Protect Function: PR.AC 1, PR.AC 6, PR.AC 7*	Identification and Authentication (Organizational Users)	X	X	X	X	X	X				The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).	
IA-2(1)	Identification and Authentication (Organizational Users) Network Access to Privileged Accounts	X	X	X	X	X	X				The information system implements multifactor authentication for network access to privileged accounts.	
IA-2(2)	Identification and Authentication (Organizational Users)	X	X	X	X	X	X				The information system implements multifactor authentication for network access to non-privileged accounts.	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
	Network Access to Non - Privileged Accounts											
IA-2(3)	Identification and Authentication (Organizational Users) Local Access to Privileged Accounts	X	X		X	X					The information system implements multifactor authentication for local access to privileged accounts.	
IA-2(4)	Identification and Authentication (Organizational Users) Local Access to Non - Privileged Accounts	X	X		X	X					The information system implements multifactor authentication for local access to non-privileged accounts.	
IA-2(5)	Identification and Authentication (Organizational Users) Group Authentication	X	X	X	X	X	X				The organization requires individuals to be authenticated with an individual authenticator when a group authenticator is employed	
IA-2(8)	Identification and Authentication (Organizational Users) Network Access to Privileged Accounts - Replay Resistant	X	X	X	X	X	X				The information system implements replay-resistant authentication mechanisms for network access to privileged accounts.	
IA-2(9)	Identification and Authentication (Organizational Users) Network Access to Non-Privileged Accounts - Replay Resistant	X	X		X	X					The information system implements replay-resistant authentication mechanisms for network access to non-privileged accounts.	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
IA-2(11)	Identification and Authentication (Organizational Users) Remote Access - Separate Device	X	X	X	X	X	X				The information system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets ***at least FIPS 140-2 Security Level 4 requirements*** **[DHS]**.	
IA-2(12)	Identification and Authentication (Organizational Users) Acceptance of PIV Credentials	X	X	X	X	X	X				The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials.	
IA 3 Protect Function: PR.AC 1, PR.AC 7*	Device Identification and Authentication	X	X	X	X	X	X				The information system uniquely identifies and authenticates ***all network connected endpoint devices*** **[CNSS]** before establishing a ***network connection*** **[DHS]**.	
IA-3(1)	Device Identification and Authentication Cryptographic Bidirectional Authentication	X	X		X	X					The information system authenticates ***all DHS approved devices (e.g., Laptop, tablet, etc.)*****[DHS]** before establishing ***a local, remote, or network*** **[DHS]** connection using bidirectional authentication that is cryptographically based.	
IA 4 Protect Function: PR.AC 1, PR.AC 6*	Identifier Management	X	X	X	X	X	X				The organization manages information system identifiers for users and devices by: a. Receiving authorization from ***a designated organizational official*** **[DHS]** to assign an individual, group, role, or device identifier; b. Selecting an identifier that identifies an individual, group, role, or device; c. Assigning the identifier to the intended individual, group, role, or device; d. Preventing reuse of identifiers for ***at least one year for individuals, groups or roles*** **[CNSS]**; and	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
											e. Disabling the identifier after ***not to exceed 35 days for individuals, groups, or roles*** **[CNSS]**.	
IA-4(4)	Identifier Management Identify User Status	X	X	X	X	X	X				The organization manages identifiers by uniquely identifying each individual as ***a contractor or government employee and citizenship*** **[CNSS]**.	
IA 5 Protect Function: PR.AC 1, PR.AC 6, PR.AC 7*	Authenticator Management	X	X	X	X	X	X				The organization manages information system authenticators for users and devices by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator; b. Establishing initial authenticator content for authenticators defined by the organization; c. Ensuring that authenticators have sufficient strength of mechanism for their intended use; d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators; e. Changing default content of authenticators prior to information system installation; f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators; g. Changing/refreshing authenticators ***not to exceed 180 days for passwords*** **[CNSS]**; h. Protecting authenticator content from unauthorized disclosure and modification; i. Requiring users to take, and having devices implement, specific measures to safeguard authenticators; and j. Changing authenticators for group/role accounts when membership to those accounts changes.	DHS HSDN Public Key Infrastructure (PKI) Tokens are good for 3 years. Level 4 encryption. DHS utilizes DOD/DISA NSS Common Service Provider (CSP) that is subordinated to the NSS Root (operated by NSA) to deploy PKI on the HSDN.
IA-5(1)	Authenticator Management Password-based Authentication	X	X	X	X	X	X				The information system, for password-based authentication: a. Enforces minimum password complexity ***of a case sensitive 12-character mix of upper case letters, lower case letters, numbers and special characters including at least one of each*** **[CNSS]**; ***no more than three consecutive characters from a single class, does not***	CNSS Note: The requirements do not apply to one-time use passwords.

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
											include the user's account name or full name **[DHS]**; b. Enforces at least the following number of changed characters when new passwords are created: ***50% of the characters*** **[CNSS]**; c. Stores and transmits only cryptographically-protected passwords; d. Enforces password minimum and maximum lifetime restrictions of ***minimum of 24 hours and 180 days maximum*** **[CNSS]**; e. Prohibits password reuse for ***a minimum of 10*** **[CNSS]** generations; and f. Allows the use of a temporary password for system logons with an immediate change to a permanent password.	
IA-5(2)	Authenticator Management PKI-based Authentication	X	X		X	X					The information system, for PKI-based authentication: a. Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information; b. Enforces authorized access to the corresponding private key; c. Maps the authenticated identity to the account of the individual or group; and d. Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.	
IA-5(3)	Authenticator Management In-Person or Trusted Third-Party Registration				X	X					The organization requires that the registration process to receive ***a hard token*** **[DHS]** be conducted ***in person*** **[DHS]** before ***a designated registration authority*** **[DHS]** with authorization by ***a supervisor*** **[DHS]**.	
IA-5(4)	Authenticator Management	X	X	X	X	X	X				The organization employs automated tools to determine if password authenticators are sufficiently strong to satisfy ***the requirements set forth in IA-5(1)*** **[DHS]**.	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
	Automated Support for Password Strength Determination											
IA-5(7)	Authenticator Management No Embedded Unencrypted Static Authenticators	X	X	X							The organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys.	
IA-5(8)	Authenticator Management Multiple Information System Accounts	X	X	X	X	X	X				The organization implements ***precautions including advising users not to use the same password for any of the following:*** ***• Domains of differing classification levels.*** ***• More than one domain of a classification level (e.g., internal agency network and Interlink).*** ***• More than one privilege level (e.g., user, administrator)*** **[CNSS]** to manage the risk of compromise due to individuals having accounts on multiple information systems.	
IA-5(11)	Authenticator Management Hardware Token-based Authentication				X	X	X				The information system, for hardware token-based authentication, employs mechanisms that satisfy ***FIPS 140-2 Security Level 4 requirements*** **[DHS]**.	Homeland Security Presidential Directive-12 (HSPD-12), Level 4 devices, applications, code-signing, and web certificates
IA-5(13)	Authenticator Management Expiration of Cached Authenticators	X	X	X	X	X	X				The information system prohibits the use of cached authenticators after ***One (1) hour*** **[CNSS]**.	
IA-5(14)	Authenticator Management Managing Content of PKI Trust Stores	X	X	X	X	X	X				The organization, for PKI-based authentication, employs a deliberate organization-wide methodology for managing the content of PKI trust stores installed across all platforms including networks, operating systems, browsers, and applications.	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
IA 6 Protect Function; PR.AC 1*	Authenticator Feedback	X	X	X							The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	
IA 7 Protect Function: PR.AC 1*	Cryptographic Module Authentication	X	X	X	X	X	X				The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.	
IA 8 Protect Function: PR.AC 1, PR.AC 6, PR.AC 7*	Identification and Authentication (Non Organizational Users)	X	X	X	X	X	X				The information system uniquely identifies and authenticates non organizational users (or processes acting on behalf of non organizational users).	
IA-8(1)	Identification and Authentication (Non-Organizational Users) Acceptance of PIV Credentials from other Agencies	X	X	X	X	X	X				The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies.	
IA-8(2)	Identification and Authentication (Non-Organizational Users) Acceptance of Third-Party Credentials				X	X	X				The information system accepts only Federal Identity Credential and Access Management (FICAM)-approved third-party credentials.	This control enhancement typically applies to organizational information systems that are accessible to the general public, for example, public-facing websites.
IA-8(3)	Identification and Authentication (Non-Organizational Users)				X	X	X				The organization employs only FICAM-approved information system components in [*Assignment: organization-defined information systems*] to accept third-party credentials.	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
	Use of FICAM-Approved Products											
IA-8(4)	Identification and Authentication (Non-Organizational Users) Use of FICAM-Issued Profiles				X	X	X				The information system conforms to FICAM-issued profiles.	
IA 9 Protect Function: PR.AC 1, PR.AC 7*	Service Identification and Authentication	X	X	X	X	X	X	X	X	X	The organization identifies and authenticates [Assignment: organization defined information system services] using [Assignment: organization defined security safeguards].	This control supports service oriented architectures and other distributed architectural approaches requiring the identification and authentication of information system services. In such architectures, external services often appear dynamically. Therefore, information systems should be able to determine in a dynamic manner, if external providers and associated services are authentic. Safeguards implemented by organizational information systems to validate provider and service authenticity include, for example, information or code signing, provenance graphs, and/or electronic signatures indicating or including the sources of services. Refer to *Cybersecurity Framework*, Version 1.1, April 16, 2018.
IA 10 Protect Function: PR.AC 1, PR.AC 7*	Adaptive Identification and Authentication	X			X						The organization requires that individuals accessing the information system employ [*Assignment: organization defined supplemental authentication techniques or mechanisms*] under specific [*Assignment: organization defined circumstances or situations*].	
IA 11 Protect Function; PR.AC 1, PR.AC 7*	Re Authentication	X			X						The organization requires users and devices to re authenticate when ***the execution of privileged functions occur*** **[DHS]**.	

Incident Response (IR)

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
IR-1	Incident Response Policy and Procedures	X	X	X	X	X	X	X	X	X	The organization: a. Develops, documents, and disseminates to ***key personnel or roles and organizational elements identified in the Incident Response plan*** **[DHS]**: 1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and b. Reviews and updates the current: 1. Incident response policy ***at least annually if not otherwise defined in organizational policy*** **[CNSS]**;and 2. Incident response procedures ***at least annually if not otherwise defined in organizational policy*** **[CNSS]**.	The DHS NSS 4300B Policy, along with the proper application and documentation of all relevant (IR) baseline controls, CNSS and DHS defined values, supplemental guidance, and any inheritable network or enterprise controls provide the basis for satisfying IR-1. However, the ISO is ultimately responsible for addressing any and all (IR) policy and procedures within the SSP. References: NIST SP 800-61, Computer Security Incident Handling Guide CNSSI No. 1001, National Instruction on Classified Information Spillage
IR 2 Protect Function: PR.AT 5*	Incident Response Training	X	X	X	X	X	X	X	X	X	The organization provides incident response training to information system users consistent with assigned roles and responsibilities: a. Within ***30 working days*** **[CNSS]** of assuming an incident response role or responsibility; b. When required by information system changes; and c. ***at least annually*** **[CNSS]** thereafter.	
IR-2(1)	Incident Response Training Simulated Events	X			X			X			The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.	
IR-2(2)	Incident Response Training Automated Training Environments				X			X			The organization employs automated mechanisms to provide a more thorough and realistic incident response training environment.	
IR 3 Identify Function: ID.SC 5*	Incident Response Testing	X	X	X	X	X	X	X	X	X	The organization tests the incident response capability for the information system ***at least annually*** **[CNSS]** using ***hot washes of actual events that occurred during the past year*** **[DHS]** to determine the incident response effectiveness and documents the results.	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
Protect Function: PR.IP 10* Respond Function: RS.CO 1*												
IR-3(2)	Incident Response Testing Coordination With Related Plans	X	X		X	X		X	X		The organization coordinates incident response testing with organizational elements responsible for related plans.	
IR 4 Identify Function: ID.SC 5* Detect Function: DE.AE 2, DE.AE 3, DE.AE 4, DE.AE 5* Respond Function: RS.RP 1, RS.CO 3, RS.CO 4, RS.AN 1, RS.AN 2, RS.AN 3, RS.AN 4, RS.MI 1, RS.MI 2, RS.IM 1, RS.IM 2* Recover	Incident Handling	X	X	X	X	X	X	X	X	X	The organization: a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; b. Coordinates incident handling activities with contingency planning activities; and c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implements the resulting changes accordingly.	Components shall follow the DHS Privacy Incident Handling Guide. Reference DHS guidance/policy for insider threats at the following document titled Information Sharing and Safeguarding: Insider Threat Program

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
Function: RC.RP 1, RC.IM 1, RC.IM 2, RC.CO 3*												
IR-4(1)	Incident Handling Automated Incident Handling Processes	X	X		X	X		X	X		The organization employs automated mechanisms to support the incident handling process.	
IR-4(3)	Incident Handling Continuity of Operations	X	X		X	X		X	X		The organization identifies [*Assignment: organization-defined classes of incidents*] and [*Assignment: organization-defined actions to take in response to classes of incidents*] to ensure continuation of organizational missions and business functions.	
IR-4(4)	Incident Handling Information Correlation	X	X	X	X	X	X	X	X	X	The organization correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.	
IR-4(6)	Incident Handling Insider Threats - Specific Capabilities	X	X	X	X	X	X	X	X	X	The organization implements incident handling capability for insider threats.	
IR-4(7)	Incident Handling Insider Threats - Intra-Organization Coordination	X	X	X	X	X	X	X	X	X	The organization coordinates incident handling capability for insider threats across [*Assignment: organization-defined components or elements of the organization*].	
IR-4(8)	Incident Handling Correlation With External Organizations	X	X	X	X	X	X	X	X	X	The organization coordinates ***with the appropriate CIRT/Computer Emergency Readiness Team (CERT) (such as US-CERT, DoD CERT, IC CERT)*** **[CNSS]** to correlate and share [*Assignment: organization-defined incident information*] to achieve a cross-organization perspective on incident awareness and more effective incident responses.	
IR 5 Detect Function: DE.AE 3, DE.AE 5*	Incident Monitoring	X	X	X	X	X	X	X	X	X	The organization tracks and documents information system security incidents.	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
Respond Function: RS.AN 1, RS.AN 4*												
IR-5(1)	Incident Monitoring Automated Tracking / Data Collection / Analysis	X			X			X			The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.	
IR 6 Identify Function: ID.SC 5* Respond Function: RS.CO 2*	Incident Reporting	X	X	X	X	X	X	X	X	X	The organization: a. Requires personnel to report suspected security incidents to the organizational incident response capability within ***2 hours if not otherwise defined in formal organizational policy*** **[CNSS]**; and b. Reports security incident information to the ***appropriate agency CIRT/CERT*** **[CNSS]**.	
IR-6(1)	Incident Reporting Automated Reporting	X	X		X	X		X	X		The organization employs automated mechanisms to assist in the reporting of security incidents.	
IR-6(2)	Incident Reporting Vulnerabilities Related to Incidents	X	X	X	X	X	X	X	X	X	The organization reports information system vulnerabilities associated with reported security incidents to [*Assignment: organization-defined personnel or roles*].	
IR 7 Protect Function: PR.IP 9*	Incident Response Assistance	X	X	X	X	X	X	X	X	X	The organization provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.	
IR-7(1)	Incident Response Assistance Automation Support For Availability of Information / Support	X	X		X	X		X	X		The organization employs automated mechanisms to increase the availability of incident response-related information and support.	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
IR-7(2)	Incident Response Assistance Coordination With External Providers	X	X	X	X	X	X	X	X	X	The organization: a. Establishes a direct, cooperative relationship between its incident response capability and external providers of information system protection capability; and b. Identifies organizational incident response team members to the external providers.	
IR 8 Identify Function: ID.SC 5* Protect Function: PR.IP 7, PR.IP 9* Detect Function: DE.AE 3, DE.AE 5* Respond Function: RS.RP 1, RS.CO 1, RS.CO 2, RS.CO 3, RS.CO 4, RS.AN 4, RS.IM 1, RS.IM 2* Recover Function: RC.RP 1, RC.IM 1, RC.IM 2*	Incident Response Plan	X	X	X	X	X	X	X	X	X	The organization: a. Develops an incident response plan that: 1. Provides the organization with a roadmap for implementing its incident response capability; 2. Describes the structure and organization of the incident response capability; 3. Provides a high level approach for how the incident response capability fits into the overall organization; 4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; 5. Defines reportable incidents; 6. Provides metrics for measuring the incident response capability within the organization; 7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and 8. Is reviewed and approved by ***CISO/SISO if not otherwise defined in formal organizational policy*** **[CNSS]**; b. Distributes copies of the incident response plan to ***all personnel with a role or responsibility for implementing the incident response plan*** **[CNSS]**; c. Reviews the incident response plan ***at least annually (incorporating lessons learned from past incidents)*** **[CNSS]**; d. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; e. Communicates incident response plan changes to ***all personnel with a role or responsibility for implementing the incident response plan, not later than 30 days after the change is made*** **[CNSS]**; and	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
											f. Protects the incident response plan from unauthorized disclosure and modification.	
IR 9 Identify Function: ID.SC 5* Protect Function: PR.IP 9*	Information Spillage Response	X	X	X							The organization responds to information spills by: a. Identifying the specific information involved in the information system contamination; b. Alerting [*Assignment: organization defined personnel or roles*] of the information spill using a method of communication not associated with the spill; c. Isolating the contaminated information system or system component; d. Eradicating the information from the contaminated information system or component; e. Identifying other information systems or system components that may have been subsequently contaminated; and f. Performing other ***post spillage activities such as lessons learned reports*** **[DHS]**.	
IR-9(1)	Information Spillage Response Responsible Personnel	X	X	X							The organization assigns [*Assignment: organization-defined personnel or roles*] with responsibility for responding to information spills.	
IR-9(2)	Information Spillage Response Training	X	X	X							The organization provides information spillage response training ***annually*** **[CNSS]**.	
IR-9(3)	Information Spillage Response Post-Spill Operations							X	X		The organization implements [*Assignment: organization-defined procedures*] to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions.	
IR-9(4)	Information Spillage Response Exposure to Unauthorized Personnel	X	X	X							The organization employs [*Assignment: organization-defined security safeguards*] for personnel exposed to information not within assigned access authorizations.	
IR-10	Integrated Information Security Cell	X	X		X	X		X	X		The organization establishes an integrated team of forensic/malicious code analysts, tool developers, and real-time operations personnel.	

