APPENDIX E
SECURITY CONTROL PARAMETER VALUES

Table E-1 contains parameter values specified for NSS. These parameter values are minimum standards for NSS. Any deviations from these values should be documented in the security plan. If a control or control enhancement does not appear in Table E-1:

- It does not have an organizationally defined parameter;
- All parameters within a control are not appropriate to define for all NSS at the CNSS level; or
- It was withdrawn from NIST SP 800-53.

Table E-1: Security Control Parameter Values for NSS

ID	Control Text	Defined Value for NSS
AC-1	a. [Assignment: organization-defined personnel or roles]	a. Not appropriate to define at the CNSS level for all organizations operating NSS.
	b.1. [Assignment: organization-defined frequency]	b.1. At least annually if not otherwise defined in formal organizational policy
	b.2. [Assignment: organization-defined frequency]	b.2. At least annually if not otherwise defined in formal organizational policy
AC-2	a. [Assignment: organization-defined information system account types]	a. Not appropriate to define at the CNSS level for all NSS.
	e. [Assignment: organization-defined personnel or roles]	e. Not appropriate to define at the CNSS level for all NSS.
	f. [Assignment: organization-defined procedures or conditions]	f. Not appropriate to define at the CNSS level for all NSS.
	j. [Assignment: organization-defined frequency]	j. At least annually if not otherwise defined in formal organizational policy.
AC-2(2)	[Selection: removes; disables] [Assignment: organization-defined time period for each type of account]	Disables Not to exceed 72 hours.
AC-2(3)	[Assignment: organization-defined time period].	Not to exceed 90 days.
AC-2(5)	[Assignment: organization-defined time-period of expected inactivity or description of when to log out]	At the end of the users standard work period unless otherwise defined in formal organizational policy.
AC-2(7)	(c) [Assignment: organization-defined actions	(c) Disables (or revokes) privileged user account.
AC-2(13)	[Assignment: organization-defined time period]	30 minutes unless otherwise defined in formal organizational policy.
AC-6(2)	[Assignment: organization-defined security functions or security-relevant information]	Privileged functions.
AC-6(8)	[Assignment: organization-defined software]	All
AC-7	a. [Assignment: organization-defined number]	3

ID	Control Text	Defined Value for NSS	
	[Assignment: organization-defined time period]	15 minutes	
	b. [Selection: locks the account/node for an [Assignment: organization-defined time period] [Assignment: organization-defined delay algorithm]]	b. locks the account/node for at least 15 minutes, or until unlocked by an administrator. Not appropriate to define at the CNSS level for all NSS.	
AC-7(2)	[Assignment: organization-defined mobile devices] [Assignment: organization-defined purging/wiping requirements/techniques] [Assignment: organization-defined number]	Not appropriate to define at the CNSS level for all NSS. Not appropriate to define at the CNSS level for all NSS. 10	
AC-9(3)	[Assignment: organization-defined security-related characteristics/parameters of the user's account] [Assignment: organization-defined time period]	Not appropriate to define at the CNSS level for all NSS. Since last successful logon	
AC-10	[Assignment: organization-defined account and/or account type] [Assignment: organization-defined number]	Non-Privileged maximum of 3 sessions	Privileged maximum of 3 sessions
AC-11	a. [Assignment: organization-defined time period]	Not to exceed 30 minutes	
AC-12(1)	(a) [Assignment: organization-defined information resources]	(a) All	
AC-14	a. [Assignment: organization-defined user actions]	a. No user actions	
AC-17(9)	[Assignment: organization-defined time period]	Low confidentiality or integrity impact: ...30 minutes Moderate confidentiality or integrity impact: ...20 minutes High confidentiality or integrity impact: ...10 minutes	
AC-18(1)	[Selection (one or more): users; devices]	Both users and devices as appropriate. See supplemental guidance. Supplemental Guidance: devices to wireless networks (e.g., Wi-Fi) and users to enterprise services.	
AC-19(5)	[Selection: full-device encryption; container encryption] [Assignment: organization-defined mobile devices]	Not appropriate to define at the CNSS level for all NSS. All mobile devices authorized to connect to the organization's ISs.	

