

# Cross Domain Overlay

Unified Cross Domain Management Office  
(UCDMO)

1 December 2011

ver 1.0



# Cross Domain Overlay

## 1. Characteristics and Assumptions

This Cross Domain Solution (CDS) overlay is intended for use by any organization or entity involved in the development, security evaluation, and implementation of a CDS. For the purposes of this overlay, CDS fall into three distinct categories: access, transfer, and multi-level.

Access solutions provide simultaneous visualization of information from multiple security domains via a single workstation. Transfer solutions facilitate the movement of data between interconnected networks or information systems operating in different security domains. Finally, multi-level solutions store data in multiple security domains at varied security levels and allow users to access the data at an appropriate security level.

As this document demonstrates, many controls apply to cross domain solutions. However, how the controls are implemented and validated can vary. Implementation varies because of differences in risk and in both technical and operational constraints. For example, because transfer CDS's are used to move data between differing security domains, they require additional characteristics such as security, robustness, integrity, availability and confidentiality. Additionally, extra attention needs to be paid to auditing, access controls, account management, system integrity, confirmation management, etc. Without this extra attention paid to security controls, information could be compromised or the correct information could be delayed in reaching its destination.

## 2. Applicability

The following questions are used to determine CDS overlay applicability:

1. Will the CDS be connected to 2 or more security domains?
2. Will the CDS be used to transfer data at different security classifications?
3. Will the CDS be used to access data at different security classifications?
4. Will the CDS be used to store data at different security classifications?

If you answer yes to any of the above questions this overlay applies.

## 3. Implementation

The Cross Domain System Overlay is based on:

- NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009 with May 2010 errata updates
- CNSS Instruction No. 1253, July 2011 Revision, *Security Controls and Control Selections for National Security Systems*, Draft July 2011

This Cross Domain Solution Overlay is designed for use with the low confidentiality, low

integrity, and low availability control baseline defined in CNSSI 1253 and NIST SP 800-53, Revision 3. It does not require any additional overlays for use with cross domain solutions. However, it is recommended extreme care be given when tailoring the security controls in this overlay as might be required by differing authorizing officials and security assessment processes. See Section 7 for the list of security controls required to meet regulatory/statutory requirements.

#### 4. Table of Overlay Controls

Legend: A plus sign (“+”) in the overlay column indicates the applicability of the control above the controls identified in CNSSI 1253 and the NIST SP 800-53, Revision 3 baseline. Two dashes (“--”) in the overlay column indicates that the security control is not required and is effectively tailored from the final control set. An asterisk “\*” in the overlay column denotes the value from the *CNSSI 1253CNSS, July 2011 Revision LLL* profile.

**Table 1: Cross Domain Solutions Overlay Security Controls**

ID#	Supplemental Guidance	Transfer			Access			Multilevel		
		C	I	A	C	I	A	C	I	A
AC-1	Yes	*	*	*	*	*	*	*	*	*
AC-2	Yes	*	*		*	*		*	*	
AC-2(1)	Yes	*	*		*	*		*	*	
AC-2(2)	Yes	*	*		*	*		*	*	
AC-2(3)	Yes	*	*		*	*		*	*	
AC-2(4)	Yes	*	*		*	*		*	*	
AC-2(5)	Yes	+	+		+	+		+	+	
AC-2(6)										
AC-2(7)	Yes	*	*		*	*		*	*	
AC-3	Yes	*	*		*	*		*	*	
AC-3(1)										
AC-3(2)	Yes	+	+		+	+		+	+	
AC-3(3)	Yes	+	+		+	+		+	+	
AC-3(4)	Yes	*	*		*	*		*	*	
AC-3(5)	Yes	+	+	+	+	+	+	+	+	+
AC-3(6)	Yes	+	+		+	+		+	+	
AC-3(7)										
AC-4	Yes	*	*		*	*		*	*	
AC-4(1)	Yes	+	+					+	+	
AC-4(2)	Yes	+	+		+	+		+	+	
AC-4(3)	Yes	+	+		+	+		+	+	
AC-4(4)	Yes	+	+					+	+	
AC-4(5)	Yes	+	+					+	+	
AC-4(6)	Yes	+	+					+	+	
AC-4(7)	Yes									
AC-4(8)	Yes	+	+					+	+	
AC-4(9)	Yes									
AC-4(10)	Yes	+	+					+	+	