Maintenance (MA)

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
MA-1	System Maintenance Policy and Procedures	X	X	X	X	X	X	X	X	X	The organization: a. Develops, documents, and disseminates to ***all personnel*** **[CNSS]**: 1. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; and b. Reviews and updates the current: 1. System maintenance policy ***at least annually if not otherwise defined in formal organizational policy*** **[CNSS]**; and 2. System maintenance procedures ***at least annually if not otherwise defined in formal organizational policy*** **[CNSS]**.	The DHS NSS 4300B Policy, along with the proper application and documentation of all relevant (MA) baseline controls, CNSS and DHS defined values, supplemental guidance, and any inheritable network or enterprise controls provide the basis for satisfying MA-1. However, the ISO is ultimately responsible for addressing any and all (MA) policy and procedures within the SSP.
MA 2 Protect Function: PR.MA 1*	Controlled Maintenance	X	X	X	X	X	X	X	X	X	The organization: a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements; b. Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location; c. Requires that [*Assignment: organization defined personnel or roles*] explicitly approve the removal of the information system or system components from organizational facilities for off site maintenance or repairs; d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off site maintenance or repairs; e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and f. Includes [*Assignment: organization defined maintenance related information*] in organizational maintenance records.	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
MA-2(2)	Controlled Maintenance Automated Maintenance Activities	X			X			X			The organization: a. Employs automated mechanisms to schedule, conduct, and document maintenance and repairs; and b. Produces up-to date, accurate, and complete records of all maintenance and repair actions requested, scheduled, in process, and completed.	
MA 3 Protect Function; PR.MA 1*	Maintenance Tools				X	X	X				The organization approves, controls, and monitors information system maintenance tools.	
MA-3(1)	Maintenance Tools Inspect Tools				X	X					The organization inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.	
MA-3(2)	Maintenance Tools Inspect Media				X	X	X				The organization checks media containing diagnostic and test programs for malicious code before the media are used in the information system.	
MA-3(3)	Maintenance Tools Prevent Unauthorized Removal	X	X	X							The organization prevents the unauthorized removal of maintenance equipment containing organizational information by: a. Verifying that there is no organizational information contained on the equipment; b. Sanitizing or destroying the equipment; c. Retaining the equipment within the facility; or d. Obtaining an exemption from [Assignment: organization-defined personnel or roles] explicitly authorizing removal of the equipment from the facility.	
MA 4 Protect Function: PR.MA 2*	Non Local Maintenance				X	X	X				The organization: a. Approves and monitors nonlocal maintenance and diagnostic activities; b. Allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system; c. Employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions;	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
											d. Maintains records for nonlocal maintenance and diagnostic activities; and e. Terminates session and network connections when nonlocal maintenance is completed.	
MA-4(1)	Non-Local Maintenance Auditing and Review				X	X					The organization: a. Audits nonlocal maintenance and diagnostic sessions ***As defined in the organizations formal audit policy (AU-1)*** **[CNSS]**; and b. Reviews the records of the maintenance and diagnostic sessions.	
MA-4(2)	Non-Local Maintenance Document Nonlocal Maintenance				X	X					The organization documents in the security plan for the information system, the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.	
MA-4(3)	Non-Local Maintenance Comparable Security / Sanitization	X	X	X	X	X	X				The organization: a. Requires that nonlocal maintenance and diagnostic services be performed from an information system that implements a security capability comparable to the capability implemented on the system being serviced; or b. Removes the component to be serviced from the information system prior to nonlocal maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially malicious software) before reconnecting the component to the information system.	
MA-4(6)	Non-Local Maintenance Cryptographic Protection	X	X	X	X	X	X				The information system implements cryptographic mechanisms to protect the integrity and confidentiality of nonlocal maintenance and diagnostic communications	
MA-4(7)	Non-Local Maintenance Remote Disconnect Verification				X	X	X				The information system implements remote disconnect verification at the termination of nonlocal maintenance and diagnostic sessions.	
MA 5 Protect	Maintenance Personnel	X	X	X	X	X	X	X	X	X	The organization: a. Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel;	

					I						Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
Function: PR.MA 1*											b. Ensures that non escorted personnel performing maintenance on the information system have required access authorizations; and c. Designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.	
MA-5(1)	Maintenance Personnel Individuals Without Appropriate Access	X			X			X			The organization: a. Implements procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements: 1. Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the information system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified; 2. Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the information system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; and b. Develops and implements alternate security safeguards in the event an information system component cannot be sanitized, removed, or disconnected from the system.	
MA 6 Protect Function: PR.MA 1*	Timely Maintenance							X	X		The organization obtains maintenance support and/or spare parts for ***critical information systems as defined by the organization*** **[DHS]** within ***the time period specified by the organization*** **[DHS]** of failure.	

Media Protection (MP)

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
MP-1	Media Protection Policy and Procedures	X	X	X	X	X	X				The organization: a. Develops, documents, and disseminates to ***all personnel*** **[CNSS]**: 1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls; and b. Reviews and updates the current: 1. Media protection policy ***at least annually if not otherwise defined in formal organizational policy*** **[CNSS]**; and 2. Media protection procedures ***at least annually if not otherwise defined in formal organizational policy*** **[CNSS]**.	The DHS NSS 4300B Policy, along with the proper application and documentation of all relevant (MP) baseline controls, CNSS and DHS defined values, supplemental guidance, and any inheritable network or enterprise controls provide the basis for satisfying MP-1. However, the ISO is ultimately responsible for addressing any and all (MP) policy and procedures within the SSP. References: DHS Instruction 121-01-011, *The Department of Homeland Security Administrative Security Program* NSA Central Security Service (CSS) Policy Manual 9-12, *Storage Device Declassification Manual*
MP 2 Protect Function: PR.PT 2*	Media Access	X	X	X	X	X	X				The organization restricts access to ***all removable digital and non digital media including, but not limited to, hard disks, floppy disks, zip drives, CDs, DVDs, thumb drives, pen drives, flash drives, and similar universal serial bus (USB) storage devices*** **[DHS]** to ***AO or designee authorized individuals in the performance of assigned duties*** **[DHS]**.	All removable media used in conjunction with NSS shall have the capability to protect (control/disable) read/write functionality of the media.
MP 3 Protect Function: PR.PT 2*	Media Marking	X	X								The organization: a. Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and b. Exempts ***no media*** **[DHS]** from marking as long as the media remains within [*Assignment: organization defined controlled areas*].	Refer to DHS Instruction 121 01 011, *The Department of Homeland Security Administrative Security Program.*
MP 4 Protect Function: PR.PT 2*	Media Storage	X	X		X	X					The organization: a. Physically controls and secures ***digital and non digital media containing sensitive, controlled, and/or classified information*** **[CNSS]** within ***an area or container approved for processing and storing media based on the sensitivity and/or classification of the information maintained within the media*** **[CNSS]**; and	Refer to DHS Instruction 121 01 011, *The Department of Homeland Security Administrative Security Program*

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
											b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.	
MP 5 Protect Function: PR.PT 2*	Media Transport	X	X		X	X					The organization: a. Protects and controls ***digital and non digital media containing sensitive, controlled, and/or classified information*** **[CNSS]** during transport outside of controlled areas ***using security measures established by the DHS Office of Security*** **[DHS]**; b. Maintains accountability for information system media during transport outside of controlled areas; c. Documents activities associated with the transport of information system media; and d. Restricts the activities associated with the transport of information system media to authorized personnel.	DHS Components shall comply with the requirements of DHS Instruction 121 01 011, *The Department of Homeland Security Administrative Security Program*.
MP-5(4)	Media Transport Cryptographic Protection	X	X		X	X					The information system implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.	All removable media used in conjunction with NSS shall have the capability to protect (control/disable) read/write functionality of the media. All media from non-DHS sources shall only be introduced for use on DHS NSS after all approvals have been obtained by designated authorities and properly documented. All media shall be scanned for viruses, preferably on a standalone machine approved for the level of classified information contained on the media. The media will not be returned to the provider if the media is introduced to a system that already contains classified information.
MP 6 Protect Function: PR.DS 3, PR.IP 6*	Media Sanitization	X	X	X							The organization: a. Sanitizes [*Assignment: organization defined information system media*] prior to disposal, release out of organizational control, or release for reuse using [*Assignment: organization defined sanitization techniques and procedures*] in accordance with applicable federal and organizational standards and policies; and b. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.	DHS Components shall comply with DHS Instruction 121 01 011, *The Department of Homeland Security Administrative Security Program*, and NSA CSS Policy Manual 9 12, *Storage Device Declassification Manual*, for digital/electronic media.

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
MP-6(1)	Media Sanitization Review / Approve / Track / Document / Verify	X									The organization reviews, approves, tracks, documents, and verifies media sanitization and disposal actions.	Refer to DHS Instruction 121-01-011, *The Department of Homeland Security Administrative Security Program*.
MP-6(2)	Media Sanitization Equipment Testing	X									The organization tests sanitization equipment and procedures ***at least annually if not otherwise defined in formal organizational policy*** **[CNSS]** to verify that the intended sanitization is being achieved.	
MP-6(3)	Media Sanitization Nondestructive Techniques	X									The organization applies nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the information system under the following circumstances: ***when such devices are first purchased from the manufacturer or vendor prior to initial use, when being considered for reuse, or when the organization loses a positive chain of custody for the device. Media obtained from unknown sources shall not be sanitized and reused*** **[DHS]**.	
MP 7 Protect Function: PR.PT 2*	Media Use	X	X	X	X	X	X				The organization [*Selection: restricts; prohibits*] the use of [*Assignment: organization defined types of information system media*] on [*Assignment: organization defined information systems or system components*] using [*Assignment: organization defined security safeguards*].	
MP-7(1)	Media Use Prohibit Use without Owner				X	X	X				The organization prohibits the use of portable storage devices in organizational information systems when such devices have no identifiable owner.	
MP 8 Protect Function: PR.DS 1, PR.PT 2*	Media Downgrading	X	X	X	X	X	X	X	X	X	The organization: a. Establishes [Assignment: organization defined information system media downgrading process] that includes employing downgrading mechanisms with [Assignment: organization defined strength and integrity]; b. Ensures that the information system media downgrading process is commensurate with the security category and/or classification level of the information to be removed and the access authorizations of the potential recipients of the downgraded information; c. Identifies [Assignment: organization defined	This control applies to all information system media, digital, and non digital, subject to release outside of the organization, whether or not the media is considered removable. The downgrading process, when applied to system media, removes information from the media, typically by security category or classification level, such that the information from the media, typically by security category or classification level, such that the information cannot be retrieved or reconstructed. Downgrading of media includes redacting information to enable wider release and distribution. Downgrading of media also ensures that empty space on the media (e.g., slack space within files) is devoid of information.

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
											information system media requiring downgrading]; and d. Downgrades the identified information system media using the established process.	Refer to *Cybersecurity Framework*, Version 1.1, April 16, 2018.

Physical and Environmental Protection (PE)

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
PE-1	Physical and Environmental Protection Policy and Procedures	X	X	X	X	X	X	X	X	X	The organization: a. Develops, documents, and disseminates to ***all personnel*** **[CNSS]**: 1. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and b. Reviews and updates the current: 1. Physical and environmental protection policy ***at least annually if not otherwise defined in formal organizational policy*** **[CNSS]**; and 2. Physical and environmental protection procedures ***at least annually if not otherwise defined in formal organizational policy*** **[CNSS]**.	The DHS NSS 4300B Policy, along with the proper application and documentation of all relevant (PE) baseline controls, CNSS and DHS defined values, supplemental guidance, and any inheritable network or enterprise controls provide the basis for satisfying PE-1. However, the ISO is ultimately responsible for addressing any and all (PE) policy and procedures within the SSP. References: DHS Instruction 121-01-011, *The Department of Homeland Security Administrative Security Program* NSTISSAM TEMPEST 2-95A for exact requirements
PE 2 Protect Function: PR.AC 2, PR.AC 6*	Physical Access Authorizations	X	X	X	X	X	X	X	X	X	The organization: a. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides; b. Issues authorization credentials for facility access; c. Reviews the access list detailing authorized facility access by individuals ***at least annually*** **[CNSS]**; and d. Removes individuals from the facility access list when access is no longer required.	
PE 3 Protect Function: PR.AC 2* Detect Function: DE.CM 2,	Physical Access Control	X	X	X	X	X	X	X	X	X	The organization: a. Enforces physical access authorizations at [*Assignment: organization defined entry/exit points to the facility where the information system resides*] by; 1. Verifying individual access authorizations before granting access to the facility; and 2. Controlling ingress/egress to the facility using [*Selection (one or more): [Assignment: organization defined physical access control systems/devices]; guards*];	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
DE.CM 7, DE.DP 3*											b. Maintains physical access audit logs for [*Assignment: organization defined entry/exit points*]; c. Provides [*Assignment: organization defined security safeguards*] to control access to areas within the facility officially designated as publicly accessible; d. Escorts visitors and monitors visitor activity [*Assignment: organization defined circumstances requiring visitor escorts and monitoring*]; e. Secures keys, combinations, and other physical access devices; f. Inventories [*Assignment: organization defined physical access devices*] every [*Assignment: organization defined frequency*]; and g. Changes combinations and keys ***when first installed or used; if believed to have been subjected to compromise, and when considered necessary by the cognizant security authority (CSA)*** **[DHS]** and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.	
PE-3(1)	Physical Access Control Information System Access	X	X	X	X	X	X				The organization enforces physical access authorizations to the information system in addition to the physical access controls for the facility at [*Assignment: organization-defined physical spaces containing one or more components of the information system*].	
PE 4 Protect Function: PR.AC 2*	Access Control For Transmission Medium	X	X		X	X					The organization controls physical access to [*Assignment: organization defined information system distribution and transmission lines*] within organizational facilities using [*Assignment: organization defined security safeguards*].	
PE 5 Protect Function: PR.AC 2*	Access Control For Output Devices	X	X								The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.	
PE 6 Protect	Monitoring Physical Access	X	X	X	X	X	X	X	X	X	The organization:	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
Function: PR.AC 2* Detect Function: DE.CM 2, DE.CM 7* Respond Function: RS.CO 3, RS.AN 1*											a. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents; b. Reviews physical access logs ***at least every 90 days if not otherwise defined in formal organizational policy*** **[CNSS]** and upon occurrence of [*Assignment: organization defined events or potential indications of events*]; and c. Coordinates results of reviews and investigations with the organizational incident response capability.	
PE-6(1)	Monitoring Physical Access Intrusion Alarms / Surveillance Equipment	X	X		X	X		X	X		The organization monitors physical intrusion alarms and surveillance equipment.	
PE-6(4)	Monitoring Physical Access Monitoring Physical Access to Information Systems	X			X			X			The organization monitors physical access to the information system in addition to the physical access monitoring of the facility as [*Assignment: organization-defined physical spaces containing one or more components of the information system*].	
PE 8 Protect Function: PR.AC 2*	Visitor Access Records	X	X	X	X	X	X	X	X	X	The organization: a. Maintains visitor access records to the facility where the information system resides ***for at least one year*** **[CNSS]**; and b. Reviews visitor access records ***at least every 90 days if not otherwise defined in formal organizational policy*** **[CNSS]**.	
PE-8(1)	Visitor Access Records Automated Records Maintenance / Review	X			X						The organization employs automated mechanisms to facilitate the maintenance and review of visitor access records.	
PE 9 Identify Function: ID.BE 4*	Power Equipment and Cabling							X	X		The organization protects power equipment and power cabling for the information system from damage and destruction.	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
PE 10 Protect Function: PR.IP 5*	Emergency Shutoff							X	X		The organization: a. Provides the capability of shutting off power to the information system or individual system components in emergency situations; b. Places emergency shutoff switches or devices in ***a location defined by the organization*** **[DHS]** to facilitate safe and easy access for personnel; and c. Protects emergency power shutoff capability from unauthorized activation.	
PE 11 Identify Function: ID.BE 4*	Emergency Power							X	X		The organization provides a short term uninterruptible power supply to facilitate [*Selection (one or more): an orderly shutdown of the information system; transition of the information system to long term alternate power*] in the event of a primary power source loss.	
PE-11(1)	Emergency Power Long-Term Alternate Power Supply - Minimal Operational Capability							X			The organization provides a long-term alternate power supply 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.	
PE 12 Protect Function: PR.IP 5*	Emergency Lighting							X	X	X	The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.	
PE 13 Protect Function: PR.IP 5*	Fire Protection							X	X	X	The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.	
PE-13(1)	Fire Protection Detection Devices / Systems							X			The organization employs fire detection devices/systems for the information system that activate automatically and notify [*Assignment: organization-defined personnel or roles*] and [*Assignment: organization-defined emergency responders*] in the event of a fire.	
PE-13(2)	Fire Protection							X			The organization employs fire suppression devices/systems for the information system	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
	Suppression Devices / Systems										that provide automatic notification of any activation to [*Assignment: organization-defined personnel or roles*] and [*Assignment: organization-defined emergency responders*].	
PE-13(3)	Fire Protection Automatic Fire Suppression							X	X		The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.	
PE-13(4)	Fire Protection Inspections							X			The organization ensures that the facility undergoes ***at least annually if not otherwise defined in formal organizational policy*** **[CNSS]** inspections by authorized and qualified inspectors and resolves identified deficiencies within ***60 days*** **[CNSS]**.	
PE 14 Protect Function: PR.IP 5*	Temperature and Humidity Controls							X	X	X	The organization: a. Maintains temperature and humidity levels within the facility where the information system resides ***based on DHS supplemental guidance*** **[DHS]**; and b. Monitors temperature and humidity levels ***continuously*** **[CNSS]**.	Reference American Society of Heating, Refrigeration and Air Conditioning Engineers (ASHRAE) for temperature and humidity guidelines. 64.4 80.6 degrees Fahrenheit 40% 60% relative humidity
PE 15 Protect Function: PR.IP 5*	Water Damage Protection							X	X	X	The organization protects the information system from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.	
PE-15(1)	Water Damage Protection Automation Support							X			The organization employs automated mechanisms to detect the presence of water in the vicinity of the information system and alerts [*Assignment: organization-defined personnel or roles*].	
PE 16 Protect Function: PR.DS 3*	Delivery and Removal	X	X	X	X	X	X	X	X	X	The organization authorizes, monitors, and controls ***all information system components*** **[DHS]** entering and exiting the facility and maintains records of those items.	
PE 17 Protect	Alternate Work Site	X	X		X	X		X	X		The organization: a. Employs ***management, operational and technical information system security controls*** **[DHS]** at alternate work sites;	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
Function: PR.IP 9*											b. Assesses as feasible, the effectiveness of security controls at alternate work sites; and c. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.	
PE-18	Location of Information System Components							X			The organization positions information system components within the facility to minimize potential damage from [*Assignment: organization-defined physical and environmental hazards*] and to minimize the opportunity for unauthorized access.	
PE 19 Protect Function: PR.IP 5*	Information Leakage	X	X	X	X	X	X	X	X	X	The organization protects the information system from information leakage due to electromagnetic signals emanations.	Informational leakage is the intentional or unintentional release of information to an untrusted environment from electromagnetic signals emanations. Security categories or classifications of information systems (with respect to confidentiality) and organizational security policies guide the selection of security controls employed to protect systems against information leakage due to electromagnetic signals emanations. Refer to *Cybersecurity Framework*, Version 1.1, April 16, 2018.
PE 20 Detect Function: DE.CM 2, DE.CM 7*	Asset Monitoring and Tracking	X	X	X	X	X	X	X	X	X	The organization: a. Employs [Assignment: organization defined asset location technologies] to track and monitor the location and movement of [Assignment: organization defined assets] within [Assignment: organization defined controlled areas]; and b. Ensures that asset location technologies are employed in accordance with applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance.	Asset location technologies can help organizations ensure that critical assets such as vehicles or essential information system components remain in authorized locations. Organizations consult with the OGC and the Senior Agency Official for Privacy (SAOP)/PRIV regarding the deployment and use of asset location technologies to address potential privacy concerns. Refer to *Cybersecurity Framework*, Version 1.1, April 16, 2018.