ID	Control Text	Defined Value for NSS
AC-20(3)	[Selection: restricts; prohibits]	Restricts
AC-22	d. [Assignment: organization-defined frequency]	d. Quarterly or as new information is posted.
AT-1	a. [Assignment: organization-defined personnel or roles]	a. All personnel
	b.1. [Assignment: organization-defined frequency]	b.1. At least annually if not otherwise defined in formal organizational policy.
	b.2. [Assignment: organization-defined frequency]	b.2. At least annually if not otherwise defined in formal organizational policy.
AT-2	c. [Assignment: organization-defined frequency]	c. At least annually if not otherwise defined in formal organization.
AT-3	c. [Assignment: organization-defined frequency]	c. At least annually if not otherwise defined in formal organization.
AT-3(1)	[Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency]	Not appropriate to define at the CNSS level for all NSS. At least annually if not otherwise defined in formal organization policy or when sufficient changes are made to physical security systems.
AT-3(2)	[Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency]	Not appropriate to define at the CNSS level for all NSS. At least annually if not otherwise defined in formal organization policy or when sufficient changes are made to physical security systems.
AT-3(4)	[Assignment: organization-defined indicators of malicious code]	Minimally but not limited to indicators of potentially malicious code in suspicious email.
AU-1	a. [Assignment: organization-defined personnel or roles]	a. All personnel
	b.1. [Assignment: organization-defined frequency]	b.1. At least annually if not otherwise defined in formal organizational policy.
	b.2. [Assignment: organization-defined frequency]	b.2. At least annually if not otherwise defined in formal organizational policy.
AU-2	a. [Assignment: organization-defined auditable events]	a. 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)

ID	Control Text	Defined Value for NSS
		4. Uploads from external devices (e.g., CD/DVD drives) (Success/Failure) 5. User and Group Management events: (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, 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)
	d. [Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event]	d. Not appropriate to define at the CNSS level for all NSS.
AU-2(3)	[Assignment: organization-defined frequency]	At least annually if not otherwise defined in formal organizational policy
AU-5(1)	[Assignment: organization-defined personnel, roles, and/or locations] [Assignment: organization-defined time period] [Assignment: organization-defined percentage]	Not appropriate to define at the CNSS level for all NSS. Not appropriate to define at the CNSS level for all NSS. Max of 75%

ID	Control Text	Defined Value for NSS
AU-5(2)	[Assignment: organization-defined real-time period] [Assignment: organization-defined personnel, roles, and/or locations] [Assignment: organization-defined audit failure events requiring real-time alerts]	Not appropriate to define at the CNSS level for all NSS. Not appropriate to define at the CNSS level for all NSS. Minimally but not limited to: auditing software/hardware errors; failures in the audit capturing mechanisms; and audit storage capacity being reached or exceeded.
AU-6	a. [Assignment: organization-defined frequency] [Assignment: organization-defined inappropriate or unusual activity]	a. At least weekly (seven days) Not appropriate to define at the CNSS level for all NSS.
	b. [Assignment: organization-defined personnel or roles]	b. Not appropriate to define at the CNSS level for all NSS.
AU-8(1)	(a) [Assignment: organization-defined frequency] [Assignment: organization-defined authoritative time source]	(a) At least every 24 hours. (a) Not appropriate to define at the CNSS level for all NSS.
	(b) [Assignment: organization-defined time period]	(b) Greater than the organizationally defined granularity in AU-8.
AU-9(2)	[Assignment: organization-defined frequency]	a. At least weekly.
AU-9(5)	[Selection (one or more): movement; deletion] [Assignment: organization-defined audit information]	Not appropriate to define at the CNSS level for all NSS. Any security related audit information.
AU-11	[Assignment: organization-defined time period consistent with records retention policy]	A minimum of 5 years for Sensitive Compartmented Information and Sources And Methods Intelligence information AND A minimum of 1 year for all other information (Unclassified through Collateral Top Secret).
AU-11(1)	[Assignment: organization-defined measures]	A retention of technology to access audit records for the duration of the required retention period.
AU-12	a. [Assignment: organization-defined information system components]	a. All information systems and network components.
	b. Assignment: organization-defined personnel or roles]	b. Not appropriate to define at the CNSS level for all NSS.
AU-12(1)	[Assignment: organization-defined information system components] [Assignment: organization-defined level of tolerance for relationship between time stamps of individual records in the audit trail]	Not appropriate to define at the CNSS level for all NSS. In accordance with tolerance defined in AU-8.
AU-13(2)	[Assignment: organization-defined frequency]	At least annually if not otherwise defined in formal organizational policy.

ID	Control Text	Defined Value for NSS
CA-1	a. [Assignment: organization-defined personnel or roles]	a. All personnel.
	b.1. [Assignment: organization-defined frequency]	b.1. At least annually if not otherwise defined in formal organizational policy.
	b.2. [Assignment: organization-defined frequency]	b.2. At least annually if not otherwise defined in formal organizational policy.
CA-2	b. [Assignment: organization-defined frequency]	b. At least annually, or as stipulated in the organization's continuous monitoring program.
	d. [Assignment: organization-defined individuals or roles]	d. Not appropriate to define at the CNSS level for all NSS.
CA-3	c. [Assignment: organization-defined frequency]	c. At least annually.
CA-3(1)	[Assignment: organization-defined unclassified, national security system] [Assignment: organization-defined boundary protection device]	All unclassified NSS. Not appropriate to define at the CNSS level for all NSS.
CA-3(5)	[Selection: allow-all, deny-by-exception; deny-all, permit-by-exception] [Assignment: organization-defined information systems] to connect to external information systems.	Deny-all, permit-by-exception. All systems.
CA-5	[Assignment: organization-defined frequency]	b. At least quarterly.
CA-6	c. [Assignment: organization-defined frequency]	c. 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.
CM-1	a. [Assignment: organization-defined personnel or roles]	a. Not appropriate to define at the CNSS level for all NSS.
	b.1. [Assignment: organization-defined frequency]	b.1. At least annually if not otherwise defined in formal organizational policy.
	b.2. [Assignment: organization-defined frequency]	b.2. At least annually if not otherwise defined in formal organizational policy.
CM-2(1)	(a) [Assignment: organization-defined frequency]	(a) At least annually.
	(b) [Assignment organization-defined circumstances]	(b) Significant or security relevant changes or security incidents occur.
CM-2(3)	[Assignment: organization-defined previous versions of baseline configurations of the information system]	At least two.
CM-3	e. [Assignment: organization-defined time period]	e. 1 year or two change cycles of baseline configurations as defined in CM-2 (3), whichever is longer.

