Closed Isolated Network (CIN) Overlays v1.0

1. Identification

This document contains two Closed Isolated Network (CIN) Overlays that identify security control specifications needed to protect against threats and manage security risks in a CIN. A Closed Isolated Network is defined as a data communications enclave that operates in a single security domain, implements a security policy administered by a single authority, does not connect to any other network and has a single, common, continuous security perimeter.

These overlays apply to CINs at one or more geographic locations. A Closed Isolated Network may exist with systems at separate geographic locations in which case the Multiple Overlay will be used. Contrary to NIST 800-53 guidance, these overlays are based on the high watermark principal for Low and Moderate Impact Levels due to their self-contained nature, which inherently reduces the risk, associated with their operation.

This document applies to CINs, once the determination of a CIN has been established. Overlays can reduce or eliminate the need for additional tailoring of the security controls. The security control specifications prescribed by the CIN Overlays may be tailored based on specific characteristics of a particular implementation.

The following documents were used to create these overlays:

- Executive Order 13526, *Classified National Security Information*, 29 December 2009.
- Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, 7 October 2011.
- Committee on National Security Systems Instruction (CNSSI) No. 1253, *Security Categorization and Control Selection for National Security Systems*, 27 March 2014.
- CNSSI No.1253, Appendix F, Attachment 5, *Classified Information Overlay*, 9 May 2014.
- CNSSI No. 4009, *Committee on National Security Systems (CNSS) Glossary*, 6 April 2015.
- CNSSP No. 26, *National Policy on Reducing the Risk of Removable Media for National Security Systems*, May, 2013.
- DoD Instruction 8520.02 *Public Key Infrastructure (PKI) and Public Key (PK) Enabling*, May 24, 2011.
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800- 53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013.[1]
- NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, September 2011.
- US Army NETCOM Stand-Alone Information System and Closed Restricted Network Assessment and Authorization *Operational Tactics, Techniques, and Procedures* v1.0, 27 June 2016.

The CIN Overlays must be used with NIST SP 800-53, Revision 4, as the complete text of the selected security controls and security control enhancements is not fully represented within this document. Also, NIST SP 800-53, Revision 4, provides supplemental guidance for many security controls and security control enhancements that is not replicated within this document.

Sponsoring Organization: US Army Europe G2, Mark Hutcheson (Sponsor) can be reached at mark.d.hutcheson.civ at mail.mil and the author can be reached at michael.l.naya.ctr at mail.mil.

This overlay is intended to be used for CINs until a newer version is available. This overlay will be updated with corrections as needed or if a significant event requires an updated version to be published.

2. Overlay Characteristics

A CIN is comprised of a defined boundary with a set of mechanisms that enforces a defined security policy.

There are two types of CINs:

- **Single** – A data communications network that implements a security policy, is administered by a single authority, does not connect to any other network and is located at a single geographic location.
- **Multiple** – A data communications network that implements a security policy, is administered by a single authority, does not connect to any other network and is located at more than one geographic location.

The applicability of a particular security control depends on the CIN type, because of the differences in technical and operational constraints. The intended use of this overlay is to be applied to systems that do not connect to any other system and serve a unique purpose such as closed-circuit television (CCTV) that require a modern operating system to support the function of the system. Certain CINs are not required to meet certain security controls, such as implementing a public key infrastructure (PKI), per DoD Instruction 8520.02, May 24, 2011.

Assumptions underlying security control selections and justifying the allocation of controls in CIN Overlays include:

- CINs are special-purpose systems designed to support less than 500 users.
- CINs are generally Low and Moderate impact systems as specified in NIST SP 800-53, Revision 4.
- CINs will not have wireless capabilities.
- CINs will not have mobile devices as part of the system.

The following items explain the development and use of CIN Overlays:

- This overlay was developed to be utilized broadly and may be used by federal information systems and national security systems with the approval of authorized

federal officials as part of their official duties. The information system owner in conjunction with the authorizing official must identify and document which overlays apply.

- CIN overlays include security controls and control enhancements that are always selected, or never selected, due to their self-contained nature.
- Information system owners in conjunction with the Authorizing Official may provide justification to select or not select security controls and enhancements based on CIN-specific needs separate from this overlay.

The security controls identified in CIN overlays constitute the initial set of security controls applicable to the CIN. Any other applicable overlays (e.g., Classified Information Overlay, Intelligence Overlay, Privacy Overlay) may not be applicable to produce the full set of security controls for the CIN since additional overlays do not take into account the closed and isolated nature of the system. The CIN Security Plan documents security control selection. The allocation of common controls and the inheritance of controls is beyond the scope of this document.

Applicable CIN parameter values are defined within CIN overlays to the extent possible. Parameter values defined in other documents (e.g., CNSSI No. 1253, DoD Specific Assignment Value [DSPAV], other overlays) were reviewed to determine their applicability to CINs. In some cases, these values were used as is and are included for completeness. In other cases, these values were modified or new values specific to CINs were defined. The parameter values in the CIN Overlays generally take precedence over values defined in other documents. The CIN Authorizing Official (AO) must resolve any conflicts in parameter values. The implementing organization must ensure all parameter values are defined appropriately for all security controls and control enhancements applicable to the CIN.

3. Applicability

Use the following questions to determine the applicability of the CIN Overlays:

1. Will the system consist of a single enclave, implement a security policy administered by a single authority, not connect to any other network and have a single, common, continuous security perimeter at a single geographic location? If the answer is yes, then follow the guidance in this overlay for Single CINs.
2. Will the system consist of a single enclave, implement a security policy administered by a single authority, not connect to any other network and have a single, common, continuous security perimeter at multiple geographic locations? If the answer is yes, then follow the guidance in this overlay for Multiple CINs.

If the answer to both questions 1 and 2 is no, this overlay document does not apply.

4. Overlay Summary

The table below contains a summary of the security control specifications as they apply in the CIN overlays. The symbols used in the table are as follows:

- The letter “B” indicates the control is a CNSSI No. 1253 high watermark baseline control.
- Two dashes (“--”) indicates the control should not be selected.
- The letter “G” indicates there is supplemental guidance, including specific tailoring guidance if applicable, for the control.
- The letter “V” indicates the overlay defines a value for an organizational-defined parameter for the control.
- The letter “R” indicates there is at least one regulatory/statutory reference that requires the control selection or that the control helps to meet regulatory/statutory requirements.

Some security controls or enhancements do not warrant selection or exclusion for all CINs, but may require further consideration if CINs employ these controls to ensure security considerations related to that control or enhancement are adequately addressed. These security controls and enhancements relevant to, but not applicable to all CIN, are discussed in Section 5, “Tailoring Considerations,” and are not included in Table 1 below. Examples included in Section 5 address security controls or enhancements such as:

- AC-18, Wireless Access. If a CIN implements wireless access, then AC-18 and its enhancements must be tailored into the security control set for the CIN.
- CA-3, System Interconnections. If a CIN utilizes another organizations’ transport equipment, such as routers or switches, its enhancements must be tailored into the security control set for the CIN.

Table 1: Closed Isolated Networks (CIN)
Overlays Security Controls

Categorization	Low		Moderate	
CONTROL	Single	Multiple	Single	Multiple
AC-1	BGV	BGV	BGV	BGV
AC-2	BV	BV	BV	BV
AC-2(1)	B	B	B	B
AC-2(2)	BGV	BGV	BGV	BGV
AC-2(3)	BV	BV	BV	BV
AC-2(4)	B	B	B	B
AC-2(5)	B	B	B	B
AC-2(7)	B	B	B	B
AC-2(9)	B	B	B	B
AC-2(10)	B	B	B	B
AC-2(12)	B	B	B	B
AC-2(13)	BV	BV	BV	BV
AC-3	B	B	B	B
AC-3(4)	B	B	B	B
AC-4	--	B	B	B
AC-5	B	B	B	B
AC-6	B	B	B	B
AC-6(1)	B	B	B	B
AC-6(2)	B	B	B	B
AC-6(5)	B	B	B	B
AC-6(7)	BV	BV	BV	BV
AC-6(8)	B	B	B	B
AC-6(9)	B	B	B	B
AC-6(10)	B	B	B	B
AC-7	B	B	B	B
AC-8	B	B	B	B
AC-10	--	--	B	B
AC-11	BV	BV	BV	BV
AC-11(1)	B	B	B	B
AC-12	--	--	B	B
AC-12(1)	--	--	B	B
AC-14	B	B	B	B
AC-16	--	--	B	B
AC-16(6)	--	--	--	--
AC-17	--	--	--	--
AC-17(1)	--	--	--	--

Categorization	Low		Moderate	
CONTROL	Single	Multiple	Single	Multiple
AC-17(2)	--	--	--	--
AC-17(3)	--	--	--	--
AC-17(4)	--	--	--	--
AC-17(6)	--	--	--	--
AC-17(9)	--	--	--	--
AC-18	--	--	--	--
AC-18(1)	--	--	--	--
AC-18(3)	BG	BG	BG	BG
AC-18(4)	--	--	--	--
AC-19	--	--	--	--
AC-19(5)	--	--	--	--
AC-20	--	--	--	--
AC-20(1)	--	--	--	--
AC-20(2)	--	--	--	--
AC-20(3)	--	--	--	--
AC-21	--	--	--	--
AC-22	--	--	--	--
AC-23	--	--	--	--
AT-1	BV	BV	BV	BV
AT-2	BV	BV	BV	BV
AT-2(2)	B	B	B	B
AT-3	BV	BV	BV	BV
AT-3(2)	BV	BV	BV	BV
AT-3(4)	--	--	--	--
AT-4	BV	BV	BV	BV
AU-1	BV	BV	BV	BV
AU-2	BV	BV	BV	BV
AU-2(3)	BV	BV	BV	BV
AU-3	B	B	B	B
AU-3(1)	BV	BV	BV	BV
AU-4	BGV	BGV	BGV	BGV
AU-4(1)	BV	BV	BV	BV
AU-5	BV	BV	BV	BV
AU-5(1)	BV	BV	BV	BV
AU-6	BV	BV	BV	BV
AU-6(1)	BG	BG	BG	BG
AU-6(3)	BG	BG	BG	BG
AU-6(4)	BG	BG	BG	BG
AU-6(10)	B	B	B	B
AU-7	--	--	--	--