Planning (PL)

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
PL-1	Security Planning Policy and Procedures	X	X	X	X	X	X	X	X	X	The organization: a. Develops, documents, and disseminates to ***all personnel*** **[CNSS]**: 1. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security planning policy and associated security planning controls; and b. Reviews and updates the current: 1. Security planning policy ***at least annually if not otherwise defined in formal organizational policy*** **[CNSS]**; and 2. Security planning procedures ***at least annually if not otherwise defined in formal organizational policy*** **[CNSS]**.	The DHS NSS 4300B Policy, along with the proper application and documentation of all relevant (PL) baseline controls, CNSS and DHS defined values, supplemental guidance, and any inheritable network or enterprise controls provide the basis for satisfying PL-1. However, the ISO is ultimately responsible for addressing any and all (PL) policy and procedures within the SSP.
PL 2 Protect Function: PR.IP 7* Detect Function: DE.DP 5*	System Security Plan	X	X	X	X	X	X	X	X	X	The organization: a. Develops a security plan for the information system that: 1. Is consistent with the organization s enterprise architecture; 2. Explicitly defines the authorization boundary for the system; 3. Describes the operational context of the information system in terms of missions and business processes; 4. Provides the security categorization of the information system including supporting rationale; 5. Describes the operational environment for the information system and relationships with or connections to other information systems; 6. Provides an overview of the security requirements for the system; 7. Identifies any relevant overlays, if applicable; 8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and 9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;	SSPs including system related documentation shall be maintained in CIACS.

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
											b. Distributes copies of the security plan and communicates subsequent changes to the plan to ***all personnel with security responsibilities for the information system*** **[DHS]**; c. Reviews the security plan for the information system ***at least annually or when required due to system modifications*** **[CNSS]**; and d. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and e. Protects the security plan from unauthorized disclosure and modification.	
PL-2(3)	System Security Plan Plan / Coordinate With Other Organizational Entities	X	X		X	X		X	X		The organization plans and coordinates security-related activities affecting the information system with ***all personnel with security responsibilities for the information system*** **[DHS]** before conducting such activities in order to reduce the impact on other organizational entities.	
PL-4	Rules of Behavior	X	X	X	X	X	X	X	X	X	a. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage; b. Receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system; c. Reviews and updates the rules of behavior ***at least annually if not otherwise defined in formal organizational policy*** **[CNSS]**; and d. Requires individuals who have signed a previous version of the rules of behavior to read and re-sign when the rules of behavior are revised/updated.	
PL-4(1)	Rules of Behavior Social Media and Networking Restrictions	X	X								The organization includes in the rules of behavior, explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
PL 8 Identify Function: ID.AM 3* Protect Function: PR.IP 2, PR.PT 5*	Information Security Architecture	X	X	X	X	X	X	X	X	X	The organization: a. Develops an information security architecture for the 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. Reviews and updates the information security architecture ***at least annually or when changes to the information system or its environment warrant*** **[CNSS]** to reflect updates in the enterprise architecture; and c. Ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions.	
PL-8(1)	Information Security Architecture Defense-in-Depth	X	X	X	X	X	X	X	X	X	The organization designs its security architecture using a defense-in-depth approach that: a. Allocates ***procedural and technical safeguards*** **[DHS]** to ***physical and non-physical assets*** **[DHS]**; and b. Ensures that the allocated security safeguards operate in a coordinated and mutually reinforcing manner.	
PL-8(2)	Information Security Architecture Supplier Diversity	X	X	X	X	X	X	X	X	X	The organization requires that ***technical safeguards*** **[DHS]** allocated to ***non-physical layers of the information system*** **[DHS]** are obtained from different suppliers.	

Personnel Security (PS)

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
PS 1 Protect Function: PR.IP 11*	Personnel Security Policy and Procedures	X	X	X	X	X	X	X	X	X	The organization: a. Develops, documents, and disseminates to ***all personnel*** **[CNSS]**: 1. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls; and b. Reviews and updates the current: 1. Personnel security policy ***at least annually if not otherwise defined in organizational policy*** **[CNSS]**; and 2. Personnel security procedures ***at least annually if not otherwise defined in organizational policy*** **[CNSS]**.	The DHS NSS 4300B Policy, along with the proper application and documentation of all relevant (PS) baseline controls, CNSS and DHS defined values, supplemental guidance, and any inheritable network or enterprise controls provide the basis for satisfying PS 1. However, the ISO is ultimately responsible for addressing any and all (PS) policy and procedures within the SSP. References: DHS Instruction 121 01 011, *The Department of Homeland Security Administrative Security Program*
PS 2 Protect Function: PR.IP 11*	Position Risk Designation	X	X	X	X	X	X	X	X	X	The organization: a. Assigns a risk designation to all organizational positions; b. Establishes screening criteria for individuals filling those positions; and c. Reviews and updates position risk designations ***at least annually*** **[CNSS]**.	For DHS systems refer to DHS Instruction Handbook 121 01 007, *The Department of Homeland Security Personnel Suitability and Security Program*
PS 3 Protect Function: PR.AC 6, PR.DS 6, PR.IP 11*	Personnel Screening	X	X	X	X	X	X				The organization: a. Screens individuals prior to authorizing access to the information system; and b. Rescreens individuals according to ***DHS and/or Component personnel security guidelines*** **[DHS]**.	
PS 4 Protect Function: PR.IP 11*	Personnel Termination	X	X	X	X	X	X	X	X	X	The organization, upon termination of individual employment: a. Disables information system access within ***5 days if voluntary departure, if involuntarily terminated, access is disabled that same day*** **[CNSS]**; b. Terminates/revokes any authenticators/credentials associated with the individual;	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
											c. Conducts exit interviews that include a discussion of ***Non disclosure agreements and potential limitations on future employment*** **[DHS]**; d. Retrieves all security related organizational information system related property; e. Retains access to organizational information and information systems formerly controlled by terminated individual; and f. Notifies [*Assignment: organization defined personnel or roles*] within ***as soon as possible, not to exceed one (1) working day*** **[CNSS]**.	
PS-4(1)	Personnel Termination Post-employment Requirements	X	X	X							The organization: a. Notifies terminated individuals of applicable, legally binding post-employment requirements for the protection of organizational information; and b. Requires terminated individuals to sign an acknowledgment of post-employment requirements as part of the organizational termination process.	
PS-4(2)	Personnel Termination Automated Notification	X			X			X			The organization employs automated mechanisms to notify ***personnel who must be made aware of terminations*** **[DHS]** upon termination of an individual's employment.	
PS 5 Protect Function: PR.IP 11*	Personnel Transfer	X	X	X	X	X	X	X	X	X	The organization: a. Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization; b. ***Reassignment actions to ensure all system access no longer required (need to know) are removed or disabled*** **[CNSS]** within ***10 working days if not otherwise defined in formal organizational policy*** **[CNSS]**; c. Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and d. Notifies ***all personnel who must be made aware of transfers*** **[DHS]** within ***10 working days if not otherwise defined in formal organizational policy*** **[CNSS]**.	

					I						Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
PS 6 Protect Function: PR.DS 5, PR.IP 11*	Access Agreements	X	X	X	X	X	X				The organization: a. Develops and documents access agreements for organizational information systems; b. Reviews and updates the access ***agreements at least annually if not otherwise defined in formal organizational policy*** **[CNSS]**; and c. Ensures that individuals requiring access to organizational information and information systems: 1. Sign appropriate access agreements prior to being granted access; and 2. Re sign access agreements to maintain access to organizational information systems when access agreements have been updated or ***at least annually if not otherwise defined in formal organizational policy*** **[CNSS]**.	
PS-6(3)	Access Agreements Post-employment Requirements	X	X	X							The organization: a. Notifies individuals of applicable, legally binding post-employment requirements for protection of organizational information; and b. Requires individuals to sign an acknowledgment of these requirements, if applicable, as part of granting initial access to covered information.	
PS 7 Identify Function: ID.GV 2, ID.AM 6, ID.SC 4* Protect Function: PR.AT 3, PR.IP 11* Detect Function: DE.CM 6*	Third Party Personnel Security	X	X	X	X	X	X				The organization: a. Establishes personnel security requirements including security roles and responsibilities for third party providers; b. Requires third party providers to comply with personnel security policies and procedures established by the organization; c. Documents personnel security requirements; d. Requires third party providers to notify the ***Organizational Security Manager*** **[CNSS]** of any personnel transfers or terminations of third party personnel who possess organizational credentials and/or badges, or who have information system privileges within ***As soon as possible, not to exceed 1 working day*** **[CNSS]**; and e. Monitors provider compliance.	.

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
PS 8 Protect Function: PR.IP 11*	Personnel Sanctions	X	X	X	X	X	X	X	X	X	The organization: a. Employs a formal sanctions process for individuals failing to comply with established information security policies and procedures; and b. Notifies [*Assignment: organization defined personnel or roles*] within [*Assignment: organization defined time period*] when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.	

Risk Assessment (RA)

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
RA-1	Risk Assessment Policy and Procedures	X	X	X	X	X	X	X	X	X	The organization: a. ***Develops, documents, and disseminates to all personnel*** **[CNSS]**: 1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and b. Reviews and updates the current: 1. Risk assessment policy ***at least annually if not otherwise defined in formal organizational policy.*** **[CNSS]**; and 2. Risk assessment procedures ***at least annually if not otherwise defined in formal organizational policy*** **[CNSS]**.	The DHS NSS 4300B Policy, along with the proper application and documentation of all relevant (RA) baseline controls, CNSS and DHS defined values, supplemental guidance, and any inheritable network or enterprise controls provide the basis for satisfying RA-1. However, the ISO is ultimately responsible for addressing any and all (RA) policy and procedures within the SSP.
RA 2 Identify Function: ID.AM 5, ID.RA 4, ID.RA 5, ID.SC 2*	Security Categorization	X	X	X	X	X	X	X	X	X	The organization: a. Categorizes information and the information system in accordance with applicable federal laws, EOs, directives, policies, regulations, standards, and guidance; b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and c. Ensures that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.	
RA 3 Identify Function: ID.RA 1, ID.RA 3, ID.RA 4, ID.RA 5, ID.SC 2* Protect Function: PR.IP 12*	Risk Assessment	X	X	X	X	X	X	X	X	X	The organization: a. Conducts an assessment of risk, 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; b. Documents risk assessment results in ***a risk assessment report*** **[DHS]**; c. Reviews risk assessment results ***at least annually if not otherwise defined in formal organizational policy*** **[CNSS]**; d. Disseminates risk assessment results to [*Assignment: organization defined personnel or roles*]; and	SSPs including system related documentation shall be maintained in CIACS.

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
Detect Function: DE.AE 4* Respond Function: RS.MI 3*											e. Updates the risk assessment ***at least annually if not otherwise defined in formal organizational policy*** **[CNSS]** or whenever there are signification changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.	
RA 5 Identify Function: ID.RA 1* Protect Function: PR.IP 12* Detect Function: DE.CM 8, DE.DP 4, DE.DP 5* Respond Function: RS.CO 3, RS.MI 3*	Vulnerability Scanning	X	X	X	X	X	X	X	X	X	The organization: a. Scans for vulnerabilities in the information system and hosted applications ***at least monthly*** **[DHS]** and when new vulnerabilities potentially affecting the system/applications are identified and reported; b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: 1. Enumerating platforms, software flaws, and improper configurations; 2. Formatting checklists and test procedures; and 3. Measuring vulnerability impact; c. Analyzes vulnerability scan reports and results from security control assessments; d. Remediates legitimate vulnerabilities *[Assignment: organization defined response times]* in accordance with an organizational assessment of risk; and e. Shares information obtained from the vulnerability scanning process and security control assessments with [*Assignment: organization defined personnel or roles*] to help eliminate similar vulnerabilities in other information systems (e.g., systemic weaknesses or deficiencies).	
RA-5(1)	Vulnerability Scanning Update Tool Capability	X	X	X	X	X	X	X	X	X	The organization employs vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities to be scanned.	
RA-5(2)	Vulnerability Scanning Update by	X	X	X	X	X	X	X	X	X	The organization updates the information system vulnerabilities scanned ***within 24 hours prior to running scans*** **[CNSS]**.	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
	Frequency/Prior to New Scan/ When Identified											
RA-5(4)	Vulnerability Scanning Discoverable Information	X	X	X	X	X	X	X	X	X	The organization determines what information about the information system is discoverable by adversaries and subsequently takes [*Assignment: organization-defined corrective actions*].	
RA-5(5)	Vulnerability Scanning Privileged Access	X	X	X	X	X	X	X	X	X	The information system implements privileged access authorization to ***Authorized vulnerability scanning components*** **[CNSS]** for selected ***Authorization by the CISO/SISO or designate*** **[CNSS]**.	
RA-5(10)	Vulnerability Scanning Correlate Scanning Information	X			X			X			The organization correlates the output from vulnerability scanning tools to determine the presence of multi-vulnerability/multi-hop attack vectors.	

System and Services Acquisition (SA)

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
SA-1	System and Services Acquisition Policy and Procedures	X	X	X	X	X	X	X	X	X	The organization: a. Develops, documents, and disseminates to ***all personnel*** **[CNSS]**: 1. A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls; and b. Reviews and updates the current: 1. System and services acquisition policy ***at least annually if not otherwise defined in formal organizational policy*** **[CNSS]**; and 2. System and services acquisition procedures ***at least annually if not otherwise defined in formal organizational policy*** **[CNSS]**.	The DHS NSS 4300B Policy, along with the proper application and documentation of all relevant (SA) baseline controls, CNSS and DHS defined values, supplemental guidance, and any inheritable network or enterprise controls provide the basis for satisfying SA-1. However, the ISO is ultimately responsible for addressing any and all (SA) policy and procedures within the SSP. Acquisition of NSS and/or IT services shall be in accordance with DHS Instruction Manual 121-01-001, *Acquisition Management Instruction/Guidebook,* and the *Homeland Security Acquisition Regulation (HSAR)*.
SA 2 Identify Function: ID.GV 4*	Allocation of Resources	X	X	X	X	X	X	X	X	X	The organization: a. Determines information security requirements for the information system or information system service in mission/business process planning; b. Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process; and c. Establishes a discrete line item for information security in organizational programming and budgeting documentation.	ISOs or AOs shall ensure that information security requirements and POA&Ms are adequately funded, resourced and documented in accordance with current OMB budgetary guidance.
SA 3 Protect Function: PR.IP 2*	System Development Life Cycle	X	X	X	X	X	X	X	X	X	The organization: a. Manages the information system using [*Assignment: organization defined system development life cycle*] that incorporates information security considerations; b. Defines and documents information security roles and responsibilities throughout the system development life cycle; c. Identifies individuals having information security roles and responsibilities; and	DHS Systems Engineering Life Cycle (SELC)

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
											d. Integrates the organizational information security risk management process into system development life cycle activities.	
SA 4 Protect Function: PR.IP 2* Detect Function: DE.CM 6*	Acquisition Process	X	X	X	X	X	X	X	X	X	The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs: a. Security functional requirements; b. Security strength requirements; c. Security assurance requirements; d. Security related documentation requirements; e. Requirements for protecting security related documentation; f. Description of the information system development environment and environment in which the system is intended to operate; and g. Acceptance criteria.	ISOs shall ensure that information security requirements as described within this policy document are included in the acquisition of all DHS systems and services used to input, process, store, display, or transmit NSI.
SA-4(1)	Acquisition Process Functional Properties of Security Controls	X	X		X	X		X	X		The organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.	
SA-4(2)	Acquisition Process Design / Implementation Information for Security Controls	X	X		X	X		X	X		The organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes: [*Selection (one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; [Assignment: organization-defined design/implementation information*]] at [*Assignment: organization-defined level of detail*].	
SA-4(3)	Acquisition Process				X						The organization requires the developer of the information system, system component, or information system service to demonstrate the	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
	Development Methods / Techniques / Practices										use of a system development life cycle that includes [*Assignment: organization-defined state-of-the-practice system/security engineering methods, software development methods, testing/evaluation/validation techniques, and quality control processes*].	
SA-4(5)	Acquisition Process System / Component / Service Configurations				X						The organization requires the developer of the information system, system component, or information system service to: a. Deliver the system, component, or service with [*Assignment: organization-defined security configurations*] implemented; and b. Use the configurations as the default for any subsequent system, component, or service reinstallation or upgrade.	
SA-4(7)	Acquisition Process NIAP-Approved Protection Profiles				X	X	X				The organization: a. Limits the use of commercially provided information assurance and information assurance-enabled information technology products to those products that have been successfully evaluated against a NIAP-approved Protection Profile for a specific technology type, if such a profile exists; and b. Requires, if no NIAP-approved Protection Profile exists for a specific technology type but a commercially provided information technology product relies on cryptographic functionality to enforce its security policy, that the cryptographic module is FIPS-validated.	
SA-4(9)	Acquisition Process Functions / Ports / Protocols / Services in use	X	X	X	X	X	X	X	X	X	The organization requires 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.	
SA-4(10)	Acquisition Process Use of Approved PIV Products	X	X	X	X	X	X				The organization employs only information technology products on the FIPS 201-approved products list for PIV capability implemented within organizational information systems.	
SA 5 Identify	Information System Documentation	X	X	X	X	X	X	X	X	X	The organization: a. Obtains administrator documentation for the information system, system component, or information system service that describes:	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
Function: ID.RA 1*											1. Secure configuration, installation, and operation of the system, component, or service; 2. Effective use and maintenance of security functions/mechanisms; and 3. Known vulnerabilities regarding configuration and use of administrative (e.g., privileged) functions; b. Obtains user documentation for the information system, system component, or information system service that describes: 1. User accessible security functions/mechanisms and how to effectively use those security functions/mechanisms; 2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and 3. User responsibilities in maintaining the security of the system, component, or service; c. Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and takes [*Assignment: organization defined actions*] in response; d. Protects documentation as required, in accordance with the risk management strategy; and e. Distributes documentation to [*Assignment: organization defined personnel or roles*].	
SA 8 Protect Function: PR.IP 2*	Security Engineering Principles	X	X	X	X	X	X	X	X	X	The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.	
SA 9 Identify Function: ID.AM 4, ID.SC 1, ID.SC 3, ID.SC 4*	External Information System Services	X	X	X	X	X	X	X	X	X	The organization: a. Requires that providers of external information system services comply with organizational information security requirements and employ [*Assignment: organization defined security controls*] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
Protect Function: PR.AT 3* Detect Function: DE.CM 6*											b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and c. Employs [*Assignment: organization defined processes, methods, and techniques*] to monitor security control compliance by external service providers on an ongoing basis.	
SA-9(1)	External Information Systems Services Risk Assessments / Organizational Approvals				X	X	X				The organization: a. Conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services; and b. Ensures that the acquisition or outsourcing of dedicated information security services is approved by ***Chief Information Officer*** **[CNSS]**.	
SA-9(2)	External Information Systems Services Identification of Functions / Ports / Protocols / Services	X	X	X	X	X	X	X	X	X	The organization requires providers of ***all external information systems and services*** **[CNSS]** to identify the functions, ports, protocols, and other services required for the use of such services.	
SA 10 Protect Function: PR.DS 8, PR.IP 1, PR.IP 2, PR.IP 3*	Developer Configuration Management				X	X	X				The organization requires the developer of the information system, system component, or information system service to: a. Perform configuration management during system, component, or service [*Selection (one or more): design; development; implementation; operation*]; b. Document, manage, and control the integrity of changes to [*Assignment: organization defined configuration items under configuration management*]; c. Implement only organization approved changes to the system, component, or service; d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and e. Track security flaws and flaw resolution within the system, component, or service and report findings to ***at a minimum, the***	Refer to NIAP, mandated by CNSSP Number 11