ID#	Supplemental Guidance	Transfer			Access			Multilevel		
		C	I	A	C	I	A	C	I	A
AC-4(11)	Yes	+	+					+	+	
AC-4(12)	Yes	+	+					+	+	
AC-4(13)	Yes	+	+					+	+	
AC-4(14)	Yes	+	+					+	+	
AC-4(15)	Yes	+	+					+	+	
AC-4(16)	Yes	+	+					+	+	
AC-4(17)	Yes	+	+					+	+	
AC-5	Yes	*	*		*	*		*	*	
AC-6	Yes	*	*		*	*		*	*	
AC-6(1)	Yes	*	*		*	*		*	*	
AC-6(2)	Yes	*	*		*	*		*	*	
AC-6(3)	Yes	*	*		*	*		*	*	
AC-6(4)	Yes	+	+		+	+		+	+	
AC-6(5)	Yes	*	*		*	*		*	*	
AC-6(6)	Yes	*	*		*	*		*	*	
AC-7	Yes	*	*	*	*	*	*	*	*	*
AC-7(1)	Yes	+	+	+	+	+	+	+	+	+
AC-7(2)	Yes	*			*			*		
AC-8	Yes	*	*		*	*		*	*	
AC-9	Yes		+			+			+	
AC-9(1)	Yes		+			+			+	
AC-9(2)	Yes		+			+			+	
AC-9(3)	Yes		+			+			+	
AC-10	Yes		+			+			+	
AC-11	Yes	*	*		*	*		*	*	
AC-11(1)	Yes	*			*			*		
<del>AC-12</del>										
<del>AC-13</del>										
AC-14	Yes	--		--	--		--	--		--
AC-14(1)	Yes									
<del>AC-15</del>										
AC-16	Yes	+	+		+	+		+	+	
AC-16(1)	Yes	+	+					+	+	
AC-16(2)	Yes	+	+					+	+	
AC-16(3)	Yes	+	+		+	+		+	+	
AC-16(4)	Yes	+	+					+	+	
AC-16(5)	Yes	+	+		+	+		+	+	
AC-17	Yes	*	*		*	*		*	*	

ID#	Supplemental Guidance	Transfer			Access			Multilevel		
		C	I	A	C	I	A	C	I	A
AC-17(1)	Yes	*	*		*	*		*	*	
AC-17(2)	Yes	*	*		*	*		*	*	
AC-17(3)	Yes	*	*		*	*		*	*	
AC-17(4)	Yes	*	*		*	*		*	*	
AC-17(5)	Yes	*	*		*	*		*	*	
AC-17(6)	Yes	*			*			*		
AC-17(7)	Yes	*	*		*	*		*	*	
AC-17(8)	Yes	*	*		*	*		*	*	
AC-18	Yes	*	*		*	*		*	*	
AC-18(1)	Yes	*	*		*	*		*	*	
AC-18(2)	Yes	*	*		*	*		*	*	
AC-18(3)	Yes	*	*		*	*		*	*	
AC-18(4)	Yes	*	*		*	*		*	*	
AC-18(5)	Yes	*	*		*	*		*	*	
AC-19	Yes	*	*		*	*		*	*	
AC-19(1)	Yes	*			*			*		
AC-19(2)	Yes	*	*		*	*		*	*	
AC-19(3)	Yes	*	*		*	*		*	*	
AC-19(4)	Yes	*			*			*		
AC-20		*	*		*	*		*	*	
AC-20(1)		*	*		*	*		*	*	
AC-20(2)		*			*			*		
AC-21										
AC-21(1)	Yes									
AC-22		*			*			*		
AT-1		*	*	*	*	*	*	*	*	*
AT-2		*	*	*	*	*	*	*	*	*
AT-2(1)										
AT-3		*	*	*	*	*	*	*	*	*
AT-3(1)										
AT-3(2)		*	*	*	*	*	*	*	*	*
AT-4		*	*	*	*	*	*	*	*	*
AT-5		*	*	*	*	*	*	*	*	*
AU-1	Yes	*	*	*	*	*	*	*	*	*
AU-2	Yes	*	*		*	*		*	*	
AU-2(1)										
AU-2(2)										
AU-2(3)	Yes	*	*		*	*		*	*	

ID#	Supplemental Guidance	Transfer			Access			Multilevel		
		C	I	A	C	I	A	C	I	A
AU-2(4)	Yes	*	*		*	*		*	*	
AU-3	Yes	*	*		*	*		*	*	
AU-3(1)	Yes	*	*		*	*		*	*	
AU-3(2)	Yes	*	*		*	*		*	*	
AU-4	Yes			*			*			*
AU-5	Yes			*			*			*
AU-5(1)	Yes			*			*			*
AU-5(2)	Yes			+			+			+
AU-5(3)	Yes									
AU-5(4)	Yes		+	+		+	+		+	+
AU-6	Yes	*	*		*	*		*	*	
AU-6(1)	Yes	*	*		*	*		*	*	
<del>AU-6(2)</del>										
AU-6(3)		*	*		*	*		*	*	
AU-6(4)	Yes									
AU-6(5)	Yes									
AU-6(6)	Yes									
AU-6(7)	Yes	*	*		*	*		*	*	
<del>AU-6(8)</del>										
AU-6(9)										
AU-7	Yes		+			+			+	
AU-7(1)	Yes		+			+			+	
AU-8	Yes		*			*			*	
AU-8(1)	Yes		*			*			*	
AU-9	Yes	*	*		*	*		*	*	
AU-9(1)	Yes									
AU-9(2)	Yes									
AU-9(3)	Yes		+			+			+	
AU-9(4)	Yes		*			*			*	
AU-10	Yes	+	+		+	+		+	+	
AU-10(1)	Yes	+	+		+	+		+	+	
AU-10(2)	Yes	+	+		+	+		+	+	
AU-10(3)	Yes	+	+		+	+		+	+	
AU-10(4)	Yes	+	+		+	+		+	+	
AU-10(5)	Yes	+	+		+	+		+	+	
AU-11	Yes									
AU-12	Yes	*	*	*	*	*	*	*	*	*
AU-12(1)	Yes		+			+			+	