Categorization	Low		Moderate	
CONTROL	Single	Multiple	Single	Multiple
AU-7(1)	--	--	--	--
AU-8	BV	BV	BV	BV
AU-8(1)	BGV	BGV	BGV	BGV
AU-9	B	B	B	B
AU-9(4)	B	B	B	B
AU-10	--	--	--	--
AU-11	BGV	BGV	BGV	BGV
AU-11(1)	BV	BV	BV	BV
AU-12	BGVR	BGVR	BGVR	BGVR
AU-12(1)	BV	BV	BV	BV
AU-12(3)	BG	BG	BG	BG
AU-14	B	B	B	B
AU-14(1)	B	B	B	B
AU-14(2)	B	B	B	B
AU-14(3)	--	--	--	--
CA-1	BV	BV	BV	BV
CA-2	BV	BV	BV	BV
CA-2(1)	BV	BV	BV	BV
CA-3	--	--	--	--
CA-3(1)	--	--	--	--
CA-3(5)	BV	BV	BV	BV
CA-5	BV	BV	BV	BV
CA-6	BV	BV	BV	BV
CA-7	BG	BG	BG	BG
CA-7(1)	--	--	--	--
CA-9	BGV	BGV	BGV	BGV
CM-1	BV	BV	BV	BV
CM-2	B	B	B	B
CM-2(1)	BV	BV	BV	BV
CM-2(3)	--	--	--	--
CM-2(7)	--	--	--	--
CM-3	B	B	B	B
CM-3(2)	--	--	B	B
CM-3(4)	BGV	BGV	BGV	BGV
CM-3(6)	BV	BV	BV	BV
CM-4	B	B	B	B
CM-4(1)	--	--	--	--
CM-5	B	B	B	B
CM-5(1)	--	--	B	B
CM-5(2)	--	--	B	B

Categorization	Low		Moderate	
CONTROL	Single	Multiple	Single	Multiple
CM-5(5)	BGVR	BGVR	BGVR	BGVR
CM-5(6)	B	B	B	B
CM-6	BGV	BGV	BGV	BGV
CM-6(1)	--	--	--	--
CM-7	BGV	BGV	BGV	BGV
CM-7(1)	BV	BV	BV	BV
CM-7(2)	--	BGV	BGV	BGV
CM-7(3)	BV	BV	BV	BV
CM-7(5)	BV	BV	BV	BV
CM-8	BV	BV	BV	BV
CM-8(1)	--	--	B	B
CM-8(2)	--	--	--	--
CM-8(3)	--	--	--	--
CM-8(5)	--	--	B	B
CM-9	B	B	B	B
CM-10	B	B	B	B
CM-10(1)	BV	BV	BV	BV
CM-11	BV	BV	BV	BV
CM-11(2)	B	B	B	B
CP-1	BGV	BGV	BGV	BGV
CP-2	BV	BV	BV	BV
CP-2(1)	--	--	B	B
CP-2(3)	--	--	BV	BV
CP-2(8)	--	--	B	B
CP-3	BV	BV	BV	BV
CP-4	BV	BV	BV	BV
CP-4(1)	--	--	B	B
CP-6	--	--	B	B
CP-6(1)	--	--	--	--
CP-6(3)	--	--	--	--
CP-7	BV	BV	BV	BV
CP-7(1)	--	--	--	--
CP-7(2)	--	--	--	--
CP-7(3)	--	--	--	--
CP-8	BV	BV	BV	BV
CP-8(1)	--	--	--	--
CP-8(2)	--	--	--	--
CP-9	BGV	BGV	BGV	BGV
CP-9(1)	--	--	BV	BV
CP-9(5)	--	--	BV	BV

Categorization	Low		Moderate	
CONTROL	Single	Multiple	Single	Multiple
CP-10	B	B	B	B
CP-10(2)	--	--	--	--
IA-1	BGV	BGV	BGV	BGV
IA-2	B	B	B	B
IA-2(1)	BGR	BGR	BGR	BGR
IA-2(2)	BGR	BGR	BGR	BGR
IA-2(3)	BG	BG	BG	BG
IA-2(4)	BG	BG	BG	BG
IA-2(5)	BG	BG	BG	BG
IA-2(8)	--	--	--	--
IA-2(9)	--	--	--	--
IA-2(11)	--	--	--	--
IA-2(12)	--	--	--	--
IA-3	BV	BV	BV	BV
IA-3(1)	--	--	BV	BV
IA-4	BV	BV	BV	BV
IA-4(4)	BV	BV	BV	BV
IA-5	BV	BV	BV	BV
IA-5(1)	BV	BV	BV	BV
IA-5(2)	--	--	--	--
IA-5(3)	--	--	--	--
IA-5(4)	BV	BV	BV	BV
IA-5(7)	B	B	B	B
IA-5(8)	BV	BV	BV	BV
IA-5(11)	--	--	--	--
IA-5(13)	--	--	--	--
IA-5(14)	--	--	--	--
IA-6	B	B	B	B
IA-7	B	B	B	B
IA-8	--	--	--	--
IA-8(1)	--	--	--	--
IA-8(2)	--	--	--	--
IA-8(3)	--	--	--	--
IA-8(4)	--	--	--	--
IR-1	BGV	BGV	BGV	BGV
IR-2	BV	BV	BV	BV
IR-3	BV	BV	BV	BV
IR-3(2)	BG	BG	BG	BG
IR-4	B	B	B	B
IR-4(1)	--	--	--	--

Categorization	Low		Moderate	
CONTROL	Single	Multiple	Single	Multiple
IR-4(3)	BV	BV	BV	BV
IR-4(4)	B	B	B	B
IR-4(6)	B	B	B	B
IR-4(7)	B	B	B	B
IR-4(8)	BV	BV	BV	BV
IR-5	B	B	B	B
IR-6	BV	BV	BV	BV
IR-6(1)	--	--	--	--
IR-6(2)	BV	BV	BV	BV
IR-7	B	B	B	B
IR-7(1)	--	--	--	--
IR-7(2)	--	--	--	--
IR-8	BV	BV	BV	BV
IR-9	BV	BV	BV	BV
IR-9(1)	BV	BV	BV	BV
IR-9(2)	BV	BV	BV	BV
IR-9(3)	BV	BV	BV	BV
IR-9(4)	B	B	B	B
IR-10	--	--	--	--
MA-1	BGV	BGV	BGV	BGV
MA-2	BV	BV	BV	BV
MA-3	B	B	B	B
MA-3(1)	--	--	B	B
MA-3(2)	--	--	B	B
MA-3(3)	BV	BV	BV	BV
MA-4	--	--	--	--
MA-4(1)	--	--	--	--
MA-4(2)	--	--	--	--
MA-4(3)	--	--	--	--
MA-4(6)	--	--	--	--
MA-4(7)	--	--	--	--
MA-5	B	B	B	B
MA-6	BV	BV	BV	BV
MP-1	BGV	BGV	BGV	BGV
MP-2	BVR	BVR	BVR	BVR
MP-3	BV	BV	BV	BV
MP-4	BV	BV	BV	BV
MP-5	BV	BV	BV	BV
MP-5(4)	--	--	B	B
MP-6	BV	BV	BV	BV

Categorization	Low		Moderate	
CONTROL	Single	Multiple	Single	Multiple
MP-7	BV	BV	BV	BV
MP-7(1)	B	B	B	B
PE-1	BGV	BGV	BGV	BGV
PE-2	BV	BV	BV	BV
PE-3	BV	BV	BV	BV
PE-3(1)	BV	BV	BV	BV
PE-4	BV	BV	BV	BV
PE-5	B	B	B	B
PE-6	BV	BV	BV	BV
PE-6(1)	--	B	B	B
PE-8	BV	BV	BV	BV
PE-9	B	B	B	B
PE-10	--	BV	BV	BV
PE-11	--	BV	BV	BV
PE-12	B	B	B	B
PE-13	B	B	B	B
PE-13(3)	--	B	B	B
PE-14	--	BV	BV	BV
PE-15	B	B	B	B
PE-16	BV	BV	BV	BV
PE-17	B	B	--	--
PL-1	BV	BV	BV	BV
PL-2	BV	BV	BV	BV
PL-2(3)	BV	BV	BV	BV
PL-4	BV	BV	BV	BV
PL-4(1)	--	--	--	--
PL-8	BV	BV	BV	BV
PL-8(1)	B	B	B	B
PL-8(2)	--	B	B	B
PM-1	BV	BV	BV	BV
PM-2	B	B	B	B
PM-3	B	B	B	B
PM-4	B	B	B	B
PM-5	B	B	B	B
PM-6	B	B	B	B
PM-7	B	B	B	B
PM-8	B	B	B	B
PM-9	BV	BV	BV	BV
PM-10	B	B	B	B
PM-11	B	B	B	B

Categorization	Low		Moderate	
CONTROL	Single	Multiple	Single	Multiple
PM-12	B	B	B	B
PM-13	B	B	B	B
PM-14	B	B	B	B
PM-15	B	B	B	B
PM-16	B	B	B	B
PS-1	BGV	BGV	BGV	BGV
PS-2	BV	BV	BV	BV
PS-3	B	B	B	B
PS-4	BV	BV	BV	BV
PS-4(1)	B	B	B	B
PS-5	BV	BV	BV	BV
PS-6	BV	BV	BV	BV
PS-6(3)	B	B	B	B
PS-7	BV	BV	BV	BV
PS-8	BV	BV	BV	BV
RA-1	BV	BV	BV	BV
RA-2	B	B	B	B
RA-3	BV	BV	BV	BV
RA-5	BGV	BGV	BGV	BGV
RA-5(1)	B	B	B	B
RA-5(2)	BV	BV	BV	BV
RA-5(4)	--	--	--	--
RA-5(5)	BV	BV	BV	BV
SA-1	BV	BV	BV	BV
SA-2	B	B	B	B
SA-3	B	B	B	B
SA-4	B	B	B	B
SA-4(1)	B	B	B	B
SA-4(2)	--	BV	BV	BV
SA-4(7)	--	--	--	--
SA-4(9)	--	--	--	--
SA-4(10)	--	--	--	--
SA-5	BV	BV	BV	BV
SA-8	B	B	B	B
SA-9	--	--	--	--
SA-9(1)	--	--	--	--
SA-9(2)	--	--	--	--
SA-10	BV	BV	BV	BV
SA-10(1)	B	B	B	B
SA-11	BV	BV	BV	BV