					I						Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
											***Information System Owner, ISSM and ISSO* [DHS]**.	
SA-10(1)	Developer Configuration Management Software / Firmware Integrity Verification				X	X	X				The organization requires the developer of the information system, system component, or information system service to enable integrity verification of software and firmware components.	
SA 11 Identify Function: ID.RA 1, ID.SC 3* Protect Function: PR.IP 2*	Developer Security Testing and Evaluation	X	X		X	X		X	X		The organization requires the developer of the information system, system component, or information system service to: a. Create and implement a security assessment plan; b. Perform ***unit, integration, system, and/or regression* [DHS]** testing/evaluation on ***all applicable controls based on the categorization of the system* [DHS]**; c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation; d. Implement a verifiable flaw remediation process; and e. Correct flaws identified during security testing/evaluation.	
SA 12 Identify Function: ID.BE 1, ID.SC 1, ID.SC 2, ID.SC 3, ID.SC 4* Protect Function: PR.IP 2*	Supply Chain Protection	X	X	X	X	X	X	X	X	X	The organization protects against supply chain threats to the information system, system component, or information system service by employing: ***security safeguards in accordance with CNSSD Number 505, Supply Chain Risk Management (SCRM)* [CNSS]** as part of a comprehensive, defense in breadth information security strategy.	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
SA-12(1)	Supply Chain Protection Acquisition Strategies / Tools / Methods	X			X			X			The organization employs [*Assignment: organization-defined tailored acquisition strategies, contract tools, and procurement methods*] for the purchase of the information system, system component, or information system service from suppliers.	
SA-12(5)	Supply Chain Protection Limitation of Harm	X			X			X			The organization employs [*Assignment: organization-defined security safeguards*] to limit harm from potential adversaries identifying and targeting the organizational supply chain.	
SA-12(8)	Supply Chain Protection Use of All-Source intelligence	X			X			X			The organization uses all-source intelligence analysis of suppliers and potential suppliers of the information system, system component, or information system service.	
SA-12(9)	Supply Chain Protection Operations Security	X			X			X			The organization employs [*Assignment: organization-defined Operations Security (OPSEC) safeguards*] in accordance with classification guides to protect supply chain-related information for the information system, system component, or information system service.	
SA-12(11)	Supply Chain Protection Penetration Testing / Analysis of Elements, Processes, and Actors	X			X			X			The organization employs [*Selection (one or more): organizational analysis, independent third-party analysis, organizational penetration testing, independent third-party penetration testing*] of [*Assignment: organization-defined supply chain elements, processes, and actors*] associated with the *information system, system component, or information system service*.	
SA 13 Identify Function: ID.BE 5*	Trustworthiness	X	X	X	X	X	X	X	X	X	The organization: a. Describes the trustworthiness required in the [Assignment: organization defined information system, information system component, or information system service] supporting its critical missions/business functions; and b. Implements [Assignment: organization defined assurance overlay] to achieve such trustworthiness.	This control helps organizations to make explicit trustworthiness decisions when designing, developing, and implementing information systems that are needed to conduct critical organizational missions/business functions. Trustworthiness is a characteristic/property of an information system that expresses the degree to which the system can be expected to preserve the confidentiality, integrity, and availability of the information it processes, stores, or transmits. Trustworthy information systems are systems that are capable of being trusted to operate within defined levels of risk despite the environmental disruptions, human errors, and purposeful attacks that are expected to occur in the specified environments of operation. Trustworthy systems are important to

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
												mission/business success. Two factors affecting the trustworthiness of information systems include: (i) security functionality (e.g., the security features, functions, and/or mechanisms employed within the system and its environment of operation); and (ii) security assurance (e.g., the grounds for confidence that the security functionality is effective in its application). Developers, implementers, operators, and maintainers of organizational information systems can increase the level of assurance (and trustworthiness), for example, by employing well defined security policy models, structured and rigorous hardware, software, and firmware development techniques, sound system/security engineering principles, and secure configuration settings (defined by a set of assurance related security controls). Refer to *Cybersecurity Framework*, Version 1.1, April 16, 2018.
SA 14 Identify Function: ID.AM 5, ID.BE 3, ID.BE 4, ID.BE 5, ID.RA 4, ID.RM 3, ID.SC 2* Protect Function: PR.PT 5*	Criticality Analysis	X			X			X			The organization identifies critical information system components and functions by performing a criticality analysis for [*Assignment: organization defined information systems, information system components, or information system services*] at [*Assignment: organization defined decision points in the system development life cycle*].	
SA 15 Identify Function: ID.SC 2* Protect	Development Process, Standards, and Tools	X	X	X	X	X	X	X	X	X	The organization: a. Requires the developer of the information system, system component, or information system service to follow a documented development process that: 1. Explicitly addresses security requirements; 2. Identifies the standards and tools used in the development process;	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
Function: PR.IP 2*											3. Documents the specific tool options and tool configurations used in the development process; and 4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and b. Reviews the development process, standards, tools, and tool options/configurations [*Assignment: organization defined frequency*] to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy [*Assignment: organization defined security requirements*].	
SA-15(3)	Development Process, Standards, and Tools Criticality Analysis	X			X			X			The organization requires the developer of the information system, system component, or information system service to perform a criticality analysis at [*Assignment: organization-defined breadth/depth*] and at [*Assignment: organization-defined decision points in the system development life cycle*].	
SA-15(4)	Development Process, Standards, and Tools Threat Modeling / Vulnerability Analysis	X			X			X			The organization requires that developers perform threat modeling and a vulnerability analysis for the information system at [*Assignment: organization-defined breadth/depth*] that: a. Uses [*Assignment: organization-defined information concerning impact, environment of operations, known or assumed threats, and acceptable risk levels*]; b. Employs [*Assignment: organization-defined tools and methods*]; and c. Produces evidence that meets [*Assignment: organization-defined acceptance criteria*].	
SA-15(7)	Development Process, Standards, and Tools Automated Vulnerability Analysis				X						The organization requires the developer of the information system, system component, or information system service to: a. Perform an automated vulnerability analysis using [*Assignment: organization-defined tools*];	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
											b. Determine the exploitation potential for discovered vulnerabilities; c. Determine potential risk mitigations for delivered vulnerabilities; and d. Deliver the outputs of the tools and results of the analysis to [*Assignment: organization-defined personnel or roles*].	
SA-15(9)	Development Process, Standards, and Tools Use of Live Data	X	X	X							The organization approves, documents, and controls the use of live data in development and test environments for the information system, system component, or information system service.	
SA 16 Protect Function: PR.AT 3*	Developer Provided Training	X			X			X			The organization requires the developer of the information system, system component, or information system service to provide [*Assignment: organization defined training*] on the correct use and operation of the implemented security functions, controls, and/or mechanisms.	
SA 17 Protect Function: PR.IP 2*	Developer Security Architecture and Design	X			X			X			The organization requires the developer of the information system, system component, or information system service to produce a design specification 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. Accurately and completely 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.	
SA 18 Detect Function: DE.DP 2*	Tamper Resistance and Detection	X	X	X	X	X	X	X	X	X	The organization implements a tamper protection program for the information system, system component, or information system service.	Anti tamper technologies and techniques provide a level of protection for critical information systems, system components, and information technology products against a number of related threats including modification, reverse engineering, and substitution. Strong identification combined with tamper resistance and/or tamper detection is essential to protecting information systems, components, and products during distribution and when in use.

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
												Refer to *Cybersecurity Framework*, Version 1.1, April 16, 2018.
SA-19	Component Authenticity				X	X	X				The organization: a. Develops and implements anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the information system; and b. Reports counterfeit information system components to [*Selection (one or more): source of counterfeit component; [Assignment: organization-defined external reporting organizations]; [Assignment: organization-defined personnel or roles]*].	
SA 21 Protect Function: PR.IP 11*	Developer Screening	X	X	X	X	X	X	X	X	X	The organization requires that the developer of [Assignment: organization defined information system, system component, or information system service]: a. Have appropriate access authorizations as determined by assigned [Assignment: organization defined official government duties]; and b. Satisfy [Assignment: organization defined additional personnel screening criteria].	Because the information system, system component, or information system service may be employed in critical activities essential to the national and/or economic security interests of the United States, organizations have a strong interest in ensuring that the developer is trustworthy. The degree of trust required of the developer may need to be consistent with that of the individuals accessing the information system/component/service once deployed. Examples of authorization and personnel screening criteria include clearance, satisfactory background checks, citizenship, and nationality. Trustworthiness of developers may include a review and analysis of company ownership and any relationships the company has with entities potentially affecting the quality/reliability of the systems, components, or services being developed. Refer to *Cybersecurity Framework*, Version 1.1, April 16, 2018.
SA-22	Unsupported System Components	X			X			X			The organization: a. Replaces information system components when support for the components is no longer available from the developer, vendor, or manufacturer; and b. Provides justification and documents approval for the continued use of unsupported system components required to satisfy mission/business needs.	

System and Communications Protection (SC)

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
SC-1	System and Communications Protection Policy and Procedures	X	X	X	X	X	X	X	X	X	The organization: a. Develops, documents, and disseminates to ***all personnel*** **[CNSS]**: 1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and b. Reviews and updates the current: 1. System and communications protection policy ***at least annually if not otherwise defined in formal organizational policy*** **[CNSS]**; and 2. System and communications protection procedures ***at least annually if not otherwise defined in formal organizational policy*** **[CNSS]**.	The DHS NSS 4300B Policy, along with the proper application and documentation of all relevant (SC) baseline controls, CNSS and DHS defined values, supplemental guidance, and any inheritable network or enterprise controls provide the basis for satisfying SC-1. However, the ISO is ultimately responsible for addressing any and all (SC) policy and procedures within the SSP. References: Refer to DHS 4300B.200, *Communication Security (COMSEC)*
SC-2	Application Partitioning	X	X		X	X					The information system separates user functionality (including user interface services) from information system management functionality.	
SC-3	Security Function Isolation	X			X						The information system isolates security functions from non-security functions.	
SC-4	Information in Shared Resources	X	X								The information system prevents unauthorized and unintended information transfer via shared system resources.	
SC 5 Protect	Denial of Service Protection							X	X	X	The information system protects against or limits the effects of the following types of denial of service attacks: ***Consumption of scarce, limited, or non renewable resources;***	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
Function: PR.DS 4*											***destruction or alteration of configuration information; physical destruction or alteration of network components.*** **[CNSS]**.	
SC-5(1)	Denial of Service Protection Restrict Internal Users							X	X	X	The information system restricts the ability of users to launch denial of service attacks against other information systems or networks.	
SC-5(2)	Denial of Service Protection Excess Capacity / Bandwidth / Redundancy							X	X		The information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks.	
SC-5(3)	Denial of Service Protection Detection / Monitoring							X	X		The organization: a. Employs [*Assignment: organization-defined monitoring tools*] to detect indicators of denial of service attacks against the information system; and b. Monitors [*Assignment: organization-defined information system resources*] to determine if sufficient resources exist to prevent effective denial of service attacks.	
SC 6 Identify Function: ID.AM 5* Protect Function: PR.PT 5*	Resource Availability	X	X	X	X	X	X	X	X	X	The information system protects the availability of resources by allocating [Assignment: organization defined resources] by [Selection (one or more); priority; quota; [Assignment: organization defined security safeguards]].	Priority protection helps prevent lower priority processes from delaying or interfering with the information system servicing any higher priority processes. Quotas prevent users or processes from obtaining more than predetermined amounts of resources. This control does not apply to information system components for which they are only single users/roles. Refer to *Cybersecurity Framework*, Version 1.1, April 16, 2018.
SC 7 Protect Function: PR.AC 5, PR.DS 5, PR.PT 4* Detect	Boundary Protection	X	X	X	X	X	X				The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [*Selection: physically; logically*] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices	Systems approved for classified processing shall not share peripherals with unclassified processing equipment except through NSA approved switching devices. Approval for the use of switching devices shall be included in the accreditation documentation.

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
Function: DE.CM 1*											arranged in accordance with an organizational security architecture.	
SC-7(3)	Boundary Protection Access Points	X	X	X	X	X	X				The organization limits the number of external network connections to the information system.	
SC-7(4)	Boundary Protection External Telecommunications Services	X	X	X	X	X	X				The organization: a. Implements a managed interface for each external telecommunication service; b. Establishes a traffic flow policy for each managed interface; c. Protects the confidentiality and integrity of the information being transmitted across each interface; d. Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; e. Reviews exceptions to the traffic flow policy ***at least every 6 months*** **[CNSS]**; and f. Removes traffic flow policy exceptions that are no longer supported by an explicit mission/business need.	
SC-7(5)	Boundary Protection Deny By Default / Allow By Exception	X	X	X	X	X	X				The information system at managed interfaces, denies network traffic by default and allows network traffic by exception (e.g., deny all, permit by exception).	
SC-7(7)	Boundary Protection Prevent Split Tunneling For Remote Devices	X	X	X	X	X	X				The information system, in conjunction with a remote device, prevents the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks.	
SC-7(8)	Boundary Protection Route Traffic To Authenticated Proxy Servers	X	X	X	X	X	X				The information system routes ***all internal communications traffic except traffic specifically exempted by the AO or organizational policy*** **[CNSS]** to ***networks outside the control of the organization*** **[CNSS]** through authenticated proxy servers within the managed interfaces. The information system routes ***all internal communications traffic that may be proxied, except traffic specifically exempted by the AO***	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
											or organizational policy **[CNSS]** to ***all untrusted networks outside the control of the organization*** **[CNSS]**.	
SC-7(9)	Boundary Protection Restrict Threatening Outgoing Communications Traffic				X	X	X				The information system: a. Detects and denies outgoing communications traffic posing a threat to external information systems; and b. Audits the identity of internal users associated with denied communications.	
SC-7(10)	Boundary Protection Prevent Unauthorized Exfiltration	X	X	X							The organization prevents the unauthorized exfiltration of information across managed interfaces.	
SC-7(11)	Boundary Protection Restrict Incoming Communications Traffic				X	X	X				The information system only allows incoming communications from [*Assignment: organization-defined authorized sources*] to be routed to [*Assignment: organization-defined authorized destinations*].	
SC-7(12)	Boundary Protection Host-Based Protection	X	X	X	X	X	X	X	X	X	The information system implements host-based boundary protection mechanisms for servers, workstations, and mobile devices.	
SC-7(13)	Boundary Protection Mechanisms / Support Components	X	X	X	X	X	X				The organization isolates ***at a minimum, vulnerability scanning tools, audit log servers, patch servers, and Network Defense tools*** **[DHS]** from other internal information system components via physically separate subnets with managed interfaces to other portions of the system.	
SC-7(14)	Boundary Protection Protects Against Unauthorized Physical Connections	X	X	X	X	X	X				The organization protects against unauthorized physical connections across the boundary protections implemented at ***CDSs and controlled interfaces*** **[CNSS]**.	
SC-7(18)	Boundary Protection Boundary Protection Fail Secure	X			X			X			The information system fails securely in the event of an operational failure of a boundary protection device.	
SC-7(21)	Boundary Protection Isolation Of Information System Components	X			X						The organization employs boundary protection mechanisms to separate [*Assignment: organization-defined information system components*] supporting [*Assignment: organization-defined missions and/or business functions*].	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
SC 8 Protect Function: PR.DS 5, PR.DS 2*	Transmission Confidentiality and Integrity	X	X	X	X	X	X				The information system protects the integrity of transmitted information.	
SC-8(1)	Transmission Confidentiality and Integrity Cryptographic Or Alternate Physical Protection	X	X	X	X	X	X				The information system implements cryptographic mechanisms to [*Selection (one or more): prevent unauthorized disclosure of information; detect changes to information*] during transmission unless otherwise protected by [*Assignment: organization-defined alternative physical safeguards*].	
SC-8(2)	Transmission Confidentiality and Integrity Pre / Post Transmission Handling	X	X		X	X					The information system maintains the [*Selection (one or more): confidentiality; integrity*] of information during preparation for transmission and during reception.	
SC-10	Network Disconnect	X	X		X	X					The information system terminates the network connection associated with a communications session at the end of the session or after ***not more than 1 hour*** **[CNSS]** of inactivity.	
SC 11 Protect Function: PR.DS 2*	Trusted Path	X	X	X	X	X	X	X	X	X	The information system establishes a trusted communications path between the user and the following security functions of the system: [Assignment: organization defined security functions to include at a minimum, information system authentication and re authentication].	Trusted paths are mechanisms by which users (through input devices) can communicate directly with security functions of information systems with the requisite assurance to support information security policies. The mechanisms can be activated only by users or the security functions of organizational information systems. User responses via trusted paths are protected from modifications by or disclosure to untrusted applications. Organizations employ trusted paths for high assurance connections between security functions of information systems and users (e.g., during system logons). Enforcement of trusted communications paths is typically provided via an implementation that meets the reference monitor concept.

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
												Refer to *Cybersecurity Framework*, Version 1.1, April 16, 2018.
SC 12 Protect Function: PR.DS 1, PR.DS 2*	Cryptographic Key Establishment and Management	X	X	X	X	X	X				The organization establishes and manages cryptographic keys for required cryptography employed within the information system.	
SC-12(1)	Cryptographic Key Establishment and Management Availability							X			The organization maintains availability of information in the event of the loss of cryptographic keys by users.	
SC 13 Protect Function: PR.DS 5*	Cryptographic Protection	X	X	X	X	X	X				The information system implements [Assignment: organization defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.	NIST certified cryptography shall be used to encrypt stored classified non Sources and Methods Intelligence (SAMI) information if required by the information owner. If a classified enclave contains SAMI and is accessed by individuals lacking appropriate clearances, then NSA approved cryptography shall be used to encrypt all Sources and Materials Intelligence stored within the enclave. Refer to DHS 4300B.200, *Communication Security (COMSEC)*
SC 15 Protect Function: PR.AC 3*	Collaborative Computing Devices	X	X	X							The information system: a. Prohibits remote activation of collaborative computing devices with the following exceptions: ***Remote activation of centrally managed dedicated Video Teleconference (VTC) Suites located in approved VTC locations*** **[CNSS]**; and b. Provides an explicit indication of use to users physically present at the devices.	
SC-17	Public Key Infrastructure Certificates	X	X	X	X	X	X				The organization issues public key certificates under a ***CNSS certificate policy number, as appropriate*** **[DHS]** or obtains public key certificates under an appropriate certificate policy from an approved service provider.	
SC 18 Detect Function: DE.CM 5*	Mobile Code				X	X	X				The organization: a. Defines acceptable and unacceptable mobile code and mobile code technologies; b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
											c. Authorizes, monitors, and controls the use of mobile code within the information system.	
SC-18(1)	Identify Unacceptable Code / Take Corrective Actions				X	X	X				The information system identifies [*Assignment: organization-defined unacceptable mobile code*] and takes [*Assignment: organization-defined corrective actions*].	
SC-18(2)	Mobile Code Acquisition / Development / Use				X	X	X				The organization ensures the acquisition, development, and/or use of mobile code to be deployed in information systems meets: a. Emerging ***mobile code technologies that have not undergone a risk assessment and been assigned to a Risk Category by the AO are not used.*** b. ***Category 1 mobile code is signed with a code signing certificate; use of unsigned Category 1 mobile code is prohibited; use of Category 1 mobile code technologies that cannot block or disable unsigned mobile code (e.g., Windows Scripting Host) is prohibited.*** c. ***Category 2 mobile code which executes in a constrained environment without access to system resources (e.g., Windows registry, file system, system parameters, and network connections to other than the originating host) may be used.*** d. ***Category 2 mobile code that does not execute in a constrained environment may be used when obtained from a trusted source over an assured channel (e.g., SIPRNet, SSL connection, S/MIME, code is signed with an approved code signing certificate).*** e. ***Category 3 (mobile code having limited functionality, with no capability for unmediated access to the services and resources of a computing platform) mobile code may be used.*** **[CNSS]**.	
SC-18(3)	Mobile Code Prevent Downloading / Execution				X	X	X				The information system prevents the download and execution of prohibited mobile code.	
SC-18(4)	Mobile Code Prevent Automatic Execution				X	X	X				The information system prevents the automatic execution of mobile code in ***e-mail*** **[CNSS]** and	