ID#	Supplemental Guidance	Transfer			Access			Multilevel		
		C	I	A	C	I	A	C	I	A
AU-12(2)	Yes		+			+			+	
AU-13										
AU-14										
AU-14(1)	Yes									
CA-1		*	*	*	*	*	*	*	*	*
CA-2		*	*	*	*	*	*	*	*	*
CA-2(1)		*	*	*	*	*	*	*	*	*
CA-2(2)										
CA-3		*	*		*	*		*	*	
CA-3(1)		*			*			*		
CA-3(2)										
CA-4										
CA-5		*	*	*	*	*	*	*	*	*
CA-5(1)										
CA-6		*	*	*	*	*	*	*	*	*
CA-7		*	*	*	*	*	*	*	*	*
CA-7(1)		*	*	*	*	*	*	*	*	*
CA-7(2)		*	*	*	*	*	*	*	*	*
CM-1	Yes	*	*		*	*		*	*	
CM-2	Yes		*			*			*	
CM-2(1)	Yes		*			*			*	
CM-2(2)										
CM-2(3)	Yes		+			+			+	
CM-2(4)	Yes		--			--			--	
CM-2(5)	Yes		+			+			+	
CM-2(6)			*			*			*	
CM-3	Yes		*			*			*	
CM-3(1)										
CM-3(2)			*			*			*	
CM-3(3)										
CM-3(4)			*			*			*	
CM-4			*			*			*	
CM-4(1)			*			*			*	
CM-4(2)			*	+		*	+		*	+
CM-5	Yes		*			*			*	
CM-5(1)	Yes		*			*			*	
CM-5(2)	Yes		*			*			*	
CM-5(3)	Yes									

ID#	Supplemental Guidance	Transfer			Access			Multilevel		
		C	I	A	C	I	A	C	I	A
CM-5(4)	Yes		+			+			+	
CM-5(5)	Yes		*			*			*	
CM-5(6)	Yes		*			*			*	
CM-5(7)	Yes		+	+		+	+		+	+
CM-6			*			*			*	
CM-6(1)										
CM-6(2)	Yes		+	+		+	+		+	+
CM-6(3)	Yes		*			*			*	
CM-6(4)	Yes		*			*			*	
CM-7	Yes	*	*		*	*		*	*	
CM-7(1)	Yes	*	*		*	*		*	*	
CM-7(2)	Yes									
CM-7(3)	Yes	*	*		*	*		*	*	
CM-8			*			*			*	
CM-8(1)	Yes		*			*			*	
CM-8(2)										
CM-8(3)	Yes									
CM-8(4)			*			*			*	
CM-8(5)			*			*			*	
CM-8(6)			+			+			+	
CM-9	Yes		*			*			*	
CM-9(1)	Yes									
CP-1		*	*	*	*	*	*	*	*	*
CP-2				*			*			*
CP-2(1)										
CP-2(2)										
CP-2(3)										
CP-2(4)										
CP-2(5)										
CP-2(6)										
CP-3				*			*			*
CP-3(1)										
CP-3(2)										
CP-4				*			*			*
CP-4(1)										
CP-4(2)										
CP-4(3)										
CP-4(4)										

ID#	Supplemental Guidance	Transfer			Access			Multilevel		
		C	I	A	C	I	A	C	I	A
CP-5										
CP-6										
CP-6(1)										
CP-6(2)										
CP-6(3)										
CP-7										
CP-7(1)										
CP-7(2)										
CP-7(3)										
CP-7(4)										
CP-7(5)										
CP-8										
CP-8(1)										
CP-8(2)										
CP-8(3)										
CP-8(4)										
CP-9	Yes	*	*	*	*	*	*	*	*	*
CP-9(1)	Yes		*	*		*	*		*	*
CP-9(2)	Yes		+	+		+	+		+	+
CP-9(3)			+			+			+	
<del>CP-9(4)</del>										
CP-9(5)			+			+			+	
CP-9(6)										
CP-10	Yes			*			*			*
<del>CP-10(1)</del>										
CP-10(2)	Yes		*	*		*	*		*	*
CP-10(3)										
CP-10(4)	Yes		+			+			+	
CP-10(5)										
CP-10(6)	Yes		+	*		+	*		+	*
IA-1		*	*		*	*		*	*	
IA-2		*	*		*	*		*	*	
IA-2(1)		*	*		*	*		*	*	
IA-2(2)										
IA-2(3)	Yes									
IA-2(4)	Yes									
IA-2(5)	Yes	*	*		*	*		*	*	
IA-2(6)										