ID	Control Text	Defined Value for NSS
	g. [Assignment: organization-defined configuration change control element (e.g., committee, board] [Selection (one or more): [Assignment: organization-defined frequency] [Assignment: organization-defined configuration change conditions]]	g. Not appropriate to define at the CNSS level for all NSS. Not appropriate to define at the CNSS level for all NSS. Not appropriate to define at the CNSS level for all NSS. Not appropriate to define at the CNSS level for all NSS.
CM-3(4)	[Assignment: organization-defined configuration change control element]	The configuration change control element defined in CM-3 g. Supplemental guidance: The information security representative shall be a voting member.
CM-3(6)	[Assignment: organization-defined security safeguards]	All security safeguards that rely on cryptography
CM-5(2)	[Assignment: organization-defined frequency] [Assignment: organization-defined circumstances]	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. When there is an incident or when planned changes have been performed.
CM-5(3)	[Assignment: organization-defined software and firmware components]	All digitally signed software and firmware products.
CM-5(5)	(b) [Assignment: organization-defined frequency]	(b) At least annually.
CM-6	a. [Assignment: organization-defined security configuration checklists]	a. Organizationally approved guides such as DoD SRGs, STIGs, or NSA SCGs; if such a reference document is not available, the following are acceptable in descending order as available: (1) Commercially accepted practices (e.g., SANS) (2) Independent testing results (e.g., ICSA) or (3) Vendor literature.
	c. [Assignment: organization-defined information system components] [Assignment: organization-defined operational requirements]	c. All configurable information system components. Not appropriate to define at the CNSS level for all NSS.
CM-6(1)	[Assignment: organization-defined information system components]	Not appropriate to define at the CNSS level for all NSS but minimally for all IA enabled or related components.
CM-7(1)	(a) [Assignment: organization-defined frequency]	(a) At least annually or as system changes or incidents occur.
	(b) [Assignment: organization-defined functions,	(b) All functions, ports, protocols, and services

ID	Control Text	Defined Value for NSS
	ports, protocols, and services within the information system deemed to be unnecessary and/or nonsecure]	within the information system deemed to be unnecessary and/or nonsecure.
CM-7(4)	(a) [Assignment: organization-defined software programs not authorized to execute on the information system]	(a) Not appropriate to define at the CNSS level for all NSS.
	(c) [Assignment: organization-defined frequency]	(c) At least annually.
CM-7(5)	(a) [Assignment: organization-defined software programs authorized to execute on the information system]	(a) Not appropriate to define at the CNSS level for all NSS.
	(c) [Assignment: organization-defined frequency]	(c) At least annually.
CM-8	a.4. [Assignment: organization-defined information deemed necessary to achieve effective information system component accountability]	a.4. 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.
	b. [Assignment: organization-defined frequency]	b. At least annually.
CM-8(3)	(a) [Assignment: organization-defined frequency]	(a) Continuously.
	(b) [Selection (one or more): disables network access by such components; isolates the components; notifies [Assignment: organization-defined personnel or roles]]	(b) Not appropriate to define at the CNSS level for all NSS. Not appropriate to define at the CNSS level for all NSS.
CM-8(4)	[Selection (one or more): name; position; role]	Minimally position or role.
CM-8(9)	(a) [Assignment: organization-defined acquired information system components]	All acquired information system components. See supplemental guidance. Supplemental guidance: this is part of Security Authorization, "authorization boundary".
CM-11	a. [Assignment: organization-defined policies]	a. Not appropriate to define at the CNSS level for all NSS.
	b. [Assignment: organization-defined methods]	b. Not appropriate to define at the CNSS level for all NSS.
	c. [Assignment: organization-defined frequency]	c. Continuously.
CP-1	a. [Assignment: organization-defined personnel or roles]	a. Not appropriate to define at the CNSS level for all NSS.
	b.1. [Assignment: organization-defined frequency]	b.1. At least annually if not otherwise defined in formal organizational policy.
	b.2. [Assignment: organization-defined frequency]	b.2. At least annually if not otherwise defined in formal organizational policy.
CP-2	a.6. [Assignment: organization-defined personnel or roles]	a.6. Not appropriate to define at the CNSS level for all NSS.