											requires ***prompting the user*** **[CNSS]** prior to executing the code.	
SC 19 Protect Function: PR.PT 4*	Voice Over Internet Protocol	X	X	X	X	X	X	X	X	X	The organization: a. Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and b. Authorizes, monitors, and controls the use of VoIP within the information system.	
SC 20 Protect Function: PR.PT 4*	Secure Name/Address Resolution Service (Authoritative Source)				X	X	X				The information system: a. Provides additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and b. Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.	
SC 21 Protect Function: PR.PT 4*	Secure Name/Address Resolution Service (Recursive Or Caching Resolver)				X	X	X				The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.	
SC 22 Protect Function: PR.PT 4*	Architecture And Provisioning For Name/Address Resolution Service	X	X	X	X	X	X	X	X	X	The information systems that collectively provide name/address resolution service for an organization are fault tolerant and implement internal/external role separation.	
SC 23 Protect Function: PR.PT 4*	Session Authenticity				X	X	X				The information system protects the authenticity of communications sessions.	
SC-23(1)	Session Authenticity Invalidate Session Identifiers At Logout				X	X	X				The information system invalidates session identifiers upon user logout or other session termination.	
SC-23(3)	Session Authenticity Unique Session Identifiers With Randomization				X	X	X				The information system generates a unique session identifier for each session and recognizes only session identifiers that are system-generated.	
SC-23(5)	Session Authenticity Allowed Certificate Authorities				X	X	X				The information system only allows the use of [*Assignment: organization-defined certificate*	

											authorities] for verification of the establishment of protected sessions.	
SC 24 Protect Function: PR.PT 4*	Fail in Known State	X			X						The information system fails to a ***known secure state*** **[CNSS]** for ***all types of failures*** **[CNSS]** preserving ***information necessary to return to determine cause of failure and to return to operations with least disruption to mission/business processes*** **[CNSS]** in failure.	
SC 25 Protect Function: PR.PT 4*	Thin Nodes	X	X	X	X	X	X	X	X	X	The organization employs [Assignment: organization defined information system components] with minimal functionality and information storage.	The deployment of information system components with a reduced/minimal functionality (e.g., diskless nodes and thin client technologies) reduces the need to secure every user endpoint, and may reduce the exposure of information, information systems, and services to cyber attacks. Refer to *Cybersecurity Framework*, Version 1.1, April 16, 2018.
SC 28 Protect Function: PR.DS 1*	Protection of Information at Rest	X	X	X	X	X	X				The information system protects the confidentiality and integrity of information at rest.	
SC-28(1)	Protection of Information at Rest Cryptographic Protection	X	X	X	X	X	X				The organization employs cryptographic mechanisms to prevent unauthorized disclosure and modification of information at rest unless otherwise protected by alternative physical measures.	
SC 29 Protect Function: PR.PT 4*	Heterogeneity	X	X	X	X	X	X	X	X	X	The organization employs a diverse set of information technologies for [Assignment: organization defined information system components] in the implementation of the information system.	Increasing the diversity of information technologies within organizational information systems reduces the impact of potential exploitations of specific technologies and also defends against common mode failures, including those failures induced by supply chain attacks. Diversity in information technologies also reduces the likelihood that the means adversaries use to compromise one information system component will be equally effective against other system components, thus further increasing the adversary work factor to successfully complete planned cyber attacks. An increase in diversity may add complexity and management overhead which could ultimately lead to mistakes and unauthorized configurations. Refer to *Cybersecurity Framework*, Version 1.1, April 16, 2018.
SC 31 Protect Function: PR.DS 5*	Covert Channel Analysis	X	X	X	X	X	X	X	X	X	The organization: a. Performs a covert channel analysis to identify those aspects of communications within the information system that are potential avenues for covert [Selection (one or more): storage; timing] channels; and b. Estimates the maximum bandwidth of those channels.	Developers are in the best position to identify potential areas within systems that might lead to covert channels. Covert channel analysis is a meaningful activity when there is the potential for unauthorized information flows across security domains, for example, in the case of information systems containing export controlled information and having connections to external networks (e.g., networks not controlled by organizations). Covert channel analysis is also

												meaningful for multilevel secure (MLS) information systems, multiple security level (MSL) systems, and cross domain systems. Refer to *Cybersecurity Framework*, Version 1.1, April 16, 2018.
SC 32 Protect Function: PR.PT 4*	Information System Partitioning	X	X	X	X	X	X	X	X	X	The organization partitions the information system into [Assignment: organization defined information system components] residing in separate physical domains or environments based on [Assignment: organization defined circumstances for physical separation of components].	Information system partitioning is a part of a defense in depth protection strategy. Organizations determine the degree of physical separation of system components from physically distinct components in separate racks in the same room, to components in separate rooms for the more critical components, to more significant geographical separation of the most critical components. Security categorization can guide the selection of appropriate candidates for domain partitioning. Managed interfaces restrict or prohibit network access and information flow among partitioned information system components. Refer to *Cybersecurity Framework*, Version 1.1, April 16, 2018.
SC 36 Protect Function: PR.PT 4*	Distributed Processing and Storage	X	X	X	X	X	X	X	X	X	The organization distributes [Assignment: organization defined processing and storage] across multiple physical locations.	Distributing processing and storage across multiple physical locations provides some degree of redundancy or overlap for organizations, and therefore increases the work factor of adversaries to adversely impact organizational operations, assets, and individuals. This control does not assume a single primary processing or storage location, and thus allows for parallel processing and storage. Refer to *Cybersecurity Framework*, Version 1.1, April 16, 2018.
SC 37 Protect Function: PR.PT 4*	Out of Band Channels	X	X	X	X	X	X	X	X	X	The organization employs [Assignment: organization defined out of band channels] for the physical delivery or electronic transmission of [Assignment: organization defined information, information system components, or devices] to [Assignment: organization defined individuals or information systems].	Refer to *Cybersecurity Framework*, Version 1.1, April 16, 2018.
SC 38 Protect Function: PR.PT 4*	Operations Security	X	X	X	X	X	X	X	X	X	The organization employs [*Assignment: organization defined operations security safeguards*] to protect key organizational information throughout the system development life cycle.	
SC 39 Protect Function: PR.PT 4*	Process Isolation	X	X	X	X	X	X				The information system maintains a separate execution domain for each executing process.	
SC 40	Wireless Link Protection	X	X	X	X	X	X	X	X	X	The information system protects external and internal [Assignment: organization defined	This control applies to internal and external wireless communication links that may be visible to individuals who

Protect Function: PR.PT 4*											wireless links] from [Assignment: organization defined types of signal parameter attacks or references to sources for such attacks].	are not authorized information system users. Adversaries can exploit the signal parameters of wireless links if such links are not adequately protected. There are many ways to exploit the signal parameters of wireless links to gain intelligence, deny service, or to spoof users of organizational information systems. This control reduces the impact of attacks that are unique to wireless systems. Refer to *Cybersecurity Framework*, Version 1.1, April 16, 2018.
SC 41 Protect Function: PR.PT 4*	Port and I/O Device Access	X	X	X	X	X	X	X	X	X	The organization physically disables or removes [Assignment: organization defined connection ports or input/output devices] on [Assignment: organization defined information systems or information system components].	Connection ports include, for example, Universal Serial Bus (USB). Input/output (I/O) devices include, for example, Compact Disk (CD) and Digital Video Disk (DVID) drives. Physically disabling or removing such connection ports and I/O devices helps prevent exfiltration of information from ISs and the introduction of malicious code into systems from these ports/devices. Refer to *Cybersecurity Framework*, Version 1.1, April 16, 2018.
SC 43 Protect Function: PR.PT 4*	Usage Restrictions	X	X	X	X	X	X	X	X	X	The organization: a. Establishes usage restrictions and implementation guidance for [Assignment: organization defined information system components] based on the potential to cause damage to the IS if used maliciously; and b. Authorizes, monitors, and controls the use of such components within the IS.	Information system components include hardware, software, or firmware components (e.g., VoIP, mobile code, digital copiers, printers, scanners, optical devices, wireless technologies, and mobile devices). Refer to *Cybersecurity Framework*, Version 1.1, April 16, 2018.
SC 44 Detect Function: DE.CM 5*	Detonation Chambers	X	X	X	X	X	X	X	X	X	The organization employs a detonation chamber capability within [Assignment: organization defined information system, system component, or location].	Detonation chambers, also known as dynamic execution environments, allow organizations to open email attachments, execute untrusted or suspicious applications, and execute Universal Resource Locator (URL) requests in the safety of an isolated environment or virtualized sandbox. These protected and isolated execution environments provide a means of determining whether the associated attachments/applications contain malicious code. While related to the concept of deception nets, the control is not intended to maintain a long term environment in which adversaries can operate and their actions can be observed. Rather, it is intended to quickly identify malicious code and reduce the likelihood that the code is propagated to user environments of operation (or prevent such propagation completely). Refer to *Cybersecurity Framework*, Version 1.1, April 16, 2018.

System and Information Integrity (SI)

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
SI-1	System And Information Integrity Policy and Procedures	X	X	X	X	X	X	X	X	X	The organization: a. Develops, documents, and disseminates ***to all personnel*** **[CNSS]**: 1. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and b. Reviews and updates the current: 1. System and information integrity policy ***At least annually if not otherwise defined in formal organizational policy*** **[CNSS]**; and 2. System and information integrity ***procedures At least annually if not otherwise defined in formal organizational policy*** **[CNSS]**.	The DHS NSS 4300B Policy, along with the proper application and documentation of all relevant (SI) baseline controls, CNSS and DHS defined values, supplemental guidance, and any inheritable network or enterprise controls provide the basis for satisfying SI-1. However, the ISO is ultimately responsible for addressing any and all (SI) policy and procedures within the SSP.
SI 2 Identify Function: ID.RA 1* Protect Function: PR.IP 12*	Flaw Remediation				X	X	X				The organization: a. Identifies, reports, and corrects information system flaws; b. Tests software updates related to flaw remediation for effectiveness and potential side effects on organizational information systems be; c. Installs security relevant software and firmware updates within [*Assignment: organization defined time period*] of the release of the updates; and d. Incorporates flaw remediation into the organizational configuration management	Refer to NIAP, mandated by CNSSP Number 11

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
											process ***30 days if not otherwise defined in formal organizational policy*** **[CNSS]**.	
SI-2(1)	Flaw Remediation Central Management				X	X	X				The organization centrally manages the flaw remediation process.	
SI-2(2)	Flaw Remediation Automated Flaw Remediation Status				X	X	X				The organization employs automated mechanisms ***at least every thirty (30) days*** **[DHS]** to determine the state of information system components with regard to flaw remediation.	
SI-2(3)	Flaw Remediation Benchmarks for Corrective Actions				X	X	X				The organization: a. Measures the time between flaw identification and flaw remediation; and b. Establishes ***benchmarks*** **[DHS]** for taking corrective actions.	
SI-2(6)	Flaw Remediation Removal of Previous Versions of Software/Firmware				X	X	X				The organization removes ***all upgraded/replaced software and firmware components that are no longer required for operation when possible*** **[CNSS]** after updated versions have been installed.	
SI 3 Detect Function: DE.CM 4, DE.DP 3*	Malicious Code Protection				X	X	X				The organization: a. Employs malicious code protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code: b. Updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures; c. Configures malicious code protection mechanisms to: 1. Perform periodic scans of the information system ***at least weekly*** **[CNSS]** and real time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy; and	All media from non DHS sources shall only be introduced for use on DHS NSS after only all approvals have been obtained by designated authorities and properly documented. All media shall be scanned for virus, preferably on a standalone machine approved for the level of classified information contained on the media. The media will not be returned to the provider if the media is introduced to a system that already contains classified information. Refer to NIAP, mandated by CNSSP Number 11

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
											2. ***Block and quarantine malicious code and send an alert to the system administrator*** **[CNSS]** in response to malicious code detection; and d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the	
SI-3(1)	Malicious Code Protection Central Management				X	X	X				The organization centrally manages malicious code protection mechanisms.	
SI-3(2)	Malicious Code Protection Automatic Updates				X	X	X				The information system automatically updates malicious code protection mechanisms (including signature definitions).	
SI-3(10)	Malicious Code Protection Malicious Code Analysis				X	X	X				The organization: a. Employs [*Assignment: organization-defined tools and techniques*] to analyze the characteristics and behavior of malicious code; and b. Incorporates the results from malicious code analysis into organizational incident response and flaw remediation processes.	
SI 4 Identify Function: ID.RA 1* Protect Function: PR.DS 5, PR.IP 8* Detect Function: DE.AE 1, DE.AE 2, DE.AE 3, DE.AE 4,	Information System Monitoring	X	X	X	X	X	X	X	X	X	The organization: a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with ***DHS Continuous Monitoring Standard Operating Procedures, and with DHS Audit Management Standard Operating Procedures*** **[DHS]**; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [*Assignment: organization defined techniques and methods*]; c. Deploys monitoring devices: 1. Strategically within the information system to collect organization determined essential information; and 2. At ad hoc locations within the system to track specific types of transactions of interest to the organization;	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
DE.CM 1, DE.CM 5, DE.CM 6, DE.CM 7, DE.DP 2, DE.DP 3, DE.DP 4, DE.DP 5* Respond Function: RS.CO 3, RS.AN 1*											d. Protects information obtained from intrusion monitoring tools from unauthorized access, modification, and deletion; e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; f. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and g. Provides ***information security continuous monitoring specific to asset(s) in question*** **[DHS]** to ***DHS CISO and/or DHS NSS designee as required on a monthly basis*** **[DHS]**.	
SI-4(1)	Information System Monitoring System-Wide Intrusion Detection System	X	X	X	X	X	X	X	X	X	The organization connects and configures individual intrusion detection tools into an information system-wide intrusion detection system.	
SI-4(2)	Information System Monitoring Automated Tools For Real-Time Analysis	X	X		X	X		X	X		The organization employs automated tools to support near real-time analysis of events.	
SI-4(4)	Information System Monitoring Inbound and Outbound Communications Traffic	X	X	X	X	X	X	X	X	X	The information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions.	
SI-4(5)	Information System Monitoring System-Generated Alerts	X	X	X	X	X	X	X	X	X	The information system alerts [*Assignment: organization-defined personnel or roles*] when the following indications of compromise or potential compromise occur: [*Assignment: organization-defined compromise indicators*].	
SI-4(10)	Information System Monitoring	X	X		X	X		X	X		The organization makes provisions so that [*Assignment: organization-defined encrypted communications traffic*] is visible to	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
	Visibility of Encrypted Communications										[*Assignment: organization-defined information system monitoring tools*].	
SI-4(11)	Information System Monitoring Analyze Communications Traffic Anomalies	X	X	X	X	X	X	X	X	X	The organization analyzes outbound communications traffic at the external boundary of the information system and selected [*Assignment: organization-defined interior points within the system (e.g., subnetworks, subsystems)*] to discover anomalies.	
SI-4(12)	Information System Monitoring Automated Alerts	X	X	X	X	X	X	X	X	X	The organization employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications: ***Active or prospective violation of operational security policy and standards. Execution of malicious code/programs, behavior-based anomalous or suspicious activity using IT assets, active periodic, sustained or incidental attacks against DHS IT infrastructure*** **[DHS]**.	
SI-4(14)	Information System Monitoring Analyze Traffic / Event Patterns	X	X	X	X	X	X	X	X	X	The organization employs a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system.	
SI-4(15)	Information System Monitoring Wireless to Wireline Communications	X	X	X	X	X	X	X	X	X	The organization employs an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wireline networks.	
SI-4(16)	Information System Monitoring Correlate Monitoring Information	X	X	X	X	X	X	X	X	X	The organization correlates information from monitoring tools employed throughout the information system.	
SI-4(19)	Information System Monitoring Individuals Posing Greater Risk	X	X	X	X	X	X	X	X	X	The organization implements [*Assignment: organization-defined additional monitoring*] of individuals who have been identified by [*Assignment: organization-defined sources*] as posing an increased level of risk.	
SI-4(20)	Information System Monitoring Privileged User	X	X	X	X	X	X	X	X	X	The organization implements [*Assignment: organization-defined additional monitoring*] of privileged users.	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
SI-4(22)	Information System Monitoring Unauthorized Network Services	X	X	X	X	X	X	X	X	X	The information system detects network services that have not been authorized or approved by [*Assignment: organization-defined authorization or approval processes*] and [*Selection (one or more): audits; alerts* [*Assignment: organization-defined personnel or roles*]].	
SI-4(23)	Information System Monitoring Host-Based Devices	X	X	X	X	X	X	X	X	X	The organization implements [*Assignment: organization-defined host-based monitoring mechanisms*] at [*Assignment: organization-defined information system components*].	
SI 5 Identify Function: ID.RA 1, ID.RA 2, ID.RA 3* Respond Function: RS.CO 5, RS.AN 5*	Security Alerts, Advisories, And Directives				X	X	X				The organization: a. Receives information system security alerts, advisories, and directives from designated external organizations on an ongoing basis; b. Generates internal security alerts, advisories, and directives as deemed necessary; c. Disseminates security alerts, advisories, and directives to ***ISSM, CISO, ISSOs, and System Administrators*** **[DHS]**; and d. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.	ISOs shall report the security alert and advisory status of the information system to the AO, Component CISO, and DHS CISO upon request and on a periodic basis.
SI-5(1)	Security Alerts, Advisories, and Directives Automated Alerts and Advisories				X						The organization employs automated mechanisms to make security alert and advisory information available throughout the organization.	
SI-6	Security Functionality Verification				X						The information system: a. Verifies the correct operation of ***security assessments, including testing of security hardening/configuration, security control management and risk mitigation of the standard functional state of the system*** **[DHS]**; b. Performs this verification [*Selection (one or more): [Assignment: organization-defined system transitional states]; upon command by user with*	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
											appropriate privilege; [Assignment: organization-defined frequency]]; c. ***Minimally, notifies system/security administrator*** **[CNSS]** of failed security verification tests; and d. ***Notifies system/ security administrator*** **[DHS]** when anomalies are discovered.	
SI-6(3)	Security Functionality Verification Report Verification Results				X						The organization reports the results of security function verification to ***responsible security personnel (e.g., AO, SISO, ISSO, ISSM, etc.)*** **[CNSS]**.	
SI 7 Protect Function: PR.DS 6, PR.DS 8*	Software, Firmware, And Information Integrity				X	X					The organization employs integrity verification tools to detect unauthorized changes to [*Assignment: organization defined software, firmware, and information*].	
SI-7(1)	Software, Firmware, And Information Integrity Integrity Checks				X	X					The information system performs an integrity check of [*Assignment: organization-defined software, firmware, and information*] [*Selection (one or more): at startup; at [Assignment: organization-defined transitional states or security-relevant events]; [Assignment: organization-defined frequency]*].	
SI-7(2)	Software And Information Integrity Automated Notifications of Integrity Violations				X						The organization employs automated tools that provide notification to [*Assignment: organization-defined personnel or roles*] upon discovering discrepancies during integrity verification.	
SI-7(5)	Software And Information Integrity Automated Response to Integrity Violations				X						The information system automatically [*Selection (one or more): shuts the information system down; restarts the information system; implements [Assignment: organization-defined security safeguards]*] when integrity violations are discovered.	
SI-7(7)	Software And Information Integrity Integration of Detection and Response				X	X					The organization incorporates the detection of unauthorized [*Assignment: organization-defined security-relevant changes to the information system*] into the organizational incident response capability.	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
SI-7(8)	Software And Information Integrity Auditing Capability For Significant Events				X	X					The information system, upon detection of a potential integrity violation, provides the capability to audit the event and initiates the following actions: [*Selection (one or more): generates an audit record; alerts current user; alerts [Assignment: organization-defined personnel or roles]; [Assignment: organization-defined other actions]*].	
SI-7(14)	Software And Information Integrity Binary or Machine Executable Code				X	X	X				The organization: a. Prohibits the use of binary or machine-executable code from sources with limited or no warranty and without the provision of source code; and b. Provides exceptions to the source code requirement only for compelling mission/operational requirements and with the approval of the authorizing official.	
SI 8 Detect Function: DE.CM 4*	Spam Protection				X	X		X	X		The organization: a. Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and b. Updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.	Refer to NIAP, mandated by CNSSP Number 11
SI-8(1)	Spam Protection Central Management of Protection Mechanisms				X	X		X	X		The organization centrally manages spam protection mechanisms.	
SI-8(2)	Spam Protection Automatic Updates				X	X		X	X		The information system automatically updates spam protection mechanisms (including signature definitions).	
SI-10	Information Input Validation				X	X	X				The information system checks the validity of all inputs to web/application servers, database servers, and any system or application input that might receive a crafted exploit toward executing some code or buffer overflow.	
SI-10(3)	Information Input Validation Predictable Behavior				X	X					The information system behaves in a predictable and documented manner that reflects organizational and system objectives when invalid inputs are received.	
SI-11	Error Handling				X	X	X				The information system:	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
											a. Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and b. Reveals error messages only to [*Assignment: organization-defined personnel or roles*].	
SI 12 Protect Function: PR.IP 2*	Information Output Handling And Retention	X	X	X	X	X	X				The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, EOs, directives, policies, regulations, standards, and operational requirements.	
SI 13 Protect Function: PR.IP 2*	Predictable Failure Prevention	X	X	X	X	X	X	X	X	X	The organization: a. Determines mean time to failure (MTTF) for [Assignment: organization defined information system components] in specific environments of operation; and b. Provides substitute information system components and a means to exchange active and standby components at [Assignment: organization defined MTTF substitution criteria].	While MTTF is primarily a reliability issue, this control addresses potential failures of specific information system components that provide security capability. Failure rates reflect installation specific consideration, not industry average. Organizations defined criteria for substitution of information system components based on MTTF value with consideration for resulting potential harm from component failures. Transfer of responsibilities between active and standby components does not compromise safety, operational readiness or security capability (e.g., preservation of state variables). Standby components remain available at all times except for maintenance issues or recovery failures in progress. Refer to *Cybersecurity Framework*, Version 1.1, April 16, 2018.
SI 14 Protect Function: PR.IP 2*	Non Persistence	X	X	X	X	X	X	X	X	X	The organization implements non persistent [Assignment; organization defined information system components and services] that are initiated in a known state and terminated [Selection (one or more): upon end of session of use; periodically at [Assignment: organization defined frequency]].	This control mitigates risk from advanced persistent threats (APTs) by significantly reducing the targeting capability of adversaries (e.g., window of opportunity and available attack surface) to initiate and complete cyber attacks. By implementing the concept of non persistence for selected IS components, organizations can provide a known state computing resource for a specific period of time that does not give adversaries sufficient time on target to exploit vulnerabilities in organizational ISs and the environments in which those systems operate. Since the APT is a high end threat with regard to capability, intent, and targeting, organizations assume that over an extended period of time, a percentage of cyber attacks will be successful. Non persistent IS components and services are activated as required using protected information and terminated periodically or upon the end of sessions. Non