ID#	Supplemental Guidance	Transfer			Access			Multilevel		
		C	I	A	C	I	A	C	I	A
IA-2(7)										
IA-2(8)	Yes	*	*		*	*		*	*	
IA-2(9)	Yes	+	+		+	+		+	+	
IA-3	Yes	*	*		*	*		*	*	
IA-3(1)	Yes	+	+		+	+		+	+	
IA-3(2)	Yes	+	+		+	+		+	+	
IA-3(3)										
IA-4		*	*		*	*		*	*	
IA-4(1)										
IA-4(2)										
IA-4(3)			*			*			*	
IA-4(4)	Yes	*	*		*	*		*	*	
IA-4(5)										
IA-5	Yes	*	*		*	*		*	*	
IA-5(1)	Yes	*	*		*	*		*	*	
IA-5(2)	Yes		*			*			*	
IA-5(3)			*			*			*	
IA-5(4)		*	*		*	*		*	*	
IA-5(5)										
IA-5(6)	Yes	*	*		*	*		*	*	
IA-5(7)	Yes	*			*			*		
IA-5(8)		*	*		*	*		*	*	
IA-6	Yes	*	*		*	*		*	*	
IA-7		*	*		*	*		*	*	
IA-8		*	*		*	*		*	*	
IR-1		*	*	*	*	*	*	*	*	*
IR-2		*	*	*	*	*	*	*	*	*
IR-2(1)		*	*	*	*	*	*	*	*	*
IR-2(2)										
IR-3		*	*	*	*	*	*	*	*	*
IR-3(1)										
IR-4		*	*	*	*	*	*	*	*	*
IR-4(1)		*	*	*	*	*	*	*	*	*
IR-4(2)										
IR-4(3)		*	*	*	*	*	*	*	*	*
IR-4(4)		*	*	*	*	*	*	*	*	*
IR-4(5)										
IR-5		*	*	*	*	*	*	*	*	*

ID#	Supplemental Guidance	Transfer			Access			Multilevel		
		C	I	A	C	I	A	C	I	A
IR-5(1)		*	*	*	*	*	*	*	*	*
IR-6		*	*	*	*	*	*	*	*	*
IR-6(1)		*	*	*	*	*	*	*	*	*
IR-6(2)		*	*	*	*	*	*	*	*	*
IR-7		*	*	*	*	*	*	*	*	*
IR-7(1)		*	*	*	*	*	*	*	*	*
IR-7(2)		*	*	*	*	*	*	*	*	*
IR-8		*	*	*	*	*	*	*	*	*
MA-1		*	*	*	*	*	*	*	*	*
MA-2		*	*	*	*	*	*	*	*	*
MA-2(1)		*	*	*	*	*	*	*	*	*
MA-2(2)										
MA-3			*	*		*	*		*	*
MA-3(1)										
MA-3(2)			*	*		*	*		*	*
MA-3(3)		*			*			*		
MA-3(4)										
MA-4			*			*			*	
MA-4(1)			*			*			*	
MA-4(2)			*			*			*	
MA-4(3)		*	*	*	*	*	*	*	*	*
MA-4(4)		+	+		+	+		+	+	
MA-4(5)			*			*			*	
MA-4(6)		*	*		*	*		*	*	
MA-4(7)			*			*			*	
MA-5		*	*	*	*	*	*	*	*	*
MA-5(1)		*	*	*	*	*	*	*	*	*
MA-5(2)		+	+		+	+		+	+	
MA-5(3)		+	+		+	+		+	+	
MA-5(4)		+	+		+	+		+	+	
MA-6										
MP-1		*	*	*	*	*	*	*	*	*
MP-2		*			*			*		
MP-2(1)										
MP-2(2)										
MP-3		*			*			*		
MP-4		*			*			*		
MP-4(1)										

ID#	Supplemental Guidance	Transfer			Access			Multilevel		
		C	I	A	C	I	A	C	I	A
MP-5		*	*		*	*		*	*	
<del>MP-5(1)</del>										
MP-5(2)		*	*		*	*		*	*	
MP-5(3)										
MP-5(4)										
MP-6		*			*			*		
MP-6(1)										
MP-6(2)		*			*			*		
MP-6(3)		*			*			*		
MP-6(4)		*			*			*		
MP-6(5)		*			*			*		
MP-6(6)		*			*			*		
PE-1		*	*	*	*	*	*	*	*	*
PE-2		*	*	*	*	*	*	*	*	*
PE-2(1)		*	*	*	*	*	*	*	*	*
PE-2(2)										
PE-2(3)		*			*			*		
PE-3		*	*	*	*	*	*	*	*	*
PE-3(1)		*	*		*	*		*	*	
PE-3(2)		*			*			*		
PE-3(3)		*	*		*	*		*	*	
PE-3(4)	Yes									
PE-3(5)	Yes									
PE-3(6)										
PE-4										
PE-5	Yes	*			*			*		
PE-6		*	*	*	*	*	*	*	*	*
PE-6(1)										
PE-6(2)										
PE-7		*	*		*	*		*	*	
PE-7(1)		*	*		*	*		*	*	
PE-7(2)										
PE-8		*	*		*	*		*	*	
PE-8(1)										
PE-8(2)										
PE-9				*			*			*
PE-9(1)										
PE-9(2)										