Categorization	Low		Moderate	
CONTROL	Single	Multiple	Single	Multiple
SA-12	BGV	BGV	BGV	BGV
SA-15	--	BV	BV	BV
SA-15(9)	BG	BG	BG	BG
SA-19	BV	BV	BV	BV
SC-1	BV	BV	BV	BV
SC-2	--	--	--	--
SC-4	--	--	--	--
SC-5	--	--	--	--
SC-5(1)	--	--	--	--
SC-5(2)	--	--	--	--
SC-5(3)	--	--	--	--
SC-7	BG	BG	BG	BG
SC-7(3)	--	--	--	--
SC-7(4)	BGV	BGV	BGV	BGV
SC-7(5)	B	B	B	B
SC-7(7)	--	--	--	--
SC-7(8)	--	--	--	--
SC-7(9)	--	--	--	--
SC-7(10)	--	--	--	--
SC-7(11)	BGV	BGV	BGV	BGV
SC-7(12)	BV	BV	BV	BV
SC-7(13)	--	--	--	--
SC-7(14)	BV	BV	BV	BV
SC-8	BV	BV	BV	BV
SC-8(1)	BGV	BGV	BGV	BGV
SC-8(2)	--	--	--	--
SC-10	BGV	BGV	BGV	BGV
SC-12	--	--	--	--
SC-13	BV	BV	BV	BV
SC-15	--	--	--	--
SC-17	--	--	--	--
SC-18	--	--	--	--
SC-18(1)	--	--	--	--
SC-18(2)	--	--	--	--
SC-18(3)	--	--	--	--
SC-18(4)	--	--	--	--
SC-19	--	--	--	--
SC-20	--	--	--	--
SC-21	--	--	--	--
SC-22	--	--	--	--
SC-23	--	--	--	--

Categorization	Low		Moderate	
CONTROL	Single	Multiple	Single	Multiple
SC-23(1)	--	--	--	--
SC-23(3)	--	--	--	--
SC-23(5)	--	--	--	--
SC-24	BV	BV	BV	BV
SC-28	BV	BV	BV	BV
SC-28(1)	BV	BV	BV	BV
SC-38	BG	BG	BG	BG
SC-39	--	--	--	--
SI-1	BV	BV	BV	BV
SI-2	BGV	BGV	BGV	BGV
SI-2(1)	--	--	--	--
SI-2(2)	--	--	--	--
SI-2(3)	--	--	--	--
SI-2(6)	BV	BV	BV	BV
SI-3	BV	BV	BV	BV
SI-3(1)	--	--	--	--
SI-3(2)	--	--	--	--
SI-3(10)	--	--	--	--
SI-4	--	--	--	--
SI-4(1)	--	--	--	--
SI-4(2)	--	--	--	--
SI-4(4)	--	--	--	--
SI-4(5)	--	--	--	--
SI-4(10)	--	--	--	--
SI-4(11)	--	--	--	--
SI-4(12)	--	--	--	--
SI-4(14)	--	--	--	--
SI-4(15)	--	--	--	--
SI-4(16)	--	--	--	--
SI-4(19)	--	--	--	--
SI-4(20)	--	--	--	--
SI-4(22)	--	--	--	--
SI-4(23)	BV	BV	BV	BV
SI-5	BV	BV	BV	BV
SI-7	BV	BV	BV	BV
SI-7(1)	--	--	--	--
SI-7(7)	--	--	--	--
SI-7(8)	--	--	--	--
SI-7(14)	--	--	--	--
SI-8	--	--	--	--

Categorization	Low		Moderate	
CONTROL	Single	Multiple	Single	Multiple
SI-8(1)	--	--	--	--
SI-8(2)	--	--	--	--
SI-10	--	BV	BV	BV
SI-10(3)	--	--	--	--
SI-11	BV	BV	BV	BV
SI-12	B	B	B	B
SI-16	B	B	B	B

4. Detailed Overlay Control Specifications

This section provides justification to select or not select, CIN-specific supplemental guidance, parameter values, and regulatory/statutory references for the security controls and enhancements where these symbols apply as indicated in Table 1. The supplemental guidance provided in this section elaborates on the supplemental guidance in NIST SP 800-53. Security controls and enhancements designated only as “B,” “H,” or “BH” in Table 1 are not further addressed in this section.

Per NIST SP 800-53, security control enhancements are not intended to be selected independently from the base security control (i.e., if a security control enhancement is selected, then the corresponding base security control must also be selected). Organizations must ensure that, during system-specific tailoring, base controls associated with enhancements are tailored as appropriate in the final control set.

AC-1, ACCESS CONTROL POLICY AND PROCEDURES

Supplemental Guidance *for Single and Multiple*: Organizations should have access control policy and procedures that address information specific to CINs.

Parameter Value *for Single and Multiple CINs*: The organization:
a. Develops, documents, and disseminates to *all personnel with CIN responsibilities (including maintenance personnel, administrators, etc.)*:
b. Reviews and updates the current:
b.1. Access control policy *at least annually if not otherwise defined in formal organizational policy;* and
b.2. Access control procedures *at least annually if not otherwise defined in formal organizational policy.*

AC-2, ACCOUNT MANAGEMENT

Parameter Value *for Single and Multiple*: The organization:
j. Reviews accounts for compliance with account management requirements *at least annually.*

AC-2 (2), Account Management | Removal of Temporary / Emergency Accounts

Supplemental Guidance *for Single and Multiple*: Temporary accounts are accounts intended for short-term use. Temporary accounts are established as part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation. Emergency accounts may be used on CINs depending on the nature of the system. Temporary accounts are not to be confused with infrequently used accounts.

Infrequently used accounts (e.g., recovery accounts) are often established for CINs to provide a capability to restore operation in case of catastrophic failure. Account information (to include passwords) must be stored in an approved manner and access limited to authorized personnel only.

Parameter Value *for Single and Multiple*: The information system automatically *disables* temporary and emergency accounts *after 72 hours*.

AC-2(3), Account Management | Disable Inactive Accounts

Parameter Value *for Single and Multiple*: The information system automatically disables inactive accounts after *a period not to exceed 35 calendar days.*

AC-2(13), Account Management | Disable Accounts for High-Risk Individuals

Parameter Value *for Single and Multiple*: The organization disables accounts of users posing a significant risk within *30 minutes* of discovery of the risk.

AC-6(7), Least Privilege | Review of User Privileges

Parameter Value *for Single and Multiple*: The organization:
(a) Reviews *annually, at a minimum,* the privileges assigned to *all CIN roles or classes of users* to validate the need for such privileges;

AC-11, SESSION LOCK

Parameter Value *for Single and Multiple*: The information system:
a. Prevents further access to the system by initiating a session lock after *a period not to exceed 15 minutes* of inactivity or upon receiving a request from a user;

AC-18 (3), WIRELESS ACCESS | DISABLE WIRELESS NETWORKING

Supplemental Guidance *for Single and Multiple*: The pervasiveness of wireless capabilities into systems may prove difficult to find equipment without wireless capabilities. Some equipment may come with embedded wireless and may have to be disabled and/or removed prior to adding it to the information system.

AT-1, SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES

Parameter Value *for Single and Multiple*: The organization:
a. Develops, documents, and disseminates to *appropriate personnel with CIN responsibilities (including maintenance personnel, administrators, etc.)*:
b. Reviews and updates the current:
b.1. Security awareness and training policy *at least annually if not otherwise defined in formal organizational policy;* and
b.2. Security awareness and training procedures *at least annually if not otherwise defined in formal organizational policy.*

AT-2, SECURITY AWARENESS TRAINING

Parameter Value *for Single and Multiple*: The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors):
c. *at least annually if not defined in the Security Plan* thereafter.

AT-3, ROLE-BASED SECURITY TRAINING

Parameter Value *for Single or Multiple*: The organization provides role-based security training to personnel with assigned security roles and responsibilities:
c. *at least annually if not defined in the Security Plan* thereafter.

AT-3(2), Security Training | Physical Security Controls

Parameter Value *for Single or Multiple*: The organization provides *CIN personnel or roles* with initial and *annual* training in the employment and operation of physical security controls.

AT-4, SECURITY TRAINING RECORDS

Supplemental Guidance *for Single and Multiple*: Organizations training specific to CINs. In particular, the some CINs may be a CCTV or a monitoring system that may require special training specific to the CIN.

Parameter Value *for Single or Multiple*: The organization:
b. Retains individual training records for *the period of one year*.

AU-1, AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES

Parameter Value *for Single and Multiple*: The organization:

a. Develops, documents, and disseminates to *all personnel with CIN responsibilities (including maintenance personnel, administrators, etc.)*:
b. Reviews and updates the current:
b.1. Audit policy *at least annually if not otherwise defined in formal organizational policy;* and
b.2. Audit procedures *at least annually if not otherwise defined in formal organizational policy.*

AU-2, AUDIT EVENTS

Parameter Value *for Single and Multiple*: The organization:
a. Determines that the information system is capable of auditing the following events:
1. Authentication events:
(1) Logons (Success/Failure)
(2) Logoffs (Success)
2. File events:
(1) Access (Success/Failure of system configuration files)
(2) Delete (Success/Failure)
(3) Modify (Success/Failure)
(4) Permission Modification (Success/Failure)
(5) Ownership Modification (Success/Failure)
3. Writes/downloads to external devices/media (e.g., 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) 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/interface initialization (e.g., CIN and any associated applications, protocol adapters, Firefox, Internet Explorer, MS Office Suite, etc.) (Success/Failure)
14. CIN processes (e.g., filters, auditing, access control mechanisms, integrity monitor mechanisms, etc.) (Failure)
15. Export of information (e.g., to CDRW, thumb drives, or remote systems) (Success/Failure)
16. Import of information (e.g., from CDRW, thumb drives, or remote systems) (Success/Failure)
17. Information about data processed by the CIN including filters applied (e.g., filename, file size, file type, file metadata, filter actions/results) (Success/Failure)
18. System fault/failure

d. Determines that the following events are to be audited within the information system: *At a minimum, at every occurrence,*

- *Logons (Success/Failure)*
- *Logoffs (Success)*
- *Information about data processed by the CIN including filters applied (e.g., filename, file size, file type, file metadata, filter actions/results) (Success/Failure)*
- *Writes/downloads to external devices/media (Success/Failure)*
- *Use of Privileged/Special Rights events:*
    - *Security or audit policy changes (Success/Failure)*
    - *Configuration changes (Success/Failure)*
    - *Admin or root-level access (Success/Failure)*
    - *Privilege/Role escalation (Success/Failure)*
- *Audit and log data accesses (Success/Failure)*
- *System reboot, restart and shutdown (Success/Failure)*
- *System fault/failure*
- *Export/import of information (Success/Failure) (e.g., to/from CDRW, thumb drives, or remote systems)*

AU-2(3), Audit Events | Reviews and Updates

Parameter Value *for Single and Multiple*: The organization:

a. Reviews and updates audited events *at least annually if not otherwise defined in formal organizational policy.*

AU-3, CONTENT OF AUDIT RECORDS

AU-3(1), Content of Audit Records | Additional Audit Information

Parameter Value *for Single and Multiple*: The information system generates audit records containing the following additional information: *date/time of the audit event, full-text recording of privileged commands and the individual identities of group account users, at a minimum.*

AU-4, AUDIT STORAGE CAPACITY

Supplemental Guidance *for Single or Multiple*: The CIN must be configured to ensure audit storage capacity is not exceeded under normal operation, to avoid a halt in CIN processing or an automatic shutdown of the CIN.