ID	Control Text	Defined Value for NSS
	b. [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]	b. Key personnel or roles and organizational elements identified in the contingency plan.
	d. [Assignment: organization-defined frequency]	d. At least annually unless otherwise defined in organizational policy.
	f. [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]	f. Key personnel and .organizational elements identified in the contingency plan.
CP-2(3)	[Assignment: organization-defined time period]	A time period as defined in the contingency plan.
CP-2(4)	[Assignment: organization-defined time period]	A time period as defined in the contingency plan.
CP-3	a. [Assignment: organization-defined time period]	a. 10 working days .
	c. [Assignment: organization-defined frequency]	c. Annually or as defined in the contingency plan.
CP-4	a. [Assignment: organization-defined frequency] [Assignment: organization-defined tests]	a. At a frequency as defined in the contingency plan. Tests as defined in the contingency plan.
CP-7	a. [Assignment: organization-defined information system operations] [Assignment: organization-defined time period consistent with recovery time and recovery point objectives]	a. Information system operations as defined in the contingency plan. A time period as defined in the contingency plan.
CP-8	[Assignment: organization-defined information system operations] [Assignment: organization-defined time period]	Information system operations as defined in the contingency plan. A time period as defined in the contingency plan.
CP-9	a. [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]	a. At least weekly or as defined in the contingency plan.
	b. [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]	b. At least weekly or as defined in the contingency plan.
	c. [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]	c. When created, received, updated, or as defined in the contingency plan.
CP-9(1)	[Assignment: organization-defined frequency]	At least monthly or as defined in the contingency plan.
CP-9(3)	[Assignment: organization-defined critical information system software and other security-related information]	Not appropriate to define at the CNSS level for all NSS but as defined in the contingency plan.
CP-9(5)	[Assignment: organization-defined time period and transfer rate consistent with the recovery time and recovery point objectives]	Not appropriate to define at the CNSS level for all NSS but as defined in the contingency plan.
CP-9(7)	[Assignment: organization-defined backup	Not appropriate to define at the CNSS level for

ID	Control Text	Defined Value for NSS
	information]	all NSS, but as defined in the contingency plan.
CP-10(4)	[Assignment: organization-defined restoration time-periods]	Not appropriate to define at the CNSS level for all NSS but as defined in the contingency plan.
CP-11	[Assignment: organization-defined alternative communications protocols]	Alternate communications protocols as defined in the contingency plan.
IA-1	a. [Assignment: organization-defined personnel or roles]	a. All personnel.
	b.1. Identification and authentication policy [Assignment: organization-defined frequency]; and	b.1. At least annually if not otherwise defined in formal organizational policy.
	b.2. Identification and authentication procedures [Assignment: organization-defined frequency]	b.2. At least annually if not otherwise defined in formal organizational policy.
IA-4	a. [Assignment: organization-defined personnel or roles]	a. Not appropriate to define at the CNSS level for all NSS.
	d.[Assignment: organization-defined time period]	d. At least a year for individuals, groups, roles ...Not appropriate to define for device identifiers (e.g., media access control (MAC), Internet protocol (IP) addresses, or device-unique token identifiers."
	e. [Assignment: organization-defined time period of inactivity]	e. Not to exceed 35 days for individuals, groups, roles. Not appropriate to define for device identifiers (e.g., media access control (MAC), Internet protocol (IP) addresses, or device-unique token identifiers."
IA-5	g. [Assignment: organization-defined time period by authenticator type]	g. Not to exceed 180 days for passwords; ...Not appropriate to define at the CNSS level for all NSS using other authenticator types.
IA-5(1)	(a) [Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type]	(a) A case sensitive 12-character mix of upper case letters, lower case letters, numbers and special characters in including at least one of each.
	(b) [Assignment: organization-defined number]	(b) 50% of the characters.
	(d) [Assignment: organization-defined numbers for lifetime minimum, lifetime maximum]	d) 24 hours minimum and 180 days maximum.
	(e) [Assignment: organization-defined number]	(e) Minimum of 10; (does not apply to one time use passwords).
IA-5(4)	[Assignment: organization-defined requirements]	Requirements as defined in IA-5 (1).
IA-5(8)	[Assignment: organization-defined security safeguards]	Precautions including advising users that they must not 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 Intelink).; More than one privilege level (e.g., user, administrator).