ID#	Supplemental Guidance	Transfer			Access			Multilevel		
		C	I	A	C	I	A	C	I	A
PE-10				*			*			*
<del>PE-10(1)</del>										
PE-11										
PE-11(1)										
PE-11(2)										
PE-12				*			*			*
PE-12(1)										
PE-13				*			*			*
PE-13(1)				*			*			*
PE-13(2)				*			*			*
PE-13(3)				*			*			*
PE-13(4)				*			*			*
PE-14				*			*			*
PE-14(1)										
PE-14(2)										
PE-15				*			*			*
PE-15(1)										
PE-16		*		*	*		*	*		*
PE-17										
PE-18				*			*			*
PE-19										
PE-19(1)										
PL-1		*	*	*	*	*	*	*	*	*
PL-2		*	*	*	*	*	*	*	*	*
PL-2(1)		*	*	*	*	*	*	*	*	*
PL-2(2)	Yes	*	*	*	*	*	*	*	*	*
<del>PL-3</del>										
PL-4		*	*	*	*	*	*	*	*	*
PL-4(1)		*			*			*		
PL-5		*			*			*		
PL-6		*	*	*	*	*	*	*	*	*
PS-1		*	*	*	*	*	*	*	*	*
PS-2		*	*	*	*	*	*	*	*	*
PS-3		*	*		*	*		*	*	
PS-3(1)		*			*			--		
PS-3(2)		*			*			--		
PS-4		*	*	*	*	*	*	*	*	*
PS-5		*	*	*	*	*	*	*	*	*

ID#	Supplemental Guidance	Transfer			Access			Multilevel		
		C	I	A	C	I	A	C	I	A
PS-6		*	*		*	*		*	*	
PS-6(1)		*	*		*	*		*	*	
PS-6(2)		*			*			*		
PS-7		*	*		*	*		*	*	
PS-8		*	*	*	*	*	*	*	*	*
RA-1		*	*	*	*	*	*	*	*	*
RA-2	Yes	*	*	*	*	*	*	*	*	*
RA-3		*	*	*	*	*	*	*	*	*
RA-4										
RA-5	Yes	*	*	*	*	*	*	*	*	*
RA-5(1)		*	*	*	*	*	*	*	*	*
RA-5(2)		*	*	*	*	*	*	*	*	*
RA-5(3)		*	*	*	*	*	*	*	*	*
RA-5(4)		*	*	*	*	*	*	*	*	*
RA-5(5)		*	*	*	*	*	*	*	*	*
RA-5(6)										
RA-5(7)		*	*	*	*	*	*	*	*	*
RA-5(8)										
RA-5(9)		+	+		+	+		+	+	
SA-1		*	*		*	*		*	*	
SA-2			*			*			*	
SA-3			*			*			*	
SA-4			*			*			*	
SA-4(1)			*			*			*	
SA-4(2)			+			+			+	
SA-4(3)										
SA-4(4)										
SA-4(5)										
SA-4(6)		*	+		*	+		*	+	
SA-4(7)										
SA-5	Yes		*			*			*	
SA-5(1)	Yes		*			*			*	
SA-5(2)	Yes		*			*			*	
SA-5(3)	Yes		*			*			*	
SA-5(4)	Yes		+			+			+	
SA-5(5)	Yes									
SA-6		*	*		*	*		*	*	
SA-6(1)										

ID#	Supplemental Guidance	Transfer			Access			Multilevel		
		C	I	A	C	I	A	C	I	A
SA-7			*			*			*	
SA-8			*			*			*	
SA-9			*			*			*	
SA-9(1)			*			*			*	
SA-10	Yes		*			*			*	
SA-10(1)	Yes		*			*			*	
SA-10(2)										
SA-11	Yes		*			*			*	
SA-11(1)			+			+			+	
SA-11(2)			+			+			+	
SA-11(3)	Yes		+			+			+	
SA-12			*			*			*	
SA-12(1)										
SA-12(2)			*			*			*	
SA-12(3)										
SA-12(4)										
SA-12(5)										
SA-12(6)										
SA-12(7)										
SA-13			+			+			+	
SA-14										
SA-14(1)										
SC-1		*	*	*	*	*	*	*	*	*
SC-2		*	*		*	*		*	*	
SC-2(1)		*	*		*	*		*	*	
SC-3		+	+		+	+		+	+	
SC-3(1)										
SC-3(2)		+	+		+	+		+	+	
SC-3(3)		+	+		+	+		+	+	
SC-3(4)										
SC-3(5)										
SC-4		*	+		*	+		*	+	
SC-4(1)		+	+		+	+		+	+	
SC-5				*			*			*
SC-5(1)	Yes			*			*			*
SC-5(2)	Yes									
SC-6				+						+
SC-7		*	*		*	*		*	*	

ID#	Supplemental Guidance	Transfer			Access			Multilevel		
		C	I	A	C	I	A	C	I	A
SC-7(1)		*	*		*	*		*	*	
SC-7(2)		*	*		*	*		*	*	
SC-7(3)		*	*		*	*		*	*	
SC-7(4)		*	*		*	*		*	*	
SC-7(5)		*	*		*	*		*	*	
SC-7(6)		*			*			*		
SC-7(7)		*	*		*	*		*	*	
SC-7(8)		*	*		*	*		*	*	
SC-7(9)		+	+					+	+	
SC-7(10)		+						+		
SC-7(11)			*			*			*	
SC-7(12)	Yes	*	*	*	*	*	*	*	*	*
SC-7(13)		*	*		*	*		*	*	
SC-7(14)		*	*		*	*		*	*	
SC-7(15)	Yes	+			+			+		
SC-7(16)	Yes	+			+			+		
SC-7(17)	Yes	+	+		+	+		+	+	
SC-7(18)	Yes	*	*	*	*	*	*	*	*	*
SC-8	Yes		*			*			*	
SC-8(1)										
SC-8(2)		+	+	+				+	+	+
SC-9	Yes	*			*			*		
SC-9(1)		*			*			*		
SC-9(2)		+	+	+				+	+	+
SC-10		*	*		*	*		*	*	
SC-11			*			*			*	
SC-12		*	*		*	*		*	*	
SC-12(1)				*			*			*
SC-12(2)		+	+	+	+	+	+	+	+	+
SC-12(3)										
SC-12(4)										
SC-12(5)										
SC-13	Yes	*	*		*	*		*	*	
SC-13(1)	Yes	*			*			*		
SC-13(2)	Yes	*			*			*		
SC-13(3)	Yes	*			*			*		
SC-13(4)	Yes	+	+		+	+		+	+	
SC-14			*	*		*	*		*	*