Parameter Value *for Single and Multiple*: The organization:

b. Reviews and analyzes information system audit records *no longer than 60 days for Single and 90 days for multiple* for indications of *inappropriate or unusual activity*; and
c. Reports findings to *the CIN Security Administrator and ISSM, at a minimum.*

AU-4(1), Audit Storage Capacity | Transfer to Alternate Storage

Parameter Value *for Single and Multiple*: The information system off- loads audit records *at a frequency determined to prevent halting the CIN or system due to audit storage reaching maximum capacity* onto a different system or media than the system being audited.

AU-5, RESPONSE TO AUDIT PROCESSING FAILURES

Parameter Value *for Single and Multiple*: The information system:
a. Alerts *the CIN System Administrator and/or Security Administrator, at a minimum,* in the event of an audit processing failure; and
b. Takes the following additional actions: *halts CIN processing, at a minimum.*

AU-5(1), Response to Audit Processing Failures | Audit Storage Capacity

Parameter Value *for Single and Multiple*: The information system provides a warning to *the CIN System Administrator and/or Security Administrator, at a minimum,* within *seconds* when allocated audit record storage volume reaches a*t a maximum 75%* of repository maximum audit record storage capacity.

AU-6, AUDIT REVIEW, ANALYSIS, AND REPORTING

Parameter Value *for Single and Multiple*: The organization:
a. Reviews and analyzes information system audit records *every 90 days for Single and 60 days for Multiple CINs* for indications of *inappropriate or unusual activity*; and
b. Reports findings to *the CIN Security Administrator and ISSM, at a minimum.*

AU-6(1), Audit Review, Analysis, and Reporting | Process Integration

Supplemental Guidance *for Single and Multiple*: The size, scope and impact level of the CIN may not warrant a real-time auditing system for continuous monitoring.

AU-6(3), Audit Review, Analysis, and Reporting | Correlate Audit Repositories

Supplemental Guidance *for Single and Multiple*: The size, scope and impact level of the CIN may not warrant a real-time auditing system for continuous monitoring.

AU-6(4), Audit Review, Analysis, and Reporting | Central Review and Analysis

Supplemental Guidance *for Single and Multiple*: The size, scope and impact level of the CIN may not warrant a real-time auditing system for continuous monitoring.

AU-8, TIME STAMPS

Parameter Value *for Single and Multiple*: The information system:
b. Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets *a granularity of time within one second*.

AU-8(1), Time Stamps | Synchronization with Authoritative Time Source

Supplemental Guidance *for Single and Multiple*: The CIN may not have a GPS antenna for connecting to an authoritative time source and instead may rely on the central server(s) providing services to the CIN.

Parameter Value *for Single and Multiple*: The information system:
(a) Compares the internal information system clocks *at least every 24 hours* with *a central server providing services.*; and
(b) Synchronizes the internal system clocks to the authoritative time source when the time difference is greater than *one second*.

AU-9, PROTECTION OF AUDIT INFORMATION

AU-9(4), Protection of Audit Information | Access by Subset of Privileged Users

Parameter Value *for Single and Multiple*: The organization authorizes access to management of audit functionality to only *a subset of authorized CIN privileged users, whereby users who have the capability to review audit information cannot also manage audit functionality.*

AU-11, AUDIT RECORD RETENTION

Supplemental Guidance *for Single and Multiple*: As of the date of publication, the General Records Schedule 3.2 item 030 specifies retention of audit records for a minimum of 5 years for Sensitive Compartmented Information and a minimum of 1 year for all other information (Unclassified through Collateral Top Secret).

Parameter Value *for Single and Multiple*: The organization retains audit records for *the period of one year unless otherwise specified in the General Records Schedule 3.2 item 030* 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 | Long-Term Retrieval Capability

Parameter Value *for Single and Multiple*: The organization employs *a capability to access audit records for the duration of the required retention period* to ensure that long-term audit records generated by the information system can be retrieved.

AU-12, AUDIT GENERATION

Supplemental Guidance *for Single and Multiple*: EO 13587 requires the establishment of an insider threat program for deterring, detecting, and mitigating insider threats, including the safeguarding of classified information from exploitation, compromise, or other unauthorized disclosure. The White House Memorandum, *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*, requires agencies to monitor and audit user activity on classified and unclassified networks. Generating audit records supports the detection of insider threat activities. The list of audited events for specific components within a CIN is determined as part of the CIN assessment process. The list of audited events should not be modified following CIN authorization without approval of the AO.

Parameter Value *for Single and Multiple*: The information system:
a. Provides audit record generation capability for the auditable events defined in AU-2 a. at *all CIN components*;
b. Allows *only the Audit Administrator* to select which auditable events are to be audited by specific components of the information system;

c. Regulatory/Statutory Reference(s) *for Single and Multiple*: EO 13578, Sec 2.1(b) and Sec 5.2; White House Memorandum, National Insider Threat Policy, Tab 1, Sec B.2(1) and Minimum Standards for Executive Branch Insider Threat Programs, Tab 2, Sec H.1.

AU-12(1), Audit Generation | System-Wide / Time-Correlated Audit Trail

Parameter Value *for Single and Multiple*: The information system compiles audit records from *all CIN components* into a system-wide (logical or physical) audit trail that is time-correlated to within *one second*.

AU-12(3), Audit Generation | Changes by Authorized Individuals

Supplemental Guidance *for Single and Multiple*: Unless specifically allowed and documented in the CIN authorization, no changes to CIN auditing are to be made. If allowed, changes are to be made only by the Audit Administrator.

CA-1, SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES

Parameter Value *for Single and Multiple*: The organization:
a. Develops, documents, and disseminates to *all personnel with CIN responsibilities (including maintenance personnel, administrators, etc.)*:
b. Reviews and updates the current:
b.1. Security assessment and authorization policy *at least annually if not otherwise defined in formal organizational policy;* and
b.2. Security assessment and authorization procedures *at least annually if not otherwise defined in formal organizational policy.*

CA-2, SECURITY ASSESSMENTS

Parameter Value *for Single and Multiple*: The organization:
b. Assesses the security controls in the information system and its environment of operation *as part of initial security authorization and at least annually thereafter, or as stipulated by the AO,* 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;
d. Provides the results of the security control assessment to *the AO, at a minimum*.

CA-2(1), Security Assessments | Independent Assessors

Parameter Value *for Single and Multiple*: The organization employs assessors or assessment teams with *a level of independence as defined by the AO* to conduct security control assessments.

CA-3(5), System Interconnections | Restrictions on External System Connections

Parameter Value *for Single and Multiple*: The organization employs a *deny-all* policy for allowing *any system* to connect to external information systems.

CA-5, PLAN OF ACTION AND MILESTONES

Parameter Value *for Single and Multiple*: The organization:
b. Updates existing plan of action and milestones *at least every 90 days* based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

CA-6, SECURITY AUTHORIZATION

Parameter Value *for Single and Multiple*: The organization:
c. Updates the security authorization *at least every three years (unless the CIN is approved for continuous authorization and implements a continuous monitoring strategy), whenever there is a significant change to the system, or if there is a change to the environment in which the system operates.*

CA-7, CONTINUOUS MONITORING

Supplemental Guidance *for Single and Multiple*: Given the nature, size, impact level and future expansion of the CIN, management may commit to implement a strategy for continuous monitoring of security control effectiveness and any proposed or actual changes to the CIN capability or its operational environment. See NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, for guidance.

CA-9, INTERNAL SYSTEM CONNECTIONS

Supplemental Guidance *for Single and Multiple*: Given the nature of the CIN, internal connections to peripherals such as printers or scanners may be critical components for the system and must be documented as part of the CIN.

Parameter Value *for Single and Multiple*: The organization:
a. Authorizes internal connections of *all connections for all components identified as part of the CIN (including printers, scanners, etc.)*:

CM-1, CONFIGURATION MANAGEMENT POLICY AND PROCEDURES

Parameter Value *for Single and Multiple*: The organization:
b. Develops, documents, and disseminates to *all personnel with CIN responsibilities (including maintenance personnel, administrators, etc.)*:
c. Reviews and updates the current:
c.1. Configuration management policy *at least annually if not otherwise defined in formal organizational policy;* and
c.2. Configuration management procedures *at least annually if not otherwise defined in formal organizational policy.*

CM-2(1), Baseline Configuration | Reviews and Updates

Parameter Value *for Single and Multiple*: The organization reviews and updates the baseline configuration of the information system:
(a) *at least annually*;
(b) When required due to *significant or security relevant changes or security incidents occur;* and
(c) As an integral part of information system component installations and upgrades.

CM-3(4), Configuration Change Control | Security Representative

Supplemental Guidance *for Single and Multiple*: The information security representative to the configuration control board shall be a voting member.

Parameter Value *for Single and Multiple*: The organization requires an information security representative to be a member of the *configuration control board*.

CM-3(6), Configuration Change Control | Cryptography Management

Parameter Value *for Single and Multiple*: The organization ensures that cryptographic mechanisms used to provide *all security safeguards that rely on cryptography* are under configuration management.

CM-5(5), Access Restrictions for Change | Limit Production / Operational Privileges

Supplemental Guidance *for Single and Multiple*: Limiting privileges to change information system components reduces the opportunities for insiders to grant access to information by unauthorized personnel.

Parameter Value *for Single*: The organization:
(b) Reviews and reevaluates privileges *at least every 90 calendar days for Single and 60 calendar days for Multiple*.

Regulatory/Statutory Reference(s) *for Single and Multiple*: EO 13526, Sec 4.1, para. (g).

CM-6, CONFIGURATION SETTINGS

Supplemental Guidance *for Single and Multiple*: Common security configurations developed by organizations for their mainstream IT systems may not generally apply to CINs (such as intrusion detection systems or CCTV). CINs may be uniquely configured and changes to the configuration should only be changed after receiving authorized approval.

Parameter Value *for Single and Multiple*: The organization:
a. Establishes and documents configuration settings for information technology products employed within the information system using *CIN-specific configuration guidance* that reflect the most restrictive mode consistent with operational requirements;
c. Identifies, documents, and approves any deviations from established configuration settings for *all configurable CIN components* based on *operational requirements as approved by the AO*;

CM-7, LEAST FUNCTIONALITY

Supplemental Guidance *for Single and Multiple*: Mechanisms such as a host-based firewall may be used to restrict CIN ports and protocols allowed. Additionally, the CIN may implement an internal monitoring capability to detect unauthorized services that may be running.

Parameter Value *for Single and Multiple*: 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: *as specified in the CIN design documentation*.