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
												persistence increases the work factor of adversaries in attempting to compromise or breach organizational ISs. Refer to *Cybersecurity Framework*, Version 1.1, April 16, 2018.
SI 16 Protect Function: PR.IP 2*	Memory Protection				X	X					The information system implements [*Assignment: organization defined security safeguards*] to protect its memory from unauthorized code execution.	
SI 17 Protect Function: PR.IP 2*	Fail Safe Procedures	X	X	X	X	X	X	X	X	X	The information system implements [Assignment: organization defined fail safe procedures] when [Assignment: organization defined failure conditions occur].	Failure conditions include, for example, loss of communications among critical system components or between system components and operational facilities. Fail safe procedures include, for example, altering operator personnel and providing specific instructions on subsequent steps to take (e.g., do nothing, reestablish system settings, shut down processes, or restart the system, or contact designated organizational personnel). Refer to *Cybersecurity Framework*, Version 1.1, April 16, 2018.

Program Management (PM)

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
PM 1 Identify Function: ID.GV 2*	Information Security Program Plan	X	X	X	X	X	X	X	X	X	The organization: a. Develops and disseminates an organization wide information security program plan that: 1. Provides 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 for meeting those requirements; 2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 3. Reflects coordination among organizational entities responsible for the different aspects of information security (e.g., technical, physical, personnel, cyber physical); and 4. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; b. Reviews the organization wide information security program plan ***at least annually if not otherwise defined informal organizational policy*** **[CNSS]**; c. Updates the plan to address organizational changes and problems identified during plan implementation or security control assessments; and d. Protects the information security program plan from unauthorized disclosure and modification.	The DHS NSS 4300B Policy, along with the proper application and documentation of all relevant (PM) baseline controls, CNSS and DHS defined values, supplemental guidance, and any inheritable network or enterprise controls provide the basis for satisfying PM 1. However, the ISO is ultimately responsible for addressing any and all (PM) policy and procedures within the SSP.
PM 2 Identify Function: ID.GV 2*	Senior Information Security Officer	X	X	X	X	X	X	X	X	X	The organization appoints a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization wide information security program.	
PM 3 Identify	Information Security Resources	X	X	X	X	X	X	X	X	X	The organization: a. Ensures that all capital planning and investment requests include the resources needed to implement the information security	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
Function: ID.GV 4*											program and documents all exceptions to this requirement; b. Employs a business case/Exhibit 300/Exhibit 53 to record the resources required; and c. Ensures that information security resources are available for expenditure as planned.	
PM 4 Identify Function: ID.RA 6*	Plan of Action and Milestones Process	X	X	X	X	X	X	X	X	X	The organization: a. Implements a process for ensuring that plans of action and milestones for the security program and associated organizational information systems: Are developed and maintained; Document the remedial information security actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and are reported in accordance with OMB FISMA reporting requirements. b. Reviews plans of action and milestones for consistency with the organizational risk management strategy and organization wide priorities for risk response actions.	Components shall comply with DHS Guidance on the development and maintenance of Plan of Actions and Milestones as established by DHS FISMA guidance.
PM 5 Identify Function: ID.AM 1, ID.AM 2*	Information System Inventory	X	X	X	X	X	X	X	X	X	The organization develops and maintains an inventory of its information systems.	
PM 6 Protect Function: PR.IP 7*	Information Security Measures of Performance	X	X	X	X	X	X	X	X	X	The organization develops, monitors, and reports on the results of information security measures of performance.	
PM 7 Identify Function: ID.GV 4*	Enterprise Architecture	X	X	X	X	X	X	X	X	X	The organization develops enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
PM 8 Identify Function: ID.BE 2, ID.BE 4, ID.RM 3*	Critical Infrastructure Plan	X	X	X	X	X	X	X	X	X	The organization addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.	
PM 9 Identify Function: ID.GV 4, ID.RA 4, ID.RA 6, ID.RM 1, ID.RM 2, ID.RM 3, ID.SC 1, ID.SC 2, ID.SC 3*	Risk Management Strategy	X	X	X	X	X	X	X	X	X	The organization: a. Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems; and b. Implements the risk management strategy consistently across the organization; and c. Reviews and updates the risk management strategy ***at least annually if not otherwise defined informal organizational policy*** **[CNSS]**.	
PM 10 Identify Function: ID.GV 4*	Security Authorization Process	X	X	X	X	X	X	X	X	X	The organization: a. Manages (e.g., documents, tracks, and reports) the security state of organizational information systems and the environments in which those systems operate through security authorization processes; b. Designates individuals to fulfill specific roles and responsibilities within the organizational risk management process; and c. Fully integrates the security authorization processes into an organization wide risk management program.	
PM 11 Identify Function: ID.GV 4, ID.RA 4,	Mission/Business Process Definition	X	X	X	X	X	X	X	X	X	The organization: a. Defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and	ISOs shall include information security requirements in their Capital Planning and Investment Control (CPIC) business cases for the current budget year and for the Future Years Homeland Security Program (FYHSP) for each DHS system.

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
ID.RM 3, ID.AM 6, ID.BE 3*											b. Determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	
PM 12 Identify Function: ID.RA 3*	Insider Threat Program	X	X	X	X	X	X	X	X	X	The organization implements an insider threat program that includes a cross discipline insider threat incident handling team.	Please refer to: http://dhsconnect.dhs.gov/org/comp/mgmt/policies/Directives/262_05_002.pdf#search_Insider%20Threat Also, EO 13587 can be referenced for Insider Threats.
PM 13 Protect Function: PR.AT 1, PR.AT 2, PR.AT 4, PR.AT 5*	Information Security Workforce	X	X	X	X	X	X	X	X	X	The organization establishes an information security workforce development and improvement program.	
PM 14 Protect Function: PR.IP 10* Detect Function: DE.DP 1, DE.DP 2, DE.DP 3, DE.DP 5*	Testing, Training, and Monitoring	X	X	X	X	X	X	X	X	X	The organization: a. Implements a process for ensuring that organizational plans for conducting security testing, training, and monitoring activities associated with organizational information systems: 1. Are developed and maintained; and 2. Continue to be executed in a timely manner; b. Reviews testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization wide priorities for risk response actions.	
PM 15 Identify Function: ID.RA 2*	Contacts With Security Groups and Associations	X	X	X	X	X	X	X	X	X	The organization establishes and institutionalizes contact with selected groups and associations within the security community: a. To facilitate ongoing security education and training for organizational personnel;	

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		H	M	L	H	M	L	H	M	L	4300B.102	
Respond Function: RS.CO 5, RS.AN 5*											b. To maintain currency with recommended security practices, techniques, and technologies; and c. To share current security related information including threats, vulnerabilities, and incidents.	
PM 16 Identify Function: ID.RA 2, ID.RA 3, ID.RA 5*	Threat Program	X	X	X	X	X	X	X	X	X	The organization implements an insider threat program that includes a cross discipline insider threat incident handling team.	Please refer to: http://dhsconnect.dhs.gov/org/comp/mgmt/policies/Directives/262_05_002.pdf#search_Insider%20Threat

Privacy Controls

ID	Title	C			I			A			Combined Security Control Text with Defined Values (NIST/CNSS/DHS)	Supplemental Policy Guidance
		L	M	H	L	M	H	L	M	H	4300B.102	
AP-1	Authority to Collect		X	X	X	X	X	X	X	X	The organization determines and documents the legal authority that permits the collection, use, maintenance, and sharing of PII, either generally or in support of a specific program or information system need	See System of Record Notification (SORN) template section "Authority for maintenance of the system" and Privacy Impact Assessment (PIA) section 1.1. The DHS PIA template requires that Systems/Program owners list all statutory and regulatory authority for operating the project, including the authority to collect the information listed in PIA question 2.1. Systems/Program owners must explain how the statutory and regulatory authority permits collection and use of the information. A simple citation without more information will not be sufficient for purposes of this document and will result in rejection of a PIA. Systems/Program owners must explain how the statutory and regulatory authority permits the project and the collection of the subject information. If the project collects Social Security numbers, Systems/Program owners must identify the specific statutory authority allowing such collection. If relying on another component and/or agency, please list their legal authorities. Where information is received from a foreign government pursuant to an international agreement or memorandum of understanding, cite the agreement and where it can be found (e.g. website).
AP-2	Purpose Specification		X	X	X	X	X	X	X	X	The organization describes the purpose(s) for which PII is collected, used, maintained, and shared in its privacy notices.	See SORN "Purpose" section and any corresponding Privacy Act Statements which inform each individual whom the System/Program asks to supply information, on the form which it uses to collect the information or on a separate form that can be retained by the individual: (A) the authority (whether granted by statute, or by executive order of the President) which authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary; (B) the principal purpose or purposes for which the information is intended to be used; (C) the routine uses which may be made of the information, as published pursuant to paragraph (4)(D) of this subsection; and (D) the effects on him, if any, of not providing all or any part of the requested information.
AR-1	Governance and Privacy Program	X	X	X	X	X	X	X	X	X	The organization: a. Appoints a SAOP/Chief Privacy Officer accountable for developing, implementing, and maintaining an organization-wide governance and	a. The DHS Chief Privacy Officer, a statutorily mandated position by Section 222 of the Homeland Security Act (6 U.S.C. § 142), serves as the DHS SAOP and reports directly to the Secretary of Homeland Security. Per DHS Directive 047-01 "Privacy Policy and Compliance" and Instruction

											privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of personally identifiable information (PII) by programs and information systems; b. Monitors federal privacy laws and policy for changes that affect the privacy program; c. Allocates [*Assignment: organization-defined allocation of budget and staffing*] sufficient resources to implement and operate the organization-wide privacy program; d. Develops a strategic organizational privacy plan for implementing applicable privacy controls, policies, and procedures; e. Develops, disseminates, and implements operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII; and f. Updates privacy plan, policies, and procedures at least biennially **[CNSS]**.	047-01-001 the DHS Chief Privacy Officer is responsible for all aspects of the privacy governance program at the Department, including establishing, overseeing the implementation of, and issuing guidance on DHS privacy policy; and ensuring that the Department's use of technology sustains, and does not erode, privacy protections relating to the collection, use, maintenance, disclosure, deletion, and/or destruction of PII. b. Per DHS Directive 047-01 "Privacy Policy and Compliance" and Instruction 047-01-001 the DHS Chief Privacy Officer is responsible for ensuring that the Department follows privacy laws applicable to DHS, and federal government-wide privacy policies in collecting, using, maintaining, disclosing, deleting, and/or destroying PII. c. The DHS PRIV allocates, through the annual appropriations process, sufficient resources to implement and operate the organization-wide privacy program. d. The strategic goals and objectives of the DHS Chief Privacy Officer are detailed in the PRIV "FY 2015-2018 Strategic Plan," DHS Directive 047-01 "Privacy Policy and Compliance"" and Instruction 047-01-001. e. DHS Privacy Office publishes policies and procedures as needed to ensure that Department technology sustains and does not erode, privacy protections relating to the collection, use, maintenance, disclosure, deletion, and/or destruction of PII. In addition to the comprehensive DHS Directive 047-01 "Privacy Policy and Compliance" and Instruction 047-01-001, the DHS Privacy Office has published policies governing the appropriate privacy and security controls for programs, information systems, or technologies involving PII on the publicly available website, www.dhs.gov/privacy. Examples include: Privacy Policy Guidance Memorandum 2011-02, "Department policy establishing a formal Department-wide approach to the roles and responsibilities accompanying the cross-component sharing of IT services" (June 30, 2011); Privacy Policy Guidance Memorandum 2008-01, "The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security," (December 29, 2008); and Privacy Policy Guidance Memorandum 2007-02, "Regarding the use of Social Security numbers at the Department of Homeland Security," (June 4, 2007), and DHS Directive 110-01, "Privacy Policy for Operational Use of Social Media," and corresponding Instruction (June 8, 2012) f. Pursuant to the authority of the DHS Chief Privacy Officer in Section 222 of the Homeland Security Act (6 U.S.C. §

											142), the DHS Privacy Office updates privacy plans, policies, and procedures on an as needed and continual basis, but at least biennially.
AR-2	Privacy Impact and Risk Assessment	X	X	X	X	X	X	X	X	X	The organization: a. Documents and implements a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of personally identifiable information (PII); and b. Conducts PIAs for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures.	a. Per DHS Directive 047-01 "Privacy Policy and Compliance" and Instruction 047-01-001, the DHS Chief Privacy Officer is responsible for the entire privacy risk management framework including (1) Establishing, overseeing the implementation of, and issuing guidance on DHS privacy policy; (2) ensuring in coordination with Component heads and Component Privacy Officers and Privacy Points of Contact (PPOC), that the Department follows DHS privacy policy, privacy laws applicable to DHS, and federal government-wide privacy policies in collecting, using, maintaining, disclosing, deleting, and/or destroying PII, and in implementing any other activity that impacts the privacy of individuals; (3) Ensuring that the Department's use of technology sustains, and does not erode, privacy protections relating to the collection, use, maintenance, disclosure, deletion, and/or destruction of PII; (4) Evaluating Department regulations, rulemakings, technologies, policies, procedures, guidelines, programs, projects, or systems (including pilot activities), whether proposed or operational, for potential privacy impacts and advising DHS leadership and Components on implementing corresponding privacy protections. The Privacy Threshold Analysis (PTA) process identifies when privacy compliance documentation and subsequent notices require an update. The DHS Chief Privacy Officer schedules completed PTAs, PIAs, and SORNs for mandatory review as follows: at least every three years for PTAs and PIAs, and every two years for SORNs. The DHS Chief Privacy Officer notifies the relevant Component Privacy Officer or PPOC that a PTA, PIA, and/or SORN review is required and begins the collaborative review process, which follows the process described in this Instruction for new PTAs, PIAs, and SORNs. b. Per DHS Directive 047-01 "Privacy Policy and Compliance" and Instruction 047-01-001 and DHS privacy policy memorandum 2008-02, the DHS Chief Privacy Officer conducts Privacy Impact Assessments (PIAs) under four specific statutory authorities. (1) Section 208 of the E-Government Act of 20021 requires PIAs of all information technology that uses, maintains, or disseminates personally identifiable information (PII) or when initiating a new collection of PII from ten or more individuals in the public. (2) Congress requires the DHS Chief Privacy Officer to conduct PIAs on certain programs and activities of the Department. (3) Section 222(a)(4) of the Homeland Security Act of 2002, as amended,2 authorizes the DHS Chief Privacy Officer to conduct PIAs on rulemakings proposed by DHS. (4) Section 222(a)(1) of the Homeland

											Security Act authorizes the DHS Chief Privacy Officer to ensure that technologies employed at DHS sustain, and do not erode, privacy protections.
AR-3	Privacy Requirements for Contractors and Service Providers	X	X	X	X	X	X	X	X	X	The organization: a. Establishes privacy roles, responsibilities, and access requirements for contractors and service providers; and b. Includes privacy requirements in contracts and other acquisition-related documents.	a. DHS adheres to the requirements in the Federal Acquisition Regulations, subpart 24.1. In addition, the DHS Chief Privacy Officer determines privacy policy and standards for the Department consistent with the Fair Information Practice Principles (FIPPs); oversees compliance with DHS privacy policy, privacy laws applicable to DHS, and federal government-wide privacy policies; provides privacy guidance and training to DHS personnel regarding the FIPPs; and provides support on privacy-related matters to senior Department leadership and to the Components. b. Per DHS Sensitive Systems Policy 4300A, subjection 3.3.j, all statements of work, contract vehicles, and other acquisition-related documents shall include privacy requirements and establish privacy roles, responsibilities, and access requirements for contractors and service providers. In addition, DHS adheres to the requirements in the Federal Acquisition Regulations, subpart 24.1.
AR-4	Privacy Monitoring and Auditing	X	X	X	X	X	X	X	X	X	The organization monitors and audits privacy controls and internal privacy policy continuously **[CNSS]** to ensure effective implementation.	a. Per DHS Directive 047-01 "Privacy Policy and Compliance" and Instruction 047-01-001, Program Managers and System Managers complete all Privacy Compliance Documentation set forth in applicable requirements (e.g., statutes regulations, Executive Orders, and policies issued by the Chief Privacy Officer),... [w]whenever a DHS IT system, technology, rulemaking, program, pilot project, or other activity involves the planned use of PII or otherwise impacts the privacy of individuals as determined by the DHS Chief Privacy Officer, the relevant manager completes a PTA in accordance with Privacy Office guidance and submits it to the Component Privacy Officer or PPOC. The Component Privacy Officer or PPOC reviews the proposed PTA in consultation with counsel for the Component and submits it, together with a recommendation as to whether a PIA is necessary, to the Chief Privacy Officer. The DHS Chief Privacy Officer schedules completed PTAs, PIAs, and SORNs for mandatory review as follows: at least every three years for PTAs and PIAs, and every two years for SORNs. b. Per DHS Directive 047-01 "Privacy Policy and Compliance" and Instruction 047-01-001, the DHS Chief Privacy Officer determines whether a PIA is required, based on answers provided in the PTA and taking into consideration the Component Privacy Officer's or PPOC's recommendation. In addition, the DHS Chief Privacy Officer may conduct a Privacy Compliance Review of the system or program.