ID#	Supplemental Guidance	Transfer			Access			Multilevel		
		C	I	A	C	I	A	C	I	A
SC-15	Yes	--			*			--		
SC-15(1)	Yes	--			*			--		
SC-15(2)	Yes	*	*		*	*		*	*	
SC-15(3)	Yes	--	--		--	--		--	--	
SC-16	Yes	+	+					+	+	
SC-16(1)	Yes		+						+	
SC-17	Yes	*	*		*	*		*	*	
SC-18	Yes		*			*			*	
SC-18(1)	Yes		*			--			*	
SC-18(2)	Yes		*			*			*	
SC-18(3)	Yes		*			--			*	
SC-18(4)	Yes		--			--			--	
SC-19	Yes	*	*		*	*		*	*	
SC-20	Yes		*			*			*	
SC-20(1)	Yes		*			*			*	
SC-21	Yes		*			*			*	
SC-21(1)	Yes		*			*			*	
SC-22	Yes	*	*	*	*	*	*	*	*	*
SC-23	Yes		*			*			*	
SC-23(1)	Yes		*			*			*	
SC-23(2)	Yes		*			*			*	
SC-23(3)	Yes		*			*			*	
SC-23(4)	Yes		*			*			*	
SC-24	Yes	*	*	+	*	*	+	*	*	+
SC-25	Yes									
SC-26	Yes									
SC-26(1)	Yes									
SC-27	Yes									
SC-28	Yes	*	*		*	*		*	*	
SC-28(1)	Yes	+	+		+	+		+	+	
SC-29										
SC-30										
SC-30(1)										
SC-30(2)										
SC-31	Yes	+	+		+	+		+	+	
SC-31(1)		+	+		+	+		+	+	
SC-32	Yes	+	+		+	+		+	+	
SC-33	Yes									

ID#	Supplemental Guidance	Transfer			Access			Multilevel		
		C	I	A	C	I	A	C	I	A
SC-34	Yes									
SC-34(1)	Yes									
SC-34(2)	Yes									
SI-1		*	*	*	*	*	*	*	*	*
SI-2			*			*			*	
SI-2(1)										
SI-2(2)			*			*			*	
SI-2(3)			*			*			*	
SI-2(4)			*			*			*	
SI-3	Yes		*			*			*	
SI-3(1)	Yes		*			*			*	
SI-3(2)	Yes		*			*			*	
SI-3(3)	Yes		*			*			*	
SI-3(4)	Yes									
SI-3(5)	Yes		+			+			+	
SI-3(6)	Yes									
SI-4	Yes		*			*			*	
SI-4(1)	Yes		*			*			*	
SI-4(2)	Yes		*			*			*	
SI-4(3)	Yes									
SI-4(4)	Yes	*	*		*	*		*	*	
SI-4(5)	Yes		*			*			*	
SI-4(6)	Yes		*			*			*	
SI-4(7)	Yes		*	*		*	*		*	*
SI-4(8)	Yes	*	*	*	*	*	*	*	*	*
SI-4(9)	Yes		*			*			*	
SI-4(10)	Yes									
SI-4(11)	Yes	*			*			*		
SI-4(12)	Yes	*	*		*	*		*	*	
SI-4(13)		*	*	*	*	*	*	*	*	*
SI-4(14)		*	*		*	*		*	*	
SI-4(15)		*	*		*	*		*	*	
SI-4(16)			*			*			*	
SI-4(17)		*	*		*	*		*	*	
SI-5	Yes		*			*			*	
SI-5(1)	Yes		*			*			*	
SI-6	Yes		*			*			*	
SI-6(1)	Yes		*			*			*	

ID#	Supplemental Guidance	Transfer			Access			Multilevel		
		C	I	A	C	I	A	C	I	A
SI-6(2)										
SI-6(3)			*			*			*	
SI-7	Yes		*			*			*	
SI-7(1)	Yes		*			*			*	
SI-7(2)	Yes		+			+			+	
SI-7(3)	Yes									
SI-7(4)	Yes		+			+			+	
SI-8	Yes		*	*		*	*		*	*
SI-8(1)	Yes		*	*		*	*		*	*
SI-8(2)			*	*		*	*		*	*
SI-9	Yes		*			*			*	
SI-10	Yes		+			+			+	
SI-11	Yes		*			*			*	
SI-12	Yes	*	*		*	*		*	*	
SI-13										
SI-13(1)										
SI-13(2)										
SI-13(3)										
SI-13(4)	Yes		+	+		+	+		+	+
PM-1		*	*	*	*	*	*	*	*	*
PM-2		*	*	*	*	*	*	*	*	*
PM-3		*	*	*	*	*	*	*	*	*
PM-4		*	*	*	*	*	*	*	*	*
PM-5		*	*	*	*	*	*	*	*	*
PM-6		*	*	*	*	*	*	*	*	*
PM-7		*	*	*	*	*	*	*	*	*
PM-8		*	*	*	*	*	*	*	*	*
PM-9		*	*	*	*	*	*	*	*	*
PM-10		*	*	*	*	*	*	*	*	*
PM-11		*	*	*	*	*	*	*	*	*

## 5. Supplemental Guidance

The following section provides additional information concerning control intent specific to a CDS, and also provides CDS-related guidance.