CM-7(1), Least Functionality | Periodic Review

Parameter Value *for Single and Multiple*: The organization:
Reviews the information system *at least annually or as system changes or incidents occur* to identify unnecessary and/or nonsecure functions, ports, protocols, and services; and
(a) Disables *all functions, ports, protocols, and services within the CIN deemed to be unnecessary and/or non-secure*.

CM-7(2), Least Functionality | Prevent Program Execution

Supplemental Guidance *for Single and Multiple*: The software programs that comprise the CIN baseline execute in accordance with the CIN policy.

Parameter Value *for Multiple*: The information system prevents program execution in accordance with *the security policy implemented by the CIN regarding software*

program usage and restrictions and rules authorizing the terms and conditions of software program usage.

CM-7(3), Least Functionality | Registration Compliance

Parameter Value *for Single and Multiple*: The organization ensures compliance with *all registration requirements for functions, ports, protocols, and services*.

CM-7(5), Least Functionality | Authorized Software / Whitelisting

Parameter Value *for Single and Multiple*: The organization:
(a) Identifies *all software programs authorized to execute on the CIN*;
(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*.

CM-8, INFORMATION SYSTEM COMPONENT INVENTORY

Parameter Value *for Single and Multiple*: 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 *at a minimum, 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. Reviews and updates the information system component inventory *at least annually*.

CM-10(1), Software Usage Restrictions | Open Source Software

Parameter Value *for Single and Multiple*: The organization establishes the following restrictions on the use of open source software: *The software must approved for use by management and the AO. Use of open source software shall be noted in the CIN design documentation.*

CM-11, USER-INSTALLED SOFTWARE

Parameter Value *for Single and Multiple*: The organization:
a. Establishes *prohibitions* governing the installation of software by users;
b. Enforces software installation policies through *CIN protective features (e.g., MAC, DAC, an integrity monitor)*; and
c. Monitors policy compliance *at least 90 days for Single and 60 days for Multiple CINs*.

CP-1, CONTINGENCY PLANNING POLICY AND PROCEDURES

Supplemental Guidance *for Single and Multiple*: Organizations should have contingency planning policy and procedures that address information specific to CINs. CINs are often implemented to satisfy specific site based needs. Contingency planning should address continued operation of CIN functions, in whole and in part, to address full or partial loss of CIN capabilities.

Parameter Value *for Single and Multiple*: The organization:
a. Develops, documents, and disseminates to *personnel identified in the contingency plan documentation*:
b. Reviews and updates the current:
b.1. Contingency planning policy *at least annually if not otherwise defined in formal organizational policy;* and
b.2. Contingency planning procedures *at least annually if not otherwise defined in formal organizational policy.*

CP-2, CONTINGENCY PLAN

Parameter Value *for Single and Multiple*: The organization:
b. Distributes copies of the contingency plan to *key personnel or roles and organizational elements identified in the contingency plan*;
d. Reviews the contingency plan for the information system *at least annually unless otherwise defined in organizational policy*;
f. Communicates contingency plan changes to *key personnel and organizational elements identified in the contingency plan*;

CP-2(3), Contingency Plan | Resume Essential Missions / Business Functions

Parameter Value *for Single and Multiple*: The organization plans for the resumption of essential missions and business functions within *a time period defined in the contingency plan* of contingency plan activation.

CP-3, CONTINGENCY TRAINING

Parameter Value *for Single and Multiple*: The organization provides contingency training to information system users consistent with assigned roles and responsibilities:
a. Within *30 working days* of assuming a contingency role or responsibility;
c. *At least annually* thereafter.

CP-4, CONTINGENCY PLAN TESTING

Parameter Value *for Single and Multiple*: The organization:
a. Tests the contingency plan for the information system *at least annually* using *tests as defined in the contingency plan* to determine the effectiveness of the plan and the organizational readiness to execute the plan;

CP-7, ALTERNATE PROCESSING SITE

Parameter Value *for Single and Multiple*: The organization:
a. Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of *CIN operations as defined in the contingency plan* for essential missions/business functions within *the time defined in the contingency plan* when the primary processing capabilities are unavailable;

CP-8, TELECOMMUNICATIONS SERVICES

Parameter Value *for Single and Multiple*: The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of *CIN operations as defined in the contingency plan* for essential missions and business functions within *the time defined in the contingency plan* when the primary

telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

CP-9, INFORMATION SYSTEM BACKUP

Supplemental Guidance *for Single and Multiple*: CIN backup media and information shall be protected consistent with the highest classification level of information processed by the CIN.

Parameter Value *for Single and Multiple*: The organization:
a. Conducts backups of user-level information contained in the information system *at as defined in the contingency plan*;
b. Conducts backups of system-level information contained in the information system *as defined in the contingency plan*;
c. Conducts backups of information system documentation including security-related documentation *when created, received, updated, or as defined in the contingency plan*;

CP-9(1), Information System Backup | Testing for Reliability / Integrity

Parameter Value *for Single and Multiple*: The organization tests backup information *as defined in the contingency plan* to verify media reliability and information integrity.

CP-9(5), Information System Backup | Transfer to Alternate Storage Site

Parameter Value *for Single and Multiple*: The organization transfers information system backup information to the alternate storage site *as defined in the contingency plan*.

IA-1, IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES

Supplemental Guidance *for Single and Multiple*: Organizations should have identification and authentication policy and procedures that address information specific to CINs.

Parameter Value *for Single and Multiple*: The organization:
a. Develops, documents, and disseminates to *appropriate personnel with CIN responsibilities (including maintenance personnel, administrators, etc.)*:
b. Reviews and updates the current:
b.1. Identification and authorization policy *at least annually if not otherwise defined in formal organizational policy;* and
b.2. Identification and authorization procedures *at least annually if not otherwise defined in formal organizational policy.*

IA-2(1), Identification and Authentication | Network Access to Privileged Accounts

Supplemental Guidance *for Single and Multiple*: The nature, size, impact level and future expansion of the CIN may be a cost prohibitive security measure to implement multifactor authentication. The justification to implement a multifactor authentication should be specified in the CIN design documentation. If it is infeasible or impractical to implement multifactor authentication, organizations may implement appropriate compensating security controls or explicitly accept the additional risk. CINs are inherently self-contained to control the security risk associated with their use. It is the organization's responsibility to identify which of the regulatory/statutory guidance applies since multifactor authentication may not be required. CNSSD 504 Annex C requires that agencies implement standardized access control methodologies, specifically

multifactor authentication. DoD Instruction 8520.02 section 2b identifies that public key infrastructure is not required for stand-alone networks.

Regulatory/Statutory Reference(s) *for Single and Multiple*: CNSSD 504, Annex A, para. 2.b.i.; DoDI 8520.02 para. 2.b.

IA-2(2), Identification and Authentication | Network Access to Non-Privileged Accounts

Supplemental Guidance *for Single and Multiple*: The nature, size, impact level and future expansion of the CIN may be a cost prohibitive security measure to implement multifactor authentication. The justification to implement a multifactor authentication should be specified in the CIN design documentation. If it is infeasible or impractical to implement multifactor authentication, organizations may implement appropriate compensating security controls or explicitly accept the additional risk. CINs are inherently self-contained to control the security risk associated with their use. CNSSD 504 Annex C requires that agencies implement standardized access control methodologies, specifically multifactor authentication. DoD Instruction 8520.02 section 2b identifies that public key infrastructure is not required for stand-alone networks.

Regulatory/Statutory Reference(s) *for Single and Multiple*: CNSSD 504, Annex A, para. 2.b.i.; DoDI 8520.02 para. 2.b.

IA-2(3), Identification and Authentication | Local Access to Privileged Accounts

Supplemental Guidance *for Single and Multiple*: The nature, size, impact level and future expansion of the CIN may be a cost prohibitive security measure to implement multifactor authentication. The justification to implement a multifactor authentication should be specified in the CIN design documentation. If it is infeasible or impractical to implement multifactor authentication, organizations may implement appropriate compensating security controls or explicitly accept the additional risk. CINs are inherently self-contained to control the security risk associated with their use.

IA-2(4), Identification and Authentication | Local Access to Non-Privileged Accounts

Supplemental Guidance *for Single and Multiple*: The nature, size, impact level and future expansion of the CIN may be a cost prohibitive security measure to implement multifactor authentication. The justification to implement a multifactor authentication should be specified in the CIN design documentation. If it is infeasible or impractical to implement multifactor authentication, organizations may implement appropriate compensating security controls or explicitly accept the additional risk. CINs are inherently self-contained to control the security risk associated with their use.

IA-2(5), Identification and Authentication | Group Authentication

Supplemental Guidance *for Single and Multiple*: The nature, size, impact level and future expansion of the CIN may be a cost prohibitive security measure to implement multifactor authentication. The justification to implement a multifactor authentication should be specified in the CIN design documentation. If group authenticators are utilized, additional authentication features are required to uniquely identify users. If it is infeasible or impractical to implement multifactor authentication, organizations may implement

appropriate compensating security controls or explicitly accept the additional risk. CINs are inherently self-contained to control the security risk associated with their use.

IA-3, DEVICE IDENTIFICATION AND AUTHENTICATION

Parameter Value *for Single and Multiple*: The information system uniquely identifies and authenticates *all devices* before establishing *any internal network* connection.

IA-3(1), Device Identification and Authentication | Cryptographic Bidirectional Authentication

Parameter Value *for Single and Multiple*: The information system authenticates *all interconnected devices* before establishing *any internal network* connection using bidirectional authentication that is cryptographically based.

IA-4, IDENTIFIER MANAGEMENT

Parameter Value *for Single and Multiple*: The organization manages information system identifiers by:
a. Receiving authorization from *the ISSO or ISSM* to assign an individual, group, role, or device identifier;
d. Preventing reuse of identifiers for *at least one year for individuals, groups, roles*; and
e. Disabling the identifier after *90 calendar days of inactivity for Single and 60 days for Multiple if not otherwise defined in formal organizational policy*.

IA-4(4), Identifier Management | Identify User Status

Parameter Value *for Single and Multiple*: The organization manages individual identifiers by uniquely identifying each individual as *contractor or government employee and by nationality*.