ID	Control Text	Defined Value for NSS
IA-5(13)	[Assignment: organization-defined time period].	1 hour.
IR-1	a. [Assignment: organization-defined personnel or roles]	a. Not appropriate to define at the CNSS level for all NSS.
	b.1. [Assignment: organization-defined frequency]	b.1. At least annually if not otherwise defined in formal organizational policy.
	b.2. [Assignment: organization-defined frequency]	b.2. At least annually if not otherwise defined in formal organizational policy.
IR-2	a. [Assignment: organization-defined time period]	a. 30 working days.
	c. [Assignment: organization-defined frequency]	c. At least annually.
IR-3	[Assignment: organization-defined frequency] [Assignment: organization-defined tests]	At least annually. Not appropriate to define at the CNSS level for all NSS.
IR-4(8)	[Assignment: organization-defined external organizations] [Assignment: organization-defined incident information]	The appropriate CIRT/CERT (such as US-CERT, DoD CERT, IC CERT) Not appropriate to define at the CNSS level for all NSS.
IR-6	a. [Assignment: organization-defined time period]	a. 2 hours if not otherwise defined in formal organizational policy.
	b. [Assignment: organization-defined authorities]	b. The appropriate Agency CIRT/CERT (see IR-4(8)).
IR-8	a.8. [Assignment: organization-defined personnel or roles]	a.8. CISO/SISO if not otherwise defined in formal organizational policy.
	b. [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]	b. All personnel with a role or responsibility for implementing the incident response plan.
	c. [Assignment: organization-defined frequency]	c. At least annually (incorporating lessons learned from past incidents).
	e. [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]	e. All personnel with a role or responsibility for implementing the incident response plan.
IR-9(2)	[Assignment: organization-defined frequency]	Annually.
MA-1	a. [Assignment: organization-defined personnel or roles]	a. All personnel.
	b.1. [Assignment: organization-defined frequency]	b.1. At least annually if not otherwise defined in formal organizational policy.
	2. [Assignment: organization-defined frequency]	b.2. At least annually if not otherwise defined in formal organizational policy.
MA-4(1)	(a) [Assignment: organization-defined audit events]	(a) As defined in the organizations formal audit policy (AU-1).
MP-1	a. [Assignment: organization-defined personnel or roles]	a. All personnel.
	b. 1. [Assignment: organization-defined frequency]	b.1. At least annually if not otherwise defined in formal organizational policy.

ID	Control Text	Defined Value for NSS
	b.2. [Assignment: organization-defined frequency]	b.2. At least annually if not otherwise defined in formal organizational policy.
MP-2	[Assignment: organization-defined types of digital and/or non-digital media] [Assignment: organization-defined personnel or roles].	All types of digital and/or non-digital media containing information not cleared for public release. Not appropriate to define at the CNSS level for all NSS.
MP-6(2)	[Assignment: organization-defined frequency]	At least annually if not otherwise defined in formal organizational policy.
MP-6(3)	[Assignment: organization-defined circumstances requiring sanitization of portable storage devices]	Not appropriate to define at the CNSS level for all NSS, however the use of nondestructive sanitization techniques are for the elimination of malicious code, not removal of approved information or software.
MP-8(2)	[Assignment: organization-defined tests] [Assignment: organization-defined frequency]	Not appropriate to define at the CNSS level for all NSS. At least annually if not otherwise defined in formal organizational policy.
PE-1	a. [Assignment: organization-defined personnel or roles]	a. All personnel.
	b. 1. [Assignment: organization-defined frequency]	b.1. At least annually if not otherwise defined in formal organizational policy.
	b.2. [Assignment: organization-defined frequency]	b.2. At least annually if not otherwise defined in formal organizational policy.
PE-2	c. [Assignment: organization-defined frequency]	c. At least annually.
PE-6	b. [Assignment: organization-defined frequency] [Assignment: organization-defined events or potential indications of events]	b. At least every 90 days if not otherwise defined in formal organizational policy. Not appropriate to define at the CNSS level for all NSS.
PE-6(3)	[Assignment: organization-defined operational areas] [Assignment: organization-defined time period]	Not appropriate to define at the CNSS level for all NSS. At least 90 days if not otherwise defined in formal organizational policy.
PE-8	a. [Assignment: organization-defined time period]	a. At least one year.
	b. [Assignment: organization-defined frequency]	b. At least every 90 days if not otherwise defined in formal organizational policy.
PE-13(4)	[Assignment: organization-defined frequency] [Assignment: organization-defined time period]	At least annually if not otherwise defined in formal organizational policy. 60 days.
PE-14	a. [Assignment: organization-defined acceptable levels]	a. Not appropriate to define at the CNSS level for all NSS.