### AC 1 Access Control Policy and Procedures

The intent of this control is that the organization implementing a CDS should develop, disseminate and review a high-level document that addresses the purpose, scope, roles, responsibilities, management commitment, coordination and compliance among organizational entities. Relevant documentation includes but is not limited to CONOPS, COOP, etc. Organization is defined as both PMO and Site. Documentation developed will support the intent of this control. The vendor should provide sites with Access Control policy documentation describing AC capabilities to the site. The vendor should comply with DCFA-1.2 so that the site can write a CONOPS.

### AC 2 Account Management

The intent of this control is to ensure that the site appropriately manages CDS system accounts, and in conjunction with organizational policy and documented process, establish rules/procedures for account and group management. CDS documentation should clearly define the account capabilities (or lack thereof) of TACDIS for the site. Vendor should supply the site with CONOPS documentation to facilitate this.

#### AC 2 1 Account Management

The intent of this control enhancement is to ease the burden of CDS account management on site.

#### AC 2 2 Account Management

The intent of this control enhancement is to ensure that nonessential accounts do not exist on the CDS, to reduce risk introduced by temporary and emergency accounts, and ease the site's burden of managing temporary accounts. The CDS product vendor should ensure that temporary and emergency accounts are not required for system functionality and that they can be removed by the CDS. The CDS vendor should also ensure that the capability to automatically terminate accounts exists and is documented within the CDS user manuals when they are required, e.g., for install.

#### AC 2 3 Account Management

The intent of this control enhancement is to reduce risk introduced by temporary and emergency accounts. The CDS vendor will ensure that temporary and emergency accounts - which cannot be removed in order for the system to function properly - will not be required to remain active and will be disabled by default.

#### AC 2 4 Account Management

The intent of this control enhancement is to ensure that the CDS tracks changes to accounts and integrity of accounts to provide administrators with evidence that improves situational awareness. The CDS should generate audit records for account creation, modification, disabling, and termination actions and notify appropriate individuals, as required by policy.

#### AC 2 5 Account Management

The intent of this control enhancement is to ensure that the site establishes and enforces CDS account daily usage policy and monitors for compliance to ensure the organization is aware of atypical account use. The CDS product vendor should ensure that automated processes exist to log users and administrators out after a given period of inactivity. The time duration will be configurable via the administrator(s) account(s).

#### AC 2 7 Account Management

The intent of this control enhancement is to ensure the organization is aware of and accountable for the assignment of accounts and roles that are created on the CDS.

The CDS product vendor should provide documentation defining all accounts, including their functions, which exist on the CDS by default or in an “out-of-the-box” state. The documentation should also specify if the account is required to remain present for the system to function properly.

**AC 3 Access Enforcement**

The intent of this control is to ensure the complexity of the authentication mechanism on the CDS correlates to the classification of the data processed by the CDS. The CDS should have the capability to enforce the use of strong passwords in accordance with IA-5.

**AC 3 2 Access Enforcement**

The intent of this control enhancement is to limit exploits possible by an insider threat. The CDS vendor should ensure that the CDS is capable of enforcing dual authorization. The vendor should also ensure that manuals are provided to the entity utilizing the CDS which define the method for proper configuration of a dual authorization feature. The organization utilizing The CDS should ensure that the CDS is configured to utilize dual authorization as per organizational policy.

**AC 3 3 Access Enforcement**

The intent of this control enhancement is to ensure that users are not able to bypass organizational defined access policy. The CDS vendor will ensure that the CDS allows for object level access control as well as provide documentation that defines the method and proper use of the access controls.

**AC 3 4 Access Enforcement**

The intent of this control enhancement is to allow the user to define access control permissions on objects they own on the CDS. The CDS should utilize DAC/MAC ensuring that users can define permissions on objects for which they are the object owner. The PMO will create documentation which defines the configuration in place as it relates to DAC/MAC.

**AC 3 5 Access Enforcement**

The intent of this control enhancement is to prevent security-relevant information from within the CDS that can potentially impact the operation of security functions in a manner that could result in failure to enforce the system security policy or maintain isolation of code and data. Processes running in maintenance/single user mode will not perform mission/business-related processing.

**AC 3 6 Access Enforcement**

The intent of this control enhancement is to reduce the probability of unauthorized disclosure of information, detect unauthorized changes to information and to eliminate the possibility of unauthorized access to the information from the network. The organization utilizing the CDS should have an Access Control policy, procedures addressing access enforcement; CDS design documentation, CDS configuration settings with associated documentation and a CDS audit records document.