AR-5	Privacy Awareness and Training	X	X	X	X	X	X	X	X	X	The organization: a. Develops, implements, and updates a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures; b. Administers basic privacy training at least annually **[CNSS]** and targeted, role-based privacy training for personnel having responsibility for personally identifiable information (PII) or for activities that involve PII at least annually **[CNSS]**; and c. Ensures that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements at least annually **[CNSS]**.	a. DHS Directive 047-01 "Privacy Policy and Compliance" and Instruction 047-01-001 require Privacy Training: New DHS Headquarters Component employees (other than Federal Law Enforcement Training Center employees) receive in-class privacy training provided by the DHS Chief Privacy Officer during their orientation and six months thereafter. All DHS employees and contractors complete annual online privacy training developed by the DHS Chief Privacy Officer or by Component Privacy Officers or PPOCs in consultation with the DHS Chief Privacy Officer. Employees who handle Sensitive PII receive additional, role-based privacy training, if required in addition to Department-wide privacy training, developed by System Managers or Program Managers in consultation with Component Privacy Officers or PPOCs and the Chief Privacy Officer. b. (1) DHS Directive 047-01 "Privacy Policy and Compliance" and Instruction 047-01-001 require new DHS Headquarters Component employees (other than Federal Law Enforcement Training Center employees) receive in-class privacy training provided by the DHS Chief Privacy Officer during their orientation and six months thereafter. All DHS employees and contractors complete annual online privacy training developed by the DHS Chief Privacy Officer or by Component Privacy Officers or PPOCs in consultation with the DHS Chief Privacy Officer. c. (2) DHS Directive 047-01 "Privacy Policy and Compliance" and Instruction 047-01-001 require employees who handle Sensitive PII receive additional, role-based privacy training developed by System Managers or Program Managers in consultation with Component Privacy Officers or PPOCs and the DHS Chief Privacy Officer. System/Program owners, in consultation with the Component Privacy Officer or PPOC and the DHS Chief Privacy Officer, are responsible for developing and implementing privacy procedures and job-related privacy training to safeguard PII in program and system operations, if necessary in addition to existing Department-wide privacy training. The frequency of the role-based training is determined by the system/program owners. d. (1) New DHS Headquarters Component employees (other than Federal Law Enforcement Training Center employees) receive in-class privacy training provided by the Chief Privacy Officer during their orientation and six months thereafter. All DHS employees and contractors must certify completion of annual online privacy training developed by the DHS Chief Privacy Officer or by Component Privacy Officers or PPOCs in consultation with

											the DHS Chief Privacy Officer. e. (2) Employees who handle Sensitive PII receive additional, role-based privacy training developed by System Managers or Program Managers in consultation with Component Privacy Officers or PPOCs and the DHS Chief Privacy Officer.
AR-6	Privacy Reporting	X	X	X	X	X	X	X	X	X	The organization develops, disseminates, and updates reports to the Office of Management and Budget (OMB), Congress, and other oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory privacy program mandates, and to senior management and other personnel with responsibility for monitoring privacy program progress and compliance	DHS Directive 047-01 "Privacy Policy and Compliance" and Instruction 047-01-001 require the DHS Chief Privacy Officer to ensure that the Department meets all reporting requirements mandated by Congress or OMB regarding DHS activities that involve PII or otherwise impact privacy. All DHS reports are published on the public-facing website, www.dhs.gov/privacy and include the DHS PRIV Annual Report to Congress, the Data Mining Report, and reports required by the Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007.
AR-7	Privacy-Enhanced System Design and Development	X	X	X	X	X	X	X	X	X	The organization designs information systems to support privacy by automating privacy controls.	Per "DHS Sensitive Systems" Policy Directive 4300A, subsection 3.14.2.g, the PTA process shall be used to ensure that DHS designs information systems to support privacy by automating privacy controls, to the greatest extent feasible.
AR-8	Accounting of Disclosures		X	X	X	X	X	X	X	X	The organization: a. Keeps an accurate accounting of disclosures of information held in each system of records under its control, including: (1) Date, nature, and purpose of each disclosure of a record; and (2) Name and address of the person or agency to which the disclosure was made; b. Retains the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer; and Makes the accounting of disclosures available to the person named in the record upon request.	All DHS systems/programs: (a) Keep an accurate accounting of disclosures of information held in each system of records under its control, including: (1) Date, nature, and purpose of each disclosure of a record; and (2) Name and address of the person or agency to which the disclosure was made; retains the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer; and makes the accounting of disclosures available to the person named in the record upon request. All DHS systems/programs: (a) Keep an accurate accounting of disclosures of information held in each system of records under its control, including: (1) Date, nature, and purpose of each disclosure of a record; and (2) Name and address of the person or agency to which the disclosure was made; retains the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer; and makes the accounting of disclosures available to the person named in the record upon request. Unless exempted by the Privacy Act, all DHS systems/programs: (a) Keep an accurate accounting of disclosures of information held in each system of records under its control, including: (1) Date, nature, and purpose of each disclosure of a record; and (2) Name and address of the person or agency to which the disclosure was made; retains the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever

											is longer; and makes the accounting of disclosures available to the person named in the record upon request.
DI-1	Data Quality	X	X	X	X	X	X	X	X	X	The organization: a. Confirms to the greatest extent practicable upon collection or creation of personally identifiable information (PII), the accuracy, relevance, timeliness, and completeness of that information; b. Collects PII directly from the individual to the greatest extent practicable; c. Checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems at least every 180 days **[CNSS]**; and d. Issues guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.	a. PIA section 2.4 requires System/Program owners to explain how the project checks the accuracy of the information that the system/program uses or maintains. Describe the process used for checking accuracy. If a commercial data aggregator is involved describe the levels of accuracy required by the contract. Sometimes information is assumed to be accurate, or in R&D, inaccurate information may not have an impact on the individual or the project. If the project does not check for accuracy, please explain why. Describe any technical solutions, policies, or procedures focused on improving data accuracy and integrity of the project. b. PIA section 2.5 Privacy Impact Analysis: Related to Characterization of the Information. Given the specific data elements collected, discuss the privacy risks identified and for each risk explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included. System/Program owners must consider the principle of Individual Participation: Does the program, to the extent possible and practical, collect information directly from the individual? c. PIA section 2.4 requires System/Program owners explain how the project checks the accuracy of the information. Describe the process used for checking accuracy. If a commercial data aggregator is involved describe the levels of accuracy required by the contract. Sometimes information is assumed to be accurate, or in R&D, inaccurate information may not have an impact on the individual or the project. If the project does not check for accuracy, please explain why. Describe any technical solutions, policies, or procedures focused on improving data accuracy and integrity of the project. DHS Directive 047-01 "Privacy Policy and Compliance" and Instruction 047-01-001 and 4300A "Sensitive Systems Policy," subsection 3.14.2 require that whenever a DHS IT system, technology, rulemaking, program, pilot project, or other activity involves the planned use of PII or otherwise impacts the privacy of individuals as determined by the Chief Privacy Officer, the relevant manager completes a PTA in accordance with Privacy Office guidance and submits it to the Component Privacy Officer or PPOC. Component Privacy Officer or PPOC reviews the proposed PTA in consultation with counsel for the Component and submits it, together with a recommendation as to whether a PIA is necessary, to the Chief Privacy Officer. PTAs expire after three years.

											d. DHS issues guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information, including the DHS "Information Sharing Access Agreements Guidebook," Privacy Policy Guidance Memorandum 2007-01, "Regarding Collection Use, Retention, and Dissemination of Information on Non-U.S. Persons" (as amended January 7, 2009), and the DHS PIA and SORN guidance.
DI-1(2)	Data Quality and Integrity Re-Validate PII	X	X	X	X	X	X	X	X	X	The organization requests that the individual or individual's authorized representative revalidate that PII collected is still accurate at least every 180 days **[CNSS]**.	**Refer to the Privacy Control Overlay, if you have Privacy data based on your PTA/PIA.**
DI-2	Data Integrity and Data Integrity Board	X	X	X	X	X	X	X	X	X	The organization: a. Documents processes to ensure the integrity of personally identifiable information (PII) through existing security controls; and b. Establishes a Data Integrity Board when appropriate to oversee organizational Computer Matching Agreements[2] and to ensure that those agreements comply with the computer matching provisions of the Privacy Act.	a. PIA section 1.3 requires System/Program owners provide the date that the ATO was granted or the date it is expected to be awarded. An operational system must comply with DHS MD 4300A, which includes all NIST 800-53 security and privacy controls. Note that all systems containing PII are categorized at a minimum as "moderate" under FIPS Publication 199. If the project does not trigger the C&A requirement, System/Program owners must state that along with an explanation. b. DHS Directive 262-01, "Computer Matching Agreements and the Data Integrity Board," effectuates a Data Integrity Board (DIB) for DHS and provides policies for engaging in and approving Computer Matching Agreements (CMAs) that fall under the Privacy Act of 1974, as amended (5 U.S.C. § 552a).
DM-1	Minimization of Personally Identifiable Information	X	X	X	X	X	X	X	X	X	The organization: a. Identifies the minimum PII elements that are relevant and necessary to accomplish the legally authorized purpose of collection; b. Limits the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent; and	a. PIA section 2.5 Privacy Impact Analysis: Related to Characterization of the Information. Given the specific data elements collected, discuss the privacy risks identified and for each risk explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included. System/Program owners must consider the principle of Minimization: Is the information directly relevant and necessary to accomplish the specific purposes of the program?

[2] Organizations enter into Computer Matching Agreements in connection with computer matching programs to which they are a party. With certain exceptions, a computer matching program is any computerized comparison of two or more automated systems of records or a system of records with nonfederal records for the purpose of establishing or verifying the eligibility of, or continuing compliance with, statutory and regulatory requirements by, applicants for, recipients or beneficiaries of, participants in, or providers of services with respect to cash or in-kind assistance or payments under federal benefit programs or computerized comparisons of two or more automated federal personnel or payroll systems of records or a system of federal personnel or payroll records with nonfederal records. See Computer Matching and Privacy Protection Act of 1988, 5 U.S.C. § 552a (a)(8)(A).

										c. Conducts an initial evaluation of PII holdings and establishes and follows a schedule for regularly reviewing those holdings at least annually **[CNSS]** to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.	b. PIA section 2.5 Privacy Impact Analysis: Related to Characterization of the Information. Given the specific data elements collected, discuss the privacy risks identified and for each risk explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included. System/Program owners must consider the principle of Minimization: Is the information directly relevant and necessary to accomplish the specific purposes of the program? c. DHS Directive 047-01 "Privacy Policy Compliance" and corresponding Instruction 047-01-001, and PTA process generally, requires whenever a DHS IT system, technology, rulemaking, program, pilot project, or other activity involves the planned use of PII or otherwise impacts the privacy of individuals as determined by the Chief Privacy Officer, the relevant manager completes a PTA in accordance with PRIV guidance and submits it to the Component Privacy Officer or PPOC. The Component Privacy Officer or PPOC reviews the proposed PTA in consultation with counsel for the Component and submits it, together with a recommendation as to whether a PIA is necessary, to the Chief Privacy Officer. The Chief Privacy Officer determines whether a PIA is required, based on answers provided in the PTA and taking into consideration the Component Privacy Officer's or PPOC's recommendation.
DM-2	Data Retention and Disposal		X	X	X	X	X	X	X	X	The organization: a. Retains each collection of personally identifiable information (PII) for [*Assignment: organization-defined time period*] to fulfill the purpose(s) identified in the notice or as required by law; b. Disposes of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and Uses [*Assignment: organization-defined techniques or methods*] to ensure secure deletion or destruction of PII (including originals, copies, and archived records).	a. PIA section 5.0, Data Retention by the Project, requires system/program owners to explain the nexus between the original purpose for the collection and this retention period. The minimum amount of information should be maintained for the minimum amount of time in order to support the project. Retention schedules will vary based on the National Archives Records Management (NARA) schedule applicable for the system/program. b. PIA section 1.5 requires the project manager, in consultation with counsel and the component records management officer, must develop a records retention schedule for the records contained in the project that considers the minimum amount of time necessary to retain information while meeting the needs of the project. After the project manager and component records management officer finalize the schedule based on the needs of the project, it is proposed to NARA for official approval. Consult with your records management office for assistance with this question if necessary. If a NARA-approved schedule does not exist, explain what stage the project is in developing and submitting a records retention schedule.

											c. Per DHS Directive 047-01 "Privacy Policy and Compliance" and Instruction 047-01-001, SOs and PMs are responsible for establishing administrative, technical, and physical controls for storing and safeguarding PII consistent with DHS privacy, security, and records management requirements to ensure the protection of PII from unauthorized access, disclosure, or destruction. See also the procedures detailed in the DHS Handbook for Safeguarding Sensitive Personally Identifiable Information.
DM-3	Minimization of PII Used in Testing, Training, and Research	X	X	X	X	X	X	X	X	X	The organization: a. Develops policies and procedures that minimize the use of personally identifiable information (PII) for testing, training, and research; and b. Implements controls to protect PII used for testing, training, and research.	a. DHS Directive 140-06 "Privacy Policy for Research Programs and Projects" establishes the DHS privacy policy for DHS privacy-sensitive research programs and projects. DHS adopts the Principles for Implementing Privacy Protections in DHS Research Projects first enunciated in the 2008 Report to Congress on Data Mining: Technology and Policy (December, 2008) as privacy policy for all DHS privacy-sensitive research. The Chief Privacy Officer determines privacy policy and standards for DHS privacy-sensitive research programs and projects consistent with the Principles for Implementing Privacy Protections in DHS Research Projects; provides privacy guidance and training to DHS personnel involved in privacy-sensitive research; and provides support on privacy-related matters to DHS Components' research efforts. Component heads work with the Chief Privacy Officer to ensure that privacy-sensitive research programs and projects follow DHS privacy policy and standards, thereby enhancing the overall consistency of privacy protections across DHS research, and develop an implementation plan for privacy-sensitive research. b. DHS Directive 140-06-001 "Privacy Policy for Research Programs and Projects Instruction," requires System and Program owners to complete a PTA in accordance with the Component privacy implementation plan. DHS Privacy Office staff and the Component Privacy Officer or PPOC review each PTA to determine how best to apply the DHS Fair Information Practice Principles to each privacy-sensitive program or project. The DHS Privacy Office assists the Component Privacy Officer or PPOC, as appropriate, in identifying privacy impacts to address in a privacy-sensitive program's or project's design and implementation, to ensure that privacy-sensitive research programs or projects sustain privacy protections relating to the collection, use, disclosure, retention, and destruction of PII pursuant to 6 U.S.C . § 142(a)(1). An appropriately cleared Component or external expert participates in the privacy assessment to explain scientific aspects of a proposed privacy-sensitive research program or project where a deeper understanding is needed to make decisions regarding the use of PII. Protections for data use in testing and training are found in Component policies regarding live data, some of which are currently in development.

IP-1	Consent		X	X	X	X	X	X	X	X	The organization: a. Provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of PII prior to its collection; b. Provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII; c. Obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII; and d. Ensures that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.	a. Section 4.2 of the PIA requires System/Program owners to provide the opportunities available for individuals to consent to uses, decline or provide information, or opt out of the project. This question is directed at whether the individual from or about whom information is collected can decline to provide the information and if so, whether the consequences of providing the information are included in the notice. Additionally, System/Program owners must state whether an individual may provide consent for specific uses or whether consent is given to cover all uses (current or potential) of his/her information. If specific consent is permitted or required, how does the individual consent to each use? If notice is provided to explain how an individual may exercise the right to consent to particular uses or decline to provide information describe the process. If this is not an option, explain why not. In some cases, declining to provide information simply means the individual chooses not to participate in the project. b. DHS provides written or oral notice before collecting information from individuals. That notice may include a posted privacy policy, a Privacy Act statement on forms, a PIA, or a SORN published in the Federal Register. Privacy Act Statements at the time of information collection, if applicable, provide individuals an opportunity to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII. For certain law enforcement projects, notice may not be appropriate – Section 4.0 of the PIA requires System/Program owners to explain how providing direct notice to the individual at the time of collection would undermine the law enforcement mission. c. Section 4.2 of the PIA requires System/Program owners to provide the opportunities available for individuals to consent to uses, decline or provide information, or opt out of the project. This question is directed at whether the individual from or about whom information is collected can decline to provide the information and if so, whether the consequences of providing the information are included in the notice. Additionally, System/Program owners must state whether an individual may provide consent for specific uses or whether consent is given to cover all uses (current or potential) of his/her information. If specific consent is permitted or required, how does the individual consent to each use? If notice is provided to explain how an individual may exercise the right to consent to particular uses or decline to provide information describe the process. If this is not an option, explain why not. In some cases, declining to provide information simply means the individual chooses not to participate in the project.

											d. Section 4.3 of the PIA requires System/Program owners to discuss how the notice provided corresponds to the purpose of the project and the stated uses. Discuss how the notice given for the initial collection is consistent with the stated use(s) of the information. Describe how the project has mitigated the risks associated with potentially insufficient notice and opportunity to decline or consent. Consider the following Fair Information Practice Principles (FIPPs) below to assist in providing a response: Principle of Transparency: Has sufficient notice been provided to the individual? Principle of Use Limitation: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice? Principle of Individual Participation: Has the program provided notice to the individual of how the program provides for redress including access and correction, including other purposes of notice such as types of information and controls over security, retention, disposal, etc.?
IP-2	Individual Access	X	X	X	X	X	X	X	X	X	The organization: a. Provides individuals the ability to have access to their PII maintained in its system(s) of records; b. Publishes rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records; c. Publishes access procedures in SORNs; and d. Adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.	a. PIA Section 7.1 requires System/Program owners to describe the procedures to allow individuals to access their information. System/Program owners must describe any procedures or regulations their component has in place that allow access to information collected by the system or project and/or to an accounting of disclosures of that information. Generally speaking, these procedures should include the Department's FOIA/Privacy Act practices. If the Privacy Act does not apply, state why this is the case. If additional mechanisms exist, include those in this section. For example, if a component has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the Department's procedures. If the system is exempt from the access provisions of the Privacy Act, explain the basis for the exemption and cite the Final Rule published in the Code of Federal Regulations (CFR) that explains this exemption. If the project is not a Privacy Act system, explain what procedures and/or regulations are in place that cover an individual gaining access to his/her own information. b. Rules and regulations governing how individuals may request access to records maintained in a DHS Privacy Act system of records are available in individual DHS System of Record Notices published in the Federal Register. Final Rules exempting systems from certain provisions of the Privacy Act are available at 6 CFR Part 5.