ID	Control Text	Defined Value for NSS
	b. [Assignment: organization-defined frequency]	b. continuously.
PL-1	a. [Assignment: organization-defined personnel or roles]	a. All personnel.
	b.1. [Assignment: organization-defined frequency]	b.1. At least annually if not otherwise defined in formal organizational policy.
	b.2. [Assignment: organization-defined frequency]	b.2. At least annually if not otherwise defined in formal organizational policy.
PL-2	b. [Assignment: organization-defined personnel or roles]	b. Not appropriate to define at the CNSS level for all NSS.
	c. [Assignment: organization-defined frequency]	c. At least annually or when required due to system changes or modifications.
PL-4	c. [Assignment: organization-defined frequency]	c. At least annually if not otherwise defined in formal organizational policy.
PL-7	b. [Assignment: organization-defined frequency]	b. At least annually or when changes to the information system or its environment warrant.
PL-8	b. [Assignment: organization-defined frequency]	b. At least annually or when changes to the information system or its environment warrant.
PS-1	a. [Assignment: organization-defined personnel or roles]	a. All personnel.
	b.1. [Assignment: organization-defined frequency]	b.1. At least annually if not otherwise defined in formal organizational policy.
	b.2. [Assignment: organization-defined frequency]	b.2. At least annually if not otherwise defined in formal organizational policy.
PS-2	c. [Assignment: organization-defined frequency]	c. At least annually or when the position description is updated or when the position is vacated.
PS-4	a. [Assignment: organization-defined time period]	a. If voluntary: As soon as possible, not to exceed 5 working days. If involuntary: Within same day as termination.
	c. [Assignment: organization-defined information security topics]	c. Not appropriate to define at the CNSS level for all NSS.
	f. [Assignment: organization-defined personnel or roles] [Assignment: organization-defined time period]	f. Not appropriate to define at the CNSS level for all NSS. As soon as possible, not to exceed 1 working day.
PS-5	b. [Assignment: organization-defined transfer or reassignment actions] [Assignment: organization-defined time period following the formal transfer action]	b. Reassignment actions to ensure all system access no longer required (need to know) are removed or disabled. b. 10 working days if not otherwise defined in formal organizational policy.
	d. [Assignment: organization-defined personnel or roles] [Assignment: organization-defined time period]	d. Not appropriate to define at the CNSS level for all NSS. Not appropriate to define at the CNSS level for

ID	Control Text	Defined Value for NSS
		all NSS.
PS-6	b. [Assignment: organization-defined frequency]	b. At least annually if not otherwise defined in formal organizational policy .
	c.2. [Assignment: organization-defined frequency]	c.2. At least annually if not otherwise defined in formal organizational policy.
PS-7	d. [Assignment: organization-defined personnel or roles] [Assignment: organization-defined time period]	d. Organizational Security Manager. As soon as possible, not to exceed 1 working day.
RA-1	a. [Assignment: organization-defined personnel or roles]	a. All personnel
	b.1. [Assignment: organization-defined frequency]	b.1. At least annually if not otherwise defined in formal organizational policy.
	b.2. [Assignment: organization-defined frequency]	b.2. At least annually if not otherwise defined in formal organizational policy.
RA-3	b. [Selection: security plan; risk assessment report; [Assignment: organization-defined document]]	b. Not appropriate to define at the CNSS level for all NSS. Not appropriate to define at the CNSS level for all NSS.
	c. [Assignment: organization-defined frequency]	c. At least annually if not otherwise defined in formal organizational policy.
	d. [Assignment: organization-defined personnel or roles]	d. Not appropriate to define at the CNSS level for all NSS.
	e. [Assignment: organization-defined frequency]	e. At least annually if not otherwise defined in formal organizational policy.
RA-5	a. [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process]	a. At least every 120 days.
	d. [Assignment: organization-defined response times]	d. Not appropriate to define at the CNSS level for all NSS.
	e. [Assignment: organization-defined personnel or roles]	e. Not appropriate to define at the CNSS level for all NSS.
RA-5(2)	[Selection (one or more): [Assignment: organization-defined frequency]; prior to a new scan; when new vulnerabilities are identified and reported].	Within 24 hours prior to running scans.
RA-5(5)	[Assignment: organization-identified information system components] [Assignment: organization-defined vulnerability scanning activities]	Authorized vulnerability scanning components. Authorization by the CISO/SISO or designate.
SA-1	a. [Assignment: organization-defined personnel or roles]	a. All personnel.
	b. 1. [Assignment: organization-defined	b.1. At least annually if not otherwise defined in