IA-5, AUTHENTICATOR MANAGEMENT

Parameter Value *for Single and Multiple*: The organization manages information system authenticators by:
g. Changing/refreshing authenticators *every 90 calendar days for passwords for Single and 60 calendar days for passwords on Multiple CINs*;

IA-5(1), Authenticator Management | Password-Based Authentication

(U) Parameter Value *for Single and Multiple*: The information system, for password-based authentication:

(a) Enforces minimum password complexity of *12 characters minimum, including one of each of the following character sets:*
- *Upper-case*
- *Lower-case*
- *Numeric*
- *Special character (e.g. ~ ! @ # $ % ^ & * ( ) _ + = - ‘ [ ] / ? > <)];*

(b) Enforces at least the following number of changed characters when new passwords are created: *50%*;

(d) Enforces password minimum and maximum lifetime restrictions of *24 hours minimum, 60 calendar days maximum*;

(e) Prohibits password reuse for *a minimum of 10* generations *(does not apply to one time use passwords)*;

IA-5(4), Authenticator Management | Automated Support for Password Strength Determination

Parameter Value *for Single and Multiple*: The organization employs automated tools to determine if password authenticators are sufficiently strong to satisfy *complexity requirements as defined in IA-5(1)*.

IA-5(8), Authenticator Management | Multiple Information System Accounts

Parameter Value *for Single and Multiple*: The organization implements *policies and user training 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 Intelink). More than one privilege level (e.g., user, administrator)...* to manage the risk of compromise due to individuals having accounts on multiple information systems.

IR-1, INCIDENT RESPONSE POLICY AND PROCEDURES

Supplemental Guidance *for Single and Multiple*: Organizations should have incident response policy and procedures that address information specific to CINs. Organizations should report any CIN-related violations to their incident response team.

Parameter Value *for Single and Multiple*: The organization:
a. Develops, documents, and disseminates to *all personnel with CIN responsibilities (including maintenance personnel, administrators, etc.)*:
b. Reviews and updates the current:
1. Incident response policy *at least annually if not otherwise defined in formal organizational policy;* and
2. Incident response procedures *at least annually if not otherwise defined in formal organizational policy.*

IR-2, INCIDENT RESPONSE TRAINING

Parameter Value *for Single and Multiple*: The organization provides incident response training to information system users consistent with assigned roles and responsibilities:
a. Within *90 working days for Single and 60 days for Multiple* of assuming an incident response role or responsibility;
c. *At least annually* thereafter.

IR-3, INCIDENT RESPONSE TESTING

Parameter Value *for Single and Multiple*: The organization tests the incident response capability for the information system *at least annually* using *tests as defined in the incident response plan* to determine the incident response effectiveness and documents the results.

IR-3(2), INCIDENT RESPONSE TESTING | Coordination with Related Plans

Supplemental Guidance *for Single and Multiple*: Some CINs may provide a service to assist in an organization wide incident response plans (e.g., Intrusion Detection System,

alarm systems, CCTV.)

IR-4, INCIDENT HANDLING

IR-4(3), Incident Handling | Continuity of Operations

Parameter Value *for Single and Multiple*: The organization identifies *classes of incidents* and *actions as defined in applicable organization-specific policy* to ensure continuation of organizational missions and business functions.

IR-4(8), Incident Handling | Correlation with External Organizations

Parameter Value *for Single and Multiple*: The organization coordinates with *the appropriate CIRT/CERT (such as US-CERT, DoD CERT, IC CERT)* to correlate and share *security relevant incident information identified in the incident response plan* to achieve a cross- organization perspective on incident awareness and more effective incident responses.

IR-6, INCIDENT REPORTING

Parameter Value *for Single and Multiple*: 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, unless the data owner provides more restrictive guidance*; and
b. Reports security incident information to *the appropriate CIRT/CERT (such as US-CERT, DoD CERT, IC CERT).*

IR-6(2), Incident Reporting | Vulnerabilities Related to Incidents

Parameter Value *for Single and Multiple*: The organization reports information system vulnerabilities associated with reported security incidents to *the AO, ISSM and ISSO*.

IR-8, INCIDENT RESPONSE PLAN

Parameter Value *for Single and Multiple*: The organization:
a. Develops an incident response plan that: Is reviewed and approved by *the CISO/SISO, if not otherwise defined in formal organizational policy*;
b. Distributes copies of the incident response plan to *all personnel with a role or responsibility for implementing the incident response plan*;
c. Reviews the incident response plan *at least annually (incorporating lessons learned from past incidents)*;
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 working days after the change is made*;
f. Protects the incident response plan from unauthorized disclosure and modification.

IR-9, INFORMATION SPILLAGE RESPONSE

Parameter Value *for Single and Multiple*: The organization responds to information spills by:
b. Alerting *at a minimum, the information owner/originator, the ISSM, the activity*

security manager, and the responsible computer incident response center of the information spill using a method of communication not associated with the spill;

IR-9(1), Information Spillage Response | Responsible Personnel

Parameter Value *for Single and Multiple*: The organization assigns *the CIN Security Administrator, at a minimum,* with responsibility for responding to information spills.

IR-9(2), Information Spillage Response | Training

Parameter Value *for Single and Multiple*: The organization provides information spillage response training *annually*.

IR-9(3), Information Spillage Response | Post-Spill Operations

Parameter Value *for Single and Multiple*: The organization implements *a contingency plan in accordance with CP-2* to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions.

MA-1, SYSTEM MAINTENANCE POLICY AND PROCEDURES

Supplemental Guidance *for Single and Multiple*: Organizations should have system maintenance policy and procedures that address information specific to CINs.

Parameter Value *for Single and Multiple*: The organization:
a. Develops, documents, and disseminates to *all personnel with CIN responsibilities (including maintenance personnel, administrators, etc.)*:
b. Reviews and updates the current:
b.1. Maintenance policy *at least annually if not otherwise defined in formal organizational policy;* and
b.2. Maintenance procedures *at least annually if not otherwise defined in formal organizational policy.*

MA-2, CONTROLLED MAINTENANCE

Parameter Value *for Single and Multiple*: The organization:
c. Requires that *at a minimum, the ISSM and ISSO,* explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;
f. Includes *the date/time of the maintenance, name of individual(s) performing the maintenance, name of the escort if necessary, a description of the maintenance performed, and information system components/equipment removed or replaced including serial numbers, if applicable* in organizational maintenance records.

MA-3(3), MAINTENANCE TOOLS | Prevent Unauthorized Removal

Parameter Value *for Single and Multiple*: 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 *at a minimum, the ISSM and the security manager*

explicitly authorizing removal of the equipment from the facility.

MA-6, TIMELY MAINTENANCE

Parameter Value *for Single and Multiple*: The organization obtains maintenance support and/or spare parts for *CIN components* within *24 hours* of failure.

MP-1, MEDIA PROTECTION POLICY AND PROCEDURES

Supplemental Guidance *for Single and Multiple*: Organizations should have media protection policy and procedures that address information specific to CINs.

Parameter Value *for Single and Multiple*: The organization:
a. Develops, documents, and disseminates to *all personnel with CIN responsibilities (including maintenance personnel, administrators, etc.)*:
b. Reviews and updates the current:
b.1. Media protection policy *at least annually if not otherwise defined in formal organizational policy;* and
b.2. Media protection procedures *at least annually if not otherwise defined in formal organizational policy.*

MP-2, MEDIA ACCESS

Parameter Value *for Single and Multiple*: The organization restricts access to *all types of digital and/or non-digital media containing information not cleared for public release* to *personnel without a valid need-to-know*.

Regulatory/Statutory Reference(s) *for Single and Multiple*: EO 13526, Sec 4.1, para. (d); EO 13578, Sec 5.2 and Sec 6.1.

MP-3, MEDIA MARKING

Parameter Value *for Single and Multiple*: The organization:

b. Exempts *no CIN media* (*digital or non-digital)* from marking as long as the media remain within [*Assignment: organization-defined controlled areas*].

MP-4, MEDIA STORAGE

Parameter Value *for Single and Multiple*: The organization:
a. Physically controls and securely stores *all CIN digital and non-digital media containing sensitive, controlled, and/or classified information* within *areas approved for processing or storing data in accordance with the sensitivity, releasability, and/or classification level of the information contained on/within the media*;

MP-5, MEDIA TRANSPORT

Parameter Value *for Single and Multiple*: The organization:
a. Protects and controls *all CIN digital and non-digital media containing sensitive, controlled, and/or classified information* during transport outside of controlled areas using *defined security safeguards, e.g., CNSSP No. 26*;

MP-6, MEDIA SANITIZATION

Parameter Value *for Single and Multiple*: The organization:
a. Sanitizes *all CIN media* prior to disposal, release out of organizational control, or

release for reuse using *approved sanitization techniques and procedures* in accordance with applicable federal and organizational standards and policies;

MP-7, MEDIA USE

Parameter Value *for Single and Multiple*: The organization *restricts* the use of *all types of media* on *CIN system components* using *approved security safeguards as documented in the CIN design documentation*.

PE-1, PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES

Supplemental Guidance *for Single and Multiple*: Organizations should have physical and environmental protection policy and procedures that address information specific to CINs.

Parameter Value *for Single and Multiple*: The organization:
a. Develops, documents, and disseminates to *all personnel with CIN responsibilities (including maintenance personnel, administrators, etc.)*:
b. Reviews and updates the current:
b.1. Physical and environmental protection policy *at least annually if not otherwise defined in formal organizational policy;* and
b.2. Physical and environmental protection procedures *at least annually if not otherwise defined in formal organizational policy.*

PE-2, PHYSICAL ACCESS AUTHORIZATIONS

Parameter Value *for Single and Multiple*: The organization:
c. Reviews the access list detailing authorized facility access by individuals *at least annually if not otherwise defined in PS-1*;

PE-3, PHYSICAL ACCESS CONTROL

Parameter Value *for Single and Multiple*: The organization:
f. Inventories *keys or any other physical token used to gain access* every *year*; and
g. Changes combinations and keys *as required by security relevant events* and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.

PE-3(1), Physical Access Control | Information System Access

Parameter Value *for Single and Multiple*: The organization enforces physical access authorizations to the information system in addition to the physical access controls for the facility at *physical spaces containing one or more components of the CIN, e.g., server rooms.*

PE-4, ACCESS CONTROL FOR TRANSMISSION MEDIUM

Parameter Value *for Single and Multiple*: The organization controls physical access to *CIN distribution and transmission lines* within organizational facilities using [*Assignment: organization-defined security safeguards*].

PE-6, MONITORING PHYSICAL ACCESS

Parameter Value *for Single and Multiple*: The organization:
b. Reviews physical access logs *every 90 calendar days for Single and 60*

calendar days for Multiple CINs and upon occurrence of [*Assignment: organization-defined events or potential indications of events*];

PE-8, VISITOR ACCESS RECORDS

Parameter Value *for Single and Multiple*: The organization:
a. Maintains visitor access records to the facility where the information system resides for *the period of time specified in an agency's records control schedule or General Records Schedule as approved by the National Archives and Records Administration (NARA)*; and
b. Reviews visitor access records *every 90 calendar days for Single and 60 calendar days for Multiple CINs*.