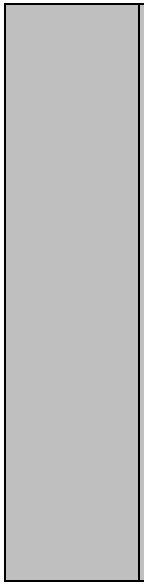
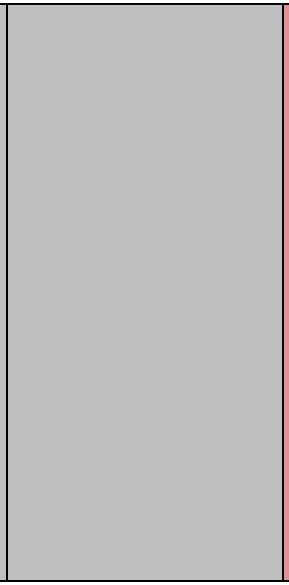
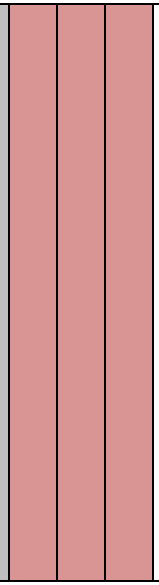
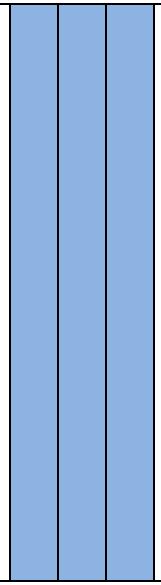
											c. All DHS SORNs must contain sections describing the notification procedures, record access procedures, and contesting record procedures. Individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the Chief Privacy Officer. Individuals seeking records about themselves from a system of records must conform to the Privacy Act regulations set forth in 6 CFR Part 5. d. See 6 CFR Part 5, and Privacy Policy Guidance Memorandum 2011-01, "Privacy Act Amendment Requests" (February 11, 2011), which sets out the Chief Privacy Officer's guidance for processing Privacy Act Amendment requests.
IP-3	Redress	X	X	X	X	X	X	X	X	X	The organization: a. Provides a process for individuals to have inaccurate PII maintained by the organization corrected or amended, as appropriate; and b. Establishes a process for disseminating corrections or amendments of the PII to other authorized users of the PII, such as external information-sharing partners and, where feasible and appropriate, notifies affected individuals that their information has been corrected or amended.	a. DHS Directive 047-01 "Privacy Policy and Compliance" and Instruction 047-01-001 and the Privacy Policy Guidance Memorandum 2011-01, "Privacy Act Amendment Requests" (February 11, 2011) sets forth DHS policy on identifying, processing, tracking, and reporting on requests for amendment of records submitted to DHS under the Privacy Act of 1974, as amended (Amendment Requests). DHS Component Privacy Officers and FOIA Officers shall have robust and documented procedures for identifying, processing, tracking, and reporting on Amendment Requests. Records found in a Privacy Act System of Records and not otherwise exempted are subject to the right to amend. This right is available to individuals whether the request is processed by Component Privacy Officers or FOIA Officers. Components should determine, as part of their documented process, whether the Component Privacy Officer or FOIA Officer will be responsible for identifying, processing, tracking, and reporting Amendment Requests understanding that significant collaboration between the two Officers shall occur. b. DHS Directive 047-01 "Privacy Policy and Compliance" and Instruction 047-01-001 and the Privacy Policy Guidance Memorandum 2011-01, "Privacy Act Amendment Requests" (February 11, 2011) sets forth DHS policy on identifying, processing, tracking, and reporting on requests for amendment of records submitted to DHS under the Privacy Act of 1974, as amended (Amendment Requests). After identifying from the requester which records in a given non-exempt Privacy Act System(s) of Records the requester would like for the Department to amend, the Component Privacy Officer or FOIA Officer should forward the request to the appropriate system manager. The system manager should then confirm that the requester is a subject of a record in the specified Privacy Act System(s) of Records. The system manager, in consultation with the Component Privacy Officer or FOIA Officer as well as

											Counsel, shall make the determination as to whether to amend the record(s) and then shall notify the requester in writing after the initial determination. If the record will be amended, a notification should be sent to system manager(s) informing them of the update and requiring the change be made. If an initial determination is made to deny amendment, the Component Privacy Officer or FOIA Officer will notify the requester of this information and how to appeal the denial, should the requestor choose to do so.
IP-4	Complaint Management	X	X	X	X	X	X	X	X	X	The organization implements a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices.	DHS Directive 047-01 "Privacy Policy and Compliance" and Instruction 047-01-001 requires that the Chief Privacy Officer processes privacy complaints from organizations and individuals regarding Department activities and ensuring that redress is provided, where appropriate. The Chief Privacy Officer collaborates with Component Privacy Officers to review privacy complaints received throughout DHS, and to provide redress as appropriate. Under the terms of a March 2008 Memorandum of Understanding between the Chief Privacy Officer and the DHS Inspector General, OIG has the opportunity to decide whether to conduct investigations of allegations of criminal misconduct, systemic violations, serious management problems, and allegations of non-criminal misconduct by employees at the GS-15 level or higher and all political and Schedule C employees, and, where it declines to do so, refers the matter to the Privacy Office for review and resolution. The Chief Privacy Officer also reviews and responds to traveler complaints related to privacy received through the DHS Traveler Redress Inquiry Program (DHS TRIP). Per DHS Directive 047-01 "Privacy Policy and Compliance" and Instruction 047-01-001, Components review component-specific complaints and refer to the Privacy Control Overlay, if you have Privacy data based on your PTA/PIA.
IP-4(1)	Individual Participation and Redress Response Times	X	X	X	X	X	X	X	X	X	The organization responds to complaints, concerns, or questions from individuals within 2 business days **[CNSS]**.	**Refer to the Privacy Control Overlay, if you have Privacy data based on your PTA/PIA.**
SE-1	Inventory of Personally Identifiable Information	X	X	X	X	X	X	X	X	X	The organization: a. Establishes, maintains, and updates at least annually **[CNSS]** an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing PII; and b. Provides each update of the PII inventory to the CIO or information security official at least annually **[CNSS]** to support the	a. DHS "Sensitive Systems" Policy Directive 4300A, subsection 3.14.2.f, requires that the PTA process is used to maintain a current inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing PII. b. DHS "Sensitive Systems" Policy Directive 4300A, subsection 3.14.2.f, requires the PTA process is used to maintain a current inventory that contains a listing of all programs and information systems identified as collecting,

										establishment of information security requirements for all new or modified information systems containing PII.	using, maintaining, or sharing PII. The DHS Privacy Office provides a component breakdown of the PII inventory and compliance status to the DHS CISO on a quarterly and annual basis as part of the Federal Information Security Management Act (FISMA) reporting requirements.
SE-2	Privacy Incident Response	X	X	X	X	X	X	X	X	X	The organization: a. Develops and implements a Privacy Incident Response Plan; and b. Provides an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan.	a. The "DHS Privacy Incident Handling Guidance" (January 2012), informs all Department personnel of their obligation to protect PII, it also establishes procedures delineating how they must respond to the potential loss or compromise of PII. b. The "DHS Privacy Incident Handling Guidance" (January 2012), informs all Department personnel of their obligation to protect PII, it also establishes procedures delineating how they must respond to the potential loss or compromise of PII.
TR-1	Privacy Notice	X	X	X	X	X	X	X	X	X	The organization: a. Provides effective notice to the public and to individuals regarding: (i) its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of PII; (ii) authority for collecting PII; (iii) the choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices; and (iv) the ability to access and have PII amended or corrected if necessary; b. Describes: (i) the PII the organization collects and the purpose(s) for which it collects that information; (ii) how the organization uses PII internally; (iii) whether the organization shares PII with external entities, the categories of those entities, and the purposes for such sharing; (iv) whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; (v) how individuals may obtain access to PII; and (vi) how the PII will be protected; and c. Revises its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change.	a. Per DHS Directive 047-01 "Privacy Policy and Compliance" and Instruction 047-01-001, System/Program owners are responsible for providing effective notice to the public and to individuals regarding: (i) its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of PII; (ii) authority for collecting PII; (iii) the choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices; and (iv) the ability to access and have PII amended or corrected if necessary. System/Program owners may provide notice through PIAs, SORNs, public-facing websites, and Privacy Act Statements as appropriate. b. Per DHS Directive 047-01 "Privacy Policy and Compliance" and Instruction 047-01-001, System/Program owners are responsible for describing (i) the PII the organization collects and the purpose(s) for which it collects that information; (ii) how the organization uses PII internally; (iii) whether the organization shares PII with external entities, the categories of those entities, and the purposes for such sharing; (iv) whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; (v) how individuals may obtain access to PII; and (vi) how the PII will be protected. System/Program owners may provide notice through PIAs, SORNs, public-facing websites, and Privacy Act Statements as appropriate. c. DHS Directive 047-01 "Privacy Policy and Compliance" and Instruction 047-01-001 require System/Program owners must revise their public notices to reflect changes in practice or policy that affect PII or changes in their activities that impact privacy, before or as soon as

											practicable after the change. The PTA process identifies when privacy compliance documentation and subsequent notices require an update. The Chief Privacy Officer schedules completed PTAs, PIAs, and SORNs for mandatory review as follows: at least every three years for PTAs and PIAs, and every two years for SORNs. The Chief Privacy Officer notifies the relevant Component Privacy Officer or PPOC that a PTA, PIA, and/or SORN review is required and begins the collaborative review process, which follows the process described in this Instruction for new PTAs, PIAs, and SORNs.
TR-2	System of Records Notices and Privacy Act Statements		X	X	X	X	X	X	X	X	The organization: a. Publishes System of Records Notices (SORNs) in the Federal Register, subject to required oversight processes, for systems containing personally identifiable information (PII); b. Keeps SORNs current; and c. Includes Privacy Act Statements on its forms that collect PII, or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected.	a. DHS Directive 047-01 "Privacy Policy and Compliance" and Instruction 047-01-001, require the Chief Privacy Officer, in consultation with the relevant Component Privacy Officer or PPOC and counsel for the Component, determines whether a particular collection of PII is a System of Records for Privacy Act purposes and whether to propose a rule that would exempt the system from certain aspects of the Privacy Act. If the system is a Privacy Act System of Records and it is not covered by an existing SORN, the Component Privacy Officer or PPOC, in consultation with counsel for the Component, prepares a SORN and, where appropriate, an NPRM describing proposed Privacy Act exemptions for the System of Records and, after public comment, a Final Rule, in accordance with guidance issued by the Chief Privacy Officer. The Chief Privacy Officer reviews and provides final approval for all SORNs, NPRMs, and Final Rules. b. System/Program owners review SORNs biennially, as required by OMB Circular A-130. c. Consistent with guidance issued by the Chief Privacy Officer, DHS Directive 047-01 "Privacy Policy and Compliance" and Instruction 047-01-001 require Program Managers and System Managers submit drafts of all Privacy Act Statements to the Chief Privacy Officer, or to the relevant Component Privacy Officer or PPOC, for review and final approval. Privacy Act Statements are included in all documents, whether in paper or electronic form, that the Department uses to collect PII from individuals to be maintained in a Privacy Act System of Records.
TR-3	Dissemination of Privacy Program Information	X	X	X	X	X	X	X	X	X	The organization: a. Ensures that the public has access to information about its privacy activities and is able to communicate with its Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer; and b. Ensures that its privacy practices are publicly available through organizational websites or otherwise.	a. All DHS privacy compliance documentation is published on the public-facing website, www.dhs.gov/privacy. b. All DHS privacy policies and public reports are published on the public-facing website, www.dhs.gov/privacy.

UL-1	Internal Use		X	X	X	X	X	X	X	X	The organization uses PII internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices.	PIA section 3.0 requires System/Program owners to describe how and why the System/Program uses the information. System/Program owners must discuss the intra-Departmental sharing of information. Identify and list the name(s) of any components or directorates within the Department with which the information is shared. Consistent with the Privacy Act, all internal sharing must be consistent with the Privacy Act, 5 U.S.C. § 552a(b)(1) and the "OneDHS" Memorandum (February 1, 2007) which requires that "information shall be shared within DHS whenever the requesting officer or employee has an authorized purpose for accessing the information in the performance of his or her duties, possesses the requisite security clearance, and assures adequate safeguarding and protection of the information.
UL-2	Information Sharing with Third Parties	X	X	X	X	X	X	X	X	X	The organization: a. Shares PII externally, only for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or for a purpose that is compatible with those purposes; b. Where appropriate, enters into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, or similar agreements, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used; c. Monitors, audits, and trains its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII; and d. Evaluates any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.	a. PIA section 6.2 requires System/Program owners to describe how external sharing is compatible with their identified SORNs. System/Program owners must also describe which Routine Uses allow for the external sharing. b. Per DHS Directive 047-01 "Privacy Policy and Compliance" and Instruction 047-01-001, Component Privacy Officers or PPOCs, the Office for Civil Rights and Civil Liberties, and the Office of the General Counsel should be involved in all phases of ISAA development. Component Privacy Officers, PPOCs, or other DHS employees, as appropriate, submit all proposed interagency ISAAs involving PII to the Chief Privacy Officer for review and approval prior to finalizing an agreement. The Office of Policy submits all proposed international ISAAs to the Chief Privacy Officer for review and approval. The Chief Privacy Officer reviews all proposed ISAAs and works with the relevant Component Privacy Officer or PPOC , or the Office of International Affairs, as appropriate, to ensure that such agreements are amended, where necessary, to fully comply with DHS privacy policy and ISAA guidance. c.(1) Per DHS Directive 047-01 "Privacy Policy and Compliance" and Instruction 047-01-001, new DHS Headquarters Component employees (other than Federal Law Enforcement Training Center employees) receive in-class privacy training provided by the Chief Privacy Officer during their orientation and six months thereafter. All DHS employees and contractors complete annual online privacy training developed by the Chief Privacy Officer or by Component Privacy Officers or PPOCs in consultation with the Chief Privacy Officer. c.(2) Per DHS Directive 047-01 "Privacy Policy and Compliance" and Instruction 047-01-001, employees who handle Sensitive PII receive additional, role-based privacy training developed by System Managers or Program

											Managers in consultation with Component Privacy Officers or PPOCs and the Chief Privacy Officer. d.(1) Per DHS Directive 047-01 "Privacy Policy and Compliance" and Instruction 047-01-001, Component Privacy Officers or PPOCs, the Office for Civil Rights and Civil Liberties, and the Office of the General Counsel should be involved in all phases of ISAA development. Component Privacy Officers, PPOCs, or other DHS employees, as appropriate, submit all proposed interagency ISAAs involving PII to the Chief Privacy Officer for review and approval prior to finalizing an agreement. The Office of Policy (PLCY) submits all proposed international ISAAs to the Chief Privacy Officer for review and approval. d.(2) Per DHS Directive 047-01 "Privacy Policy and Compliance" and Instruction 047-01-001, the Chief Privacy Officer reviews all proposed ISAAs and works with the relevant Component Privacy Officer or PPOC , or the Office of International Affairs, as appropriate, to ensure that such agreements are amended, where necessary, to fully comply with DHS privacy policy and ISAA guidance.

8.0 Abbreviations & Acronyms

AC	Access Control Family
AO	Authorizing Official
AP	Authority and Purpose Family
AR	Accountability, Audit, and Risk Management Family
ASHRAE	American Society of Heating, Refrigeration and Air Conditioning Engineers
AT	Awareness and Training Family
ATO	Authorization to Operate
AU	Audit and Accountability Family
CA	Security Assessment and Authorization Family
CCB	Configuration Control Board
CD	Compact Disk
CDS	Cross Domain Solution
CEA	Cybersecurity Enhancement Act
CERT	Computer Emergency Readiness Team
CFO	Chief Financial Officer
CFR	Code of Federal Regulations

CIACS	Classified Information Assurance Compliance System
C-ICCB	Classified Infrastructure Change Control Board
CIRT	Computer Incident Response Team
CISO	Chief Information Security Officer
CM	Configuration Management Family
CMB	Configuration Management Board
CMP	Configuration Management Plan
CNSS	Committee on National Security Systems
CNSSD	Committee on National Security Systems Directive
CNSSI	Committee on National Security Systems Instruction
CNSSP	Committee on National Security Systems Policy
COI	Community of Interest
COMSEC	Communication Security
CONOPS	Concept of Operations
CMA	Computer Matching Agreements
CP	Contingency Plan Family
CPIC	Capital Planning and Investment Control
CPP	Cybersecurity Performance Plan

CSP	Common Service Provider
CSS	Central Security Service
DBA	Database Administrator
DHS	Department of Homeland Security
DI	Data Quality and Integrity Family
DISA	Defense Information Systems Agency
DM	Data Minimization and Retention Family
DoD	Department of Defense
DVD	Digital Video Disk
EO	Executive Order
FICAM	Federal Identity Credential and Access Management
FIPPS	Fair Information Practice Principles
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FYHSP	Future Years Homeland Security Program
GMT	Greenwich Mean Time
HSAR	Homeland Security Acquisition Regulation
HSDN	Homeland Secure Data Network

HSPD	Homeland Security Presidential Directive
IA	Identification and Authentication Family
ICS	Industrial Control System
IP	Individual Participation and Redress Family
IR	Incident Response Family
I/O	Input/Output
IS	Information System
ISA	Interconnection Security Agreement
ISAA	Information Sharing and Access Agreement
ISO	Information System Owner
ISSM	Information System Security Manager
IT	Information Technology
JSCS	Joint Chief of Staff
LAN	Local Area Network
MA	Maintenance Family
MD	Management Directive
MOA	Memorandum of Agreement
MP	Media Protection Family

MS	Microsoft
MTTF	Mean Time to Failure
NARA	National Archives Records Management
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSC	National Security Cyber
NSI	National Security Information
NSS	National Security Systems
OGC	Office of the General Counsel
OMB	Office of Management and Budget
OPSEC	Operations Security
PE	Physical and Environmental Protection Family
PED	Portable Electronic Devices
PIA	Privacy Impact Assessment
PIN	Personal Identification Numbers
PIV	Personal Identity Verification
PKI	Public Key Infrastructure

PL	Planning Family
PLCY	Office of Strategy, Policy, and Plans
PM	Program Manager
POA&M	Plan of Action and Milestones
PM Family	Program Management Family
PRIV	DHS Privacy Office
PS	Personnel Security Family
PTA	Privacy Threshold Analysis
RA	Risk Assessment Family
RAR	Risk Assessment Report
RBAC	Role Based Access Control
SA	System and Services Acquisition Family
SAMI	Sources and Methods Intelligence
SAOP	Senior Agency Official for Privacy (SAOP)
SAP	Special Access Program
SAR	Security Assessment Report
SE	Security Family
SC	System and Communications Protection Family

SCA	Security Control Assessor
SCRM	Supply Chain Risk Management
SCTM	Security Control Traceability Matrix
SELC	Systems Engineering Lifecycle
SF	Standard Form
SI	System and Information Integrity Family
SISO	Supervisory Immigration Services Officer
SO	System Owner
SORN	System of Record Notification
SP	Special Publication
SSO	Special Security Officer
SSP	System Security Plan
STE	Secure Telephone Equipment
STIGs	Security Technical Implementation Guides
TCP/IP	Transmission Control Protocol/Internet Protocol
TR	Transparency
UL	Use Limitation
URL	Universal Resource Locator

USB	Universal Serial Bus
USERIDs	User Identifiers
USG	United States Government
USGCB	United States Government Configuration Baseline
UTC	Universal Time Coordinated
VoIP	Voice over Internet Protocol
VTC	Video Teleconference