ID	Control Text	Defined Value for NSS
	frequency]	formal organizational policy.
	b.2. [Assignment: organization-defined frequency]	b.2. At least annually if not otherwise defined in formal organizational policy.
SA-9(1)	(b) [Assignment: organization-defined personnel or roles].	(b) Chief Information Officer.
SA-9(2)	[Assignment: organization-defined external information system services]	All external information systems and services.
SA-12	[Assignment: organization-defined security safeguards]	Security safeguards in accordance with CNSSD No. 505, Supply Chain Risk Management.
SC-1	a. [Assignment: organization-defined personnel or roles]	a. All personnel.
	b.1. [Assignment: organization-defined frequency]	b.1. At least annually if not otherwise defined in formal organizational policy.
	b.2. [Assignment: organization-defined frequency]	b.2. At least annually if not otherwise defined in formal organizational policy.
SC-7(4)	(e) [Assignment: organization-defined frequency]	(e) At least every 180 days.
SC-7(8)	[Assignment: organization-defined internal communications traffic] [Assignment: organization-defined external networks]	All internal communications traffic that may be proxied, except traffic specifically exempted by the Authorizing Official or organizational policy. All untrusted networks outside the control of the organization.
SC-7(12)	[Assignment: organization-defined host-based boundary protection mechanisms] [Assignment: organization-defined information system components]	Not appropriate to define at the CNSS level for all NSS. All system components capable of supporting host-based boundary protection mechanisms such as but not limited to servers, workstations, and those subject to operation outside of the organizational boundary(i.e., laptops and other mobile devices).
SC-7(14)	[Assignment: organization-defined managed interfaces]	Any managed interface that crosses security domains or connects to an external network; such as but not limited to: cross domain solutions (SABI, TSABI), a network boundary with a WAN, a partner network, or the Internet.
SC-7(19)	[Assignment: organization-defined communication clients]	All.
SC-8(1)	[Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] [Assignment: organization-defined alternative physical safeguards].	Prevent unauthorized disclosure of, and detect changes to, information. Alternative physical safeguards such as keeping transmission within physical areas rated IAW the sensitivity of the information or within a Protected Distribution System (PDS) when traversing areas not approved for the sensitivity of the information.

ID	Control Text	Defined Value for NSS
SC-8(2)	[Selection (one or more): confidentiality; integrity]	Confidentiality and integrity.
SC-10	[Assignment: organization-defined time period]	No more than one hour.
SC-11	[Assignment: organization-defined security functions to include at a minimum, information system authentication and re-authentication]	Information system authentication and re-authentication; functions other than the minimum required are not appropriate to define at the CNSS level for all NSS.
SC-12	[Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction]	For unclassified NSS, NIST FIPS-compliant; and/or for classified NSS, see the Classified Information Overlay; processes/requirements for key generation, distribution, storage, access, and destruction.
SC-12(2)	[Selection: NIST FIPS-compliant; NSA-approved]	NIST FIPS-compliant for unclassified data, and/or See Classified Information Overlay for classified data.
SC-15	a. [Assignment: organization-defined exceptions where remote activation is to be allowed]	Dedicated VTC suites located in approved VTC locations that are centrally managed.
SC-15(4)	[Assignment: organization-defined online meetings and teleconferences]	All VTC and all IP based online meetings and conferences (excludes audio only teleconferences using traditional telephony).
SC-17	[Assignment: organization-defined certificate policy]	The certificate policy defined in CNSSP No. 25.
SC-18(2)	[Assignment: organization-defined mobile code requirements]	The following requirements: (a) Emerging mobile code technologies that have not undergone a risk assessment and been assigned to a Risk Category by the CIO 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

ID	Control Text	Defined Value for NSS
		functionality, with no capability for unmediated access to the services and resources of a computing platform) mobile code may be used.
SC-18(3)	[Assignment: organization-defined unacceptable mobile code]	All unacceptable mobile code such as: (a) Emerging mobile code technologies that have not undergone a risk assessment and been assigned to a Risk Category by the CIO. (b) unsigned Category 1 mobile code and Category 1 mobile code technologies that cannot block or disable unsigned mobile code (e.g., Windows Scripting Host). (d) Category 2 mobile code not 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).
SC-18(4)	[Assignment: organization-defined software applications] [Assignment: organization-defined actions]	Software applications and such as but not limited to email, scriptable document/file editing applications that support documents with embedded code (e.g., MS Office applications/documents), etc. Prompting the user for permission.
SC-24	[Assignment: organization-defined known-state] [Assignment: organization-defined types of failures] [Assignment: organization-defined system state information]	Known secure state. All types of failures. Information necessary to determine cause of failure and to return to operations with least disruption to mission/business processes.
SC-28	[Selection (one or more): confidentiality; integrity] Assignment: organization-defined information at rest]	Confidentiality and integrity. All information not cleared for public release.
SC-28(1)	[Assignment: organization-defined information] [Assignment: organization-defined information system components]	All information not cleared for public release. System components outside of organization facilities.
SC-43	a. [Assignment: organization-defined information system components]	All information system components (through the use of an acceptable use agreement).
SI-1	a. [Assignment: organization-defined personnel or roles]	a. All personnel.
	b.1. [Assignment: organization-defined frequency]	b.1. At least annually if not otherwise defined in formal organizational policy.
	b.2. [Assignment: organization-defined	b.2. At least annually if not otherwise defined in