PE-10, EMERGENCY SHUTOFF

Parameter Value *for Single and Multiple CINs*: The organization:
b. Places emergency shutoff switches or devices in *or near more than one egress point of the area housing the CIN, labeled and protected by a cover to prevent accidental shut-off*, to facilitate safe and easy access for personnel;

PE-11, EMERGENCY POWER

Parameter Value *for Single and Multiple*: The organization provides a short-term uninterruptible power supply to facilitate *an orderly shutdown of the CIN, at a minimum, or transition of the CIN to long-term alternate power*, in the event of a primary power source loss.

PE-14, TEMPERATURE AND HUMIDITY CONTROLS

Parameter Value *for Single and Multiple*: The organization:
a. Maintains temperature and humidity levels within the facility where the information system resides at *levels within CIN hardware manufacturer specifications*; and
b. Monitors temperature and humidity levels *continuously, unless CIN hardware manufacturer specifications allow for a wide enough tolerance that monitoring is not required*.

PE-16, DELIVERY AND REMOVAL

Parameter Value *for Single and Multiple*: The organization authorizes, monitors, and controls *all CIN components* entering and exiting the facility and maintains records of those items.

PL-1, SECURITY PLANNING POLICY AND PROCEDURES

Parameter Value *for Single and Multiple*: The organization:
a. Develops, documents, and disseminates to *all personnel with CIN responsibilities (including maintenance personnel, administrators, etc.)*:
b. Reviews and updates the current:
b.1. Security planning policy *at least annually if not otherwise defined in formal organizational policy;* and
b.2. Security planning procedures *at least annually if not otherwise defined in formal organizational policy.*

PL-2, SYSTEM SECURITY PLAN

Parameter Value *for Single and Multiple*: The organization:
b. Distributes copies of the security plan and communicates subsequent changes to the plan to *the CIN ISSO/ISSM, at a minimum*;
c. Reviews the security plan for the information system *at least annually or when required due to system changes or modifications*;

PL-2(3), System Security Plan | Plan / Coordinate with Other Organizational Entities

Parameter Value *for Single and Multiple*: The organization plans and coordinates security-related activities affecting the information system with *all affected parties for system outages and with the AO for security-related configuration changes to the CIN* before conducting such activities in order to reduce the impact on other organizational entities.

PL-4, RULES OF BEHAVIOR

Parameter Value *for Single and Multiple*: The organization:
c. Reviews and updates the rules of behavior *at least annually*;

PL-8, INFORMATION SECURITY ARCHITECTURE

Parameter Value *for Single and Multiple*: The organization:
b. Reviews and updates the information security architecture *at least annually or when changes to the information system or its environment warrant* to reflect updates in the enterprise architecture;

PM-1, INFORMATION SECURITY PROGRAM PLAN

Parameter Value *for Single and Multiple*: The organization:
b. Reviews the organization-wide information security program *at least annually if not otherwise defined in formal organizational policy.*

PM-9, RISK MANAGEMENT STRATEGY

Parameter Value *for Single and Multiple*: The organization:
c. Reviews and updates the risk management strategy *at least annually if not otherwise defined in formal organizational policy.*

PS-1, PERSONNEL SECURITY POLICY AND PROCEDURES

Supplemental Guidance *for Single and Multiple*: Organizations should have personnel security policy and procedures that address information specific to CINs.

Parameter Value *for Single and Multiple*: The organization:
a. Develops, documents, and disseminates to *all personnel with CIN responsibilities (including maintenance personnel, administrators, etc.)*:
b. Reviews and updates the current:
b.1. Personnel security policy *at least annually if not otherwise defined in formal organizational policy;* and
b.2. Personnel security procedures *at least annually if not otherwise defined in formal organizational policy.*

PS-2, POSITION RISK DESIGNATION

Parameter Value *for Single and Multiple*: The organization, upon termination of individual

employment:
c. Reviews and updates position risk designations *at least annually or when the position description is updated or the position is vacated*.

PS-4, PERSONNEL TERMINATION

Parameter Value *for Single and Multiple*: The organization:
a. Disables information system access within *5 working days if termination is voluntary, and within same day if termination is involuntary*;
c. Conducts exit interviews that include a discussion of *proper handling of organizational information*;
f. Notifies *at a minimum, the CIN Security Administrator and personnel responsible for revoking credentials* within *the same day of termination*.

PS-5, PERSONNEL TRANSFER

Parameter Value *for Single and Multiple*: The organization, upon termination of individual employment:
b. Initiates *reassignment actions to ensure all system accesses no longer required are removed or disabled* within *one working day*;
d. Notifies *the CIN Security Administrator and personnel responsible for assigning credentials, at a minimum,* within *one working day*.

PS-6, ACCESS AGREEMENTS

Parameter Value *for Single and Multiple*: The organization:
b. Reviews and updates the access agreements *at least annually*; and
c. Ensures that individuals requiring access to organizational information and information systems:
c.2. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or *when there is a change to the user's level of access*.

PS-7, THIRD-PARTY PERSONNEL SECURITY

Parameter Value *for Single and Multiple*: The organization:
d. Requires third-party providers to notify *the CIN Security Administrator, at a minimum,* of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within *one working day*;

PS-8, PERSONNEL SANCTIONS

Parameter Value *for Single and Multiple*: The organization:
b. Notifies *the CIN Security Administrator, at a minimum,* within *one working day* when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

RA-1, RISK ASSESSMENT POLICY AND PROCEDURES

Parameter Value *for Single and Multiple*: The organization:
a. Develops, documents, and disseminates to *all personnel with CIN responsibilities (including maintenance personnel, administrators, etc.)*:

b. Reviews and updates the current:
b.1. Risk assessment policy *at least annually if not otherwise defined in formal organizational policy;* and
b.2. Risk assessment procedures *at least annually if not otherwise defined in formal organizational policy.*

RA-3, RISK ASSESSMENT

Parameter Value *for Single and Multiple*: The organization:
b. Documents risk assessment results in *a risk assessment report;*
c. Reviews risk assessment results *at least annually*;
d. Disseminates risk assessment results to *the CIN Security Administrator, AO, and PM, at a minimum*;
e. Updates the risk assessment *at least annually* or whenever there are significant 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, VULNERABILITY SCANNING

Supplemental Guidance *for Single and Multiple*: Vulnerability scanning of CINs presents challenges as the very nature of CINs do not allow external connections. Standard vulnerability scanning tools may be used on CIN components and should produce reliable results when used on CINs. Utilizing a standalone laptop scanner to scan the CIN may be an acceptable option with the approval of the security office. Other techniques may be used to identify vulnerabilities in CIN components.

Parameter Value *for Single and Multiple*: The organization:
a. Scans for vulnerabilities in the information system and hosted applications *at least every 120 calendar days or as directed by an authoritative source (e.g.,USCYBERCOM)* and when new vulnerabilities potentially affecting the system/applications are identified and reported;
d. Remediates legitimate vulnerabilities *as specifically authorized for the CIN* in accordance with an organizational assessment of risk;
e. Shares information obtained from the vulnerability scanning process and security control assessments with *the CIN Security Administrator, at a minimum,* to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

RA-5(2), Vulnerability Scanning | Update by Frequency / Prior to New Scan / When Identified

Parameter Value *for Single and Multiple*: The organization updates the information system vulnerabilities scanned *prior to a new scan and when new vulnerabilities are identified and reported*.

RA-5(5), Vulnerability Scanning | Privileged Access

Parameter Value *for Single and Multiple*: The information system implements privileged access authorization to *CIN components* for selected *vulnerability scanning activities*.

SA-1, SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES

Parameter Value *for Single and Multiple*: The organization:
a. Develops, documents, and disseminates to *all personnel with CIN responsibilities (including maintenance personnel, administrators, etc.)*:
b. Reviews and updates the current:
b.1. System and services acquisition policy *at least annually if not otherwise defined in formal organizational policy;* and
b.2. System and services acquisition procedures *at least annually if not otherwise defined in formal organizational policy.*

SA-4, ACQUISITION PROCESS

SA-4(2), Acquisition Process | Design / Implementation Information for Security Controls

Parameter Value *for Single and Multiple*: 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: *all system interfaces, high-level design, and low-level design, at a minimum*.

SA-5, INFORMATION SYSTEM DOCUMENTATION

Parameter Value *for Single and Multiple*: The organization:
e. Distributes documentation to *CIN personnel or roles, as appropriate*.

SA-10, DEVELOPER CONFIGURATION MANAGEMENT

Parameter Value *for Single and Multiple*: The organization requires the developer of the information system, system component, or information system service to:
b. Document, manage, and control the integrity of changes to *all items under configuration management*;
e. Track security flaws and flaw resolution within the system, component, or service and report findings to *the CIN Program Manager and Information Systems Security Engineer (ISSE).*

SA-11, DEVELOPER SECURITY TESTING AND EVALUATION

Parameter Value *for Single and Multiple*: The organization requires the developer of the information system, system component, or information system service to:
b. Perform *unit, integration, system, and regression* testing/evaluation at *a level of depth and coverage to ensure the CIN functions as intended*;

SA-12, SUPPLY CHAIN PROTECTION

Supplemental Guidance *for Single and Multiple*: The CIN developer is responsible for protecting against supply chain threats for all hardware, firmware, and software under their purview. The organization implementing the CIN is responsible for protecting against supply chain threats for all items purchased in support of the CIN.

Parameter Value *for Single and Multiple*: 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 No. 505, Supply Chain Risk Management and applicable organizational regulations such as DoDI 5200.44 (Protection of Mission Critical Functions to Achieve Trusted Systems and Networks) and ICD 731 (Supply Chain Risk Management),* as part of a comprehensive, defense-in-

breadth information security strategy.

SA-15, DEVELOPMENT PROCESS, STANDARDS, AND TOOLS

Parameter Value *for Single and Multiple*: 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;
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 *before first use and annually thereafter* to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy *CIN security requirements*.

SA-15(9), Development Process, Standards, and Tools | Use of Live Data

Supplemental Guidance *for Single and Multiple*: Since CINs are designed to be closed by nature, it is critically important to minimize risk by using test or dummy data during the development and testing of information systems. CINs are inherently self-contained to control the security risk associated with their use.

SA-19, DEVELOPMENT PROCESS, STANDARDS, AND TOOLS

Parameter Value *for Single and Multiple*: The organization:

b. Reports counterfeit information system components to *USCYBERCOM and the CIN Program Manager and ISSE, at a minimum, in accordance with organizational policies and procedures.*

SC-1, SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES

Supplemental Guidance *for Single and Multiple*: Organizations should have system and communications protection policy and procedures that address information specific to CINs. In particular, CINs are required to maintain strict network separation. For example, specific procedures may be required to prevent inadvertent connection of CIN network components.