ID	Control Text	Defined Value for NSS
	frequency]	formal organizational policy.
SI-2	c. [Assignment: organization-defined time period]	c. 30 days if not otherwise defined in formal organizational policy.
SI-2(2)	[Assignment: organization-defined frequency]	At least once a quarter.
SI-2(6)	[Assignment: organization-defined software and firmware components]	All upgraded/replaced software and firmware components that are no longer required for operation when possible.
SI-3	c.1. [Assignment: organization-defined frequency] [Selection (one or more); endpoint; network entry/exit points]	c.1. At least weekly. Endpoints and network entry/exit points.
	2. [Selection (one or more): block malicious code; quarantine malicious code; send alert to administrator; [Assignment: organization-defined action]]	c2. Block and quarantine malicious code then send an alert to the system administrator. Not appropriate to define at the CNSS level for all NSS.
SI-3(8)	[Assignment: organization-defined unauthorized operating system commands] [Assignment: organization-defined information system hardware components] [Selection (one or more): issues a warning; audits the command execution; prevents the execution of the command]	Not appropriate to define at the CNSS level for all NSS. Not appropriate to define at the CNSS level for all NSS. Audits the command execution and prevents the execution of the command.
SI-4(4)	[Assignment: organization-defined frequency]	Continuously.
SI-4(9)	[Assignment: organization-defined frequency]	At least monthly.
SI-5	a. [Assignment: organization-defined external organizations]	a. Minimally the US-CERT.
	c. [Selection (one or more): [Assignment: organization-defined personnel or roles] [Assignment: organization-defined elements within the organization] [Assignment: organization-defined external organizations]]	c. Not appropriate to define at the CNSS level for all NSS. Not appropriate to define at the CNSS level for all NSS. Not appropriate to define at the CNSS level for all NSS.
SI-6	a. [Assignment: organization-defined security functions]	a. Not appropriate to define at the CNSS level for all NSS.
	b. [Selection (one or more): [Assignment: organization-defined system transitional states]; upon command by user with appropriate privilege [Assignment: organization-defined frequency]];	b. Not appropriate to define at the CNSS level for all NSS. Not appropriate to define at the CNSS level for all NSS. Not appropriate to define at the CNSS level for

ID	Control Text	Defined Value for NSS
		all NSS.
	c. [Assignment: organization-defined personnel or roles]	c. Minimally notifies system/security administrator.
	d. [Selection (one or more): shuts the information system down; restarts the information system [Assignment: organization-defined alternative action(s)]	d. Not appropriate to define at the CNSS level for all NSS. Not appropriate to define at the CNSS level for all NSS.
SI-6(3)	[Assignment: organization-defined personnel or roles].	Responsible security personnel (e.g., AO, SISO, ISSO, ISSM, etc.).
SI-7(9)	[Assignment: organization-defined devices]	All devices capable of verification of the boot process.
SI-7(13)	[Assignment: organization-defined personnel or roles]	Authorizing Official.
SI-7(15)	[Assignment: organization-defined software or firmware components]	All software and firmware from vendors/sources that provide cryptographic mechanisms to enable the validation of code authenticity and integrity.
SI-10	[Assignment: organization-defined information inputs]	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.
PM-1	b. [Assignment: organization-defined frequency]	b. At least annually if not otherwise defined informal organizational policy.
PM-9	c. [Assignment: organization-defined frequency]	c. At least annually if not otherwise defined informal organizational policy.
NIST SP 800-53 Rev4, Appendix J, Privacy Control Catalog		
AR-1	c. [Assignment: organization-defined allocation of budget and staffing]	c. Not appropriate to define at the CNSS level for all NSS.
	f. [Assignment: organization-defined frequency, at least biennially]	f. At least biennially if not otherwise defined in formal organizational policy.
AR-4	[Assignment: organization-defined frequency]	Continuously.
AR-5	b. [Assignment: organization-defined frequency, at least annually] [Assignment: organization-defined frequency, at least annually]	b. At least annually if not otherwise defined in formal organizational policy. At least annually if not otherwise defined in formal organizational policy.
	c. [Assignment: organization-defined frequency, at least annually]	c. At least annually if not otherwise defined in formal organizational policy.
DI-1	c. [Assignment: organization-defined frequency]	At least every 180 days if not otherwise defined in formal organizational policy.
DI-1(2)	[Assignment: organization-defined frequency]	At least every 180 days if not otherwise defined in formal organizational policy.
DM-1	c. [Assignment: organization-defined frequency, at least annually]	c. At least annually if not otherwise defined in formal organizational policy.
DM-2	a. [Assignment: organization-defined time	a. In accordance with National Archives and

ID	Control Text	Defined Value for NSS
	period]	Records Administration (NARA).
	c. [Assignment: organization-defined techniques or methods]	c. Not appropriate to define at the CNSS level for all NSS.
IP-4(1)	[Assignment: organization-defined time period]	2 business days.
SE-1	a. [Assignment: organization-defined frequency]	a. At least annually if not otherwise defined in formal organizational policy.
	b. [Assignment: organization-defined frequency]	b. At least annually if not otherwise defined in formal organizational policy.