Parameter Value *for Single and Multiple*: The organization:

a. Develops, documents, and disseminates to *all personnel with CIN responsibilities (including maintenance personnel, administrators, etc.)*:

b. Reviews and updates the current:

b.1. System and communications protection policy *at least annually if not otherwise defined in formal organizational policy;* and

b.2. System and communications protection procedures *at least annually if not otherwise defined in formal organizational policy.*

SC-7, BOUNDARY PROTECTION

Supplemental Guidance *for Single and Multiple*: Items b. and c. of this control do not

apply to CINs, as CINs are not accessible. If a Multiple CIN is utilizing the managed interface(s) of another network, such as gateway(s), router(s), or firewall(s), the CIN connection must be separated, physically or logically, from all traffic and must utilize encryption standards identified in SC-28(1). Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones or DMZs, which may provide sufficient separation requirements. CINs are inherently self-contained to control the security risk associated with their use.

SC-7(4), Boundary Protection | Telecommunications Services

Supplemental Guidance *for Multiple*: Organizations should ensure the isolation of the CIN when traversing untrusted networks. Determination can be based on several factors including, for example, the presence of source/destination address pairs in lists of authorized/allowed communications.
Parameter Value *for Multiple*: The organization:
(e) Reviews exceptions to the traffic flow policy *at least every 180 days* and removes exceptions that are no longer supported by an explicit mission/business need.

SC-7(11), Boundary Protection | Restrict Incoming Communications Traffic

Supplemental Guidance *for Multiple*: Organizations should ensure the isolation of the CIN when traversing untrusted networks. Determination can be based on several factors including, for example, the presence of source/destination address pairs in lists of authorized/allowed communications.

Parameter Value *for Single and Multiple*: The information system only allows incoming communications from *authorized sources, specifically approved and documented in the CIN Security Plan,* routed to *authorized destinations, specifically approved and documented in the CIN Security Plan*.

SC-7(12), Boundary Protection | Host-Based Protection

Parameter Value *for Single and Multiple*: The organization implements *host-based firewalls* at *all CIN interfaces*.

SC-7(14), Boundary Protection | Protects Against Unauthorized Physical Connections

Parameter Value *for Single and Multiple*: The organization protects against unauthorized physical connections at *all CIN interfaces*.

SC-8, TRANSMISSION CONFIDENTIALITY AND INTEGRITY

Supplemental Guidance *for Single and Multiple*: Protecting the confidentiality and/or integrity of organizational information can be accomplished by physical means (e.g., by employing protected distribution systems) or by logical means (e.g., employing encryption techniques). Organizations relying on commercial providers offering transmission services as commodity services rather than as fully dedicated services (i.e., services which can be highly specialized to individual customer needs), may find it difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission confidentiality/integrity. In such situations, organizations determine what types of confidentiality/integrity services are available in standard, commercial telecommunication service packages. If it is infeasible or

impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, organizations implement appropriate compensating security controls or explicitly accept the additional risk.

Parameter Value *for and Multiple*: The information system protects the *confidentiality and integrity* of transmitted information.

SC-8(1), Transmission Confidentiality and Integrity | Cryptographic or Alternate Physical Protection

Supplemental Guidance *for Multiple*: The confidentiality of information is maintained based upon the architecture of the CIN and its employment of MAC and DAC policies.

Parameter Value *for Multiple*: The information system implements cryptographic mechanisms to *maintain separation of information and detect changes to information* during transmission unless otherwise protected by *alternative physical safeguards defined within the CIN design documentation, such as keeping transmission within physical areas or within a Protected Distribution System (PDS).*

SC-10, NETWORK DISCONNECT

Supplemental Guidance *for Single and Multiple*: Unlike out-of-band connection, in-band connection is available only when the server is initialized and functioning properly. In-band connection relies on operating-system network drivers to establish computer connections. Example tools that use an in-band connection are; Secure Shell (SSH), Telnet, Virtual Network Computing (VNC), Microsoft Management Console (MMC), Systems Management Server, Windows Terminal Services, Remote Command Service.

Parameter Value *for Single and Multiple*: The information system terminates the network connection associated with a communications session at the end of the session or after *no more than one hour* of inactivity.

SC-13, USE OF CRYPTOGRAPHY

Parameter Value *for Single and Multiple*: The information system implements *all uses and types of cryptography required for each use (e.g., NSA-approved cryptography for protection of classified information as identified in CNSS Policy No. 15 (Use of Public Standards for the Secure Sharing of Information Among NSS); FIPS- validated cryptography for provision of digital signatures and hashing)* in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

SC-24, FAIL IN KNOWN STATE

Parameter Value *for Multiple*: The information system fails to a *known secure state (e.g., stops data flow processing, shuts down network interfaces)* for *all types of failures* preserving *information pertaining to the CIN system state* in failure.

SC-28, PROTECTION OF INFORMATION AT REST

Parameter Value *for Single and Multiple*: The information system protects the *confidentiality and integrity* of *CIN security relevant information including audits/logs, security configuration files, and all data stored on the CIN while at rest.*

SC-28(1), Protection of Information at Rest | Cryptographic Protection

Parameter Value *for Single and Multiple*: The information system implements cryptographic mechanisms to prevent unauthorized disclosure and modification of *security relevant information including audits/logs, security configuration files, and all data* on *all CIN components*.

SC-38, OPERATIONS SECURITY

Supplemental Guidance *for Single and Multiple*: Operations security (OPSEC) is a systematic process by which potential adversaries can be denied information about the capabilities and intentions of organizations by identifying, controlling, and protecting generally unclassified information that specifically relates to the planning and execution of sensitive organizational activities. The OPSEC process involves five steps: (i) identification of critical information (e.g., the security categorization process); (ii) analysis of threats; (iii) analysis of vulnerabilities; (iv) assessment of risks; and (v) the application of appropriate countermeasures. OPSEC safeguards are applied to both organizational information systems and the environments in which those systems operate. OPSEC safeguards help to protect the confidentiality of key information including, for example, limiting the sharing of information with suppliers and potential suppliers of information system components, information technology products and services, and with other non-organizational elements and individuals. Information critical to mission/business success includes, for example, user identities, element uses, suppliers, supply chain processes, functional and security requirements, system design specifications, testing protocols, and security control implementation details.

Parameter Value *for Single and Multiple*: The organization [Assignment: organization-defined operations security safeguards] to protect key organizational information throughout the system development lifecycle.

SI-1, SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES

Parameter Value *for Single and Multiple*: The organization:
a. Develops, documents, and disseminates to *all personnel with CIN responsibilities (including maintenance personnel, administrators, etc.)*:
b. Reviews and updates the current:
b.1. System and information integrity policy *at least annually if not otherwise defined in formal organizational policy;* and
b.2. System and information integrity procedures *at least annually if not otherwise defined in formal organizational policy.*

SI-2, FLAW REMEDIATION

Supplemental Guidance *for Single and Multiple*: CINs are uniquely configured since they are not connected and their configuration should be changed only if specifically authorized. All software and firmware updates must be tested and approved in accordance with the CIN Configuration Management Plan prior to their installation.

Parameter Value *for Single and Multiple*: The organization:
c. Installs security-relevant software and firmware updates within *90 calendar days for single and 60 calendar days for Multiple CINs of receipt from an authoritative source (e.g., the CIN vendor or program office)* of the release of the updates;

SI-2(6), FLAW REMEDIATION | Removal of Previous Versions of Software / Firmware

Parameter Value *for Single and Multiple*: The organization removes *all upgraded/replaced software and firmware components that are no longer required for operation when possible* after updated versions have been installed.

SI-3, MALICIOUS CODE PROTECTION

Parameter Value *for Single and Multiple*: The organization:
c. Configures malicious code protection mechanisms to:
Perform periodic scans of the information system *at least weekly* and real-time scans of files from sources at *endpoints and routable network devices* as the files are downloaded, opened, or executed in accordance with organizational security policy; and *Block, quarantine, or neutralize malicious code then send an alert to the CIN Security Administrator, at a minimum,* in response to malicious code detection;

SI-4(23), INFORMATION SYSTEM MONITORING | Host-Based Devices

Parameter Value *for Single and Multiple*: The organization implements *an authorized host-based security system* at *all possible components.*

SI-5, SECURITY ALERTS, ADVISORIES, AND DIRECTIVES

Parameter Value *for Single and Multiple*: The organization:

a. Receives information system security alerts, advisories, and directives from *an authorized government source (e.g., US-CERT, USCYBERCOM)* on an ongoing basis;
c. Disseminates security alerts, advisories, and directives to: *the CIN Security Administrator, at a minimum*;

SI-7, SOFTWARE AND INFORMATION INTEGRITY

Parameter Value *for Single and Multiple*: The organization employs integrity verification tools to detect unauthorized changes to *all security-relevant CIN software, configuration files, and firmware (if applicable), as documented in the CIN design documentation.*

SI-10, INFORMATION INPUT VALIDATION

Parameter Value *for Single and Multiple*: The information system checks the validity of *all inputs to all CIN subsystems and applications (e.g., web/application servers, database servers) via syntactic and semantic validation, that might receive a crafted exploit targeted at some weakness in the CIN code such as a buffer overflow or other flaw.*

SI-11, ERROR HANDLING

Parameter Value *for Single and Multiple*: The information system:
b. Reveals error messages only to *CIN users (including maintenance personnel, administrators, etc.), as described in the CIN design documentation*.

5. Tailoring Considerations

Organizations should consider the following specific guidance when tailoring security controls for a CIN, in addition to using the general tailoring guidance in CNSSI No. 1253 and NIST SP 800-53, Chapter 3. During tailoring, care must be taken that security controls are not removed

without a thorough understanding of the system, mission, environment and network, as removal may affect the security posture of the CIN and jeopardize the system authorization. Assurance-related security controls, for example, are particularly relevant to CINs.
Some security controls or enhancements do not warrant selection or exclusion for all CINs, but may require further consideration if CINs employ these controls to ensure security considerations related to that control or enhancement are adequately addressed. For example, AC-18, Wireless Access, is not mandatory for CINs. However, if a CIN implements wireless access, then AC-18 and its enhancements must be tailored into the security control set for the CIN in a way that safeguards access to the CIN. Another example would be CA-3, System Interconnections. If a CIN utilizes another organizations' transport equipment, such as routers or switches, its enhancements must be tailored into the security control set for the CIN thereby insuring the logical separation of traffic and maintaining a single continuous security perimeter.

6. Definitions

The terms used in this document are defined in CNSSI No. 4009, *Committee on National Security Systems (CNSS) Glossary*, or one of the other references listed in Section 1 of this document.