**AC 4 Information Flow Enforcement**

The intent of this control is to prevent the spill of confidential information to a lower domain and to prevent the acceptance of malicious information in the high domain.

This control applies to transfer and multilevel CDSs, but does not apply to access solutions. Flow control within a CDS is applied to data intended for transfer between domains, as such, this control does not apply to data intended for hosting within the CDS. This control represents both the capabilities provided by a CDS technology as well as a configuration policy implemented upon that technology. The CDS should implement flow control by means of a set of hardware and/or software collectively known as the filter. References to CDS in the guidance statements apply to CDS filtering capabilities. Enabling/Disabling of provided capabilities are confirmed when the CDS is instantiated at the site.

**AC 4 1 Information Flow Enforcement**

The intent of this control enhancement is to enforce that only data from identified sources is sent to specifically identified destinations [between systems]. By applying this control, the intent is for the CDS to use source/destination identifiers, such as credentials or other attributes, in order to make flow decisions between systems. For example, flow control policy may state that information from one coalition member only be provided to one other coalition member. The CDS should not send data with partial or mismatched source/destination attributes when required by policy and the CDS must correctly utilize source attributes in combination with destination attributes for establishing flow control decisions.

**AC 4 2 Information Flow Enforcement**

The intent of this control enhancement is to ensure that data flowing from object to object internal to the CDS follow a trusted path. The flow processing path operates in domains isolated from other domains. Subjects interacting with data along this path should be isolated from other system subjects/objects.

The CDS must ensure that subject(s) in the trusted path are confined only to interactions with the next consecutive subject(s) in the defined processing flow. (NOTE: This must include interactions with the associated objects.) The CDS must also ensure that input, processing, and output domains are not shared and that individual processes making go/no-go decisions are in independent domains.

**AC 4 3 Information Flow Enforcement**

The intent of this control enhancement is to provide for dynamic reconfiguration of the CDS based on changing operational considerations. This control would apply to pre-approved configurations, where the CDS can dynamically change the running configuration from a pre-defined, pre-approved set of configurations.

The CDS should be capable of storing multiple pre-approved configurations and of detecting site-defined operational conditions that would trigger a change in configuration. The CDS should be able to select the appropriate approved configuration based upon operational condition triggers. The CDS should be able to execute changes in configurations that were based on the selected approved configuration.

**AC 4 4 Information Flow Enforcement**

The intent of this control enhancement is to ensure that encrypted traffic is not sent straight through the CDS unless it is processed by the filtering mechanisms of the CDS. The CDS must decrypt/decode the traffic so that the system's filtering mechanisms are able to accurately document and filter the traffic/data. As defined by policy, when the CDS decrypts/decodes the traffic, it is responsible for re-encrypting/re-encoding the data prior to sending data to the destination domain. For CDSs the term encryption is extended to cover encodings (i.e., Base 64, UTF-8, etc.) not recognized by the filtering mechanisms of the CDS. The CDS should block all encrypted/encoded data it receives that it is unable to decrypt/filter. The CDS should not be capable of being configured to allow encrypted/encoded data to be sent directly through the CDS (i.e., bypassing the filtering mechanisms). The CDS should restrict access to the configuration of encryption/encoded mechanisms to only authorized, privileged users.

**AC 4 5 Information Flow Enforcement**

The intent of this control enhancement is to ensure that the CDS denies messages that include embedded objects beyond the limits established by organizational policies. The CDS should be capable of detecting embedded objects and correctly detecting and blocking embedded objects beyond established policy. The CDS should be configured to detect embedded objects within all allowable data types as defined by site policy.

**AC 4 6 Information Flow Enforcement**

The intent of this control enhancement is to make flow control decisions on the basis of metadata (e.g., deny flow if metadata is present, direct flow based upon the content of metadata, apply filters based upon metadata). The CDS should apply content filters to the content of

metadata fields and should properly handle malformed metadata structures. The CDS should also properly handle the metadata in accordance with security policy. (e.g., blocks the message, strips the metadata, or overwrites, etc.) The CDS should be capable of documenting metadata within a data object.

**AC 4 7 Information Flow Enforcement**

The intent of this control enhancement is to reduce the risk that a software failure will compromise an intended one-way cross domain dataflow. The use of hardware enforced flow direction is preferable in high risk environments. The CDS should provide flow direction enforcement by means of hardware mechanisms and not contain physical connections between domains beyond the one-way flow specified.

**AC 4 8 Information Flow Enforcement**

The intent of this control enhancement is to ensure the CDS provides the ability to define specific filters and an order of execution for those filters for each information flow. Based upon the configuration, the CDS must then enforce those filters for the flow and ensure that the data transfer is processed by each filter prior to being released to the destination. If a transfer fails a filter, the CDS shall block, strip, modify or quarantine the data, based on security policy. If the security policy requires either modification or stripping of the data, the CDS must ensure completion of the processing flow prior to release.

**AC 4 9 Information Flow Enforcement**

The intent of this control enhancement is to ensure that all content is properly inspected prior to transfer. The use of a human review is required, in some cases, when the CDS does not provide an adequate mechanism to perform this review. The CDS should be configured to initiate human review when selected criteria are encountered and the review mechanism should display the data in an easily readable and understandable format. (e.g., in the native application/reader) The CDS should require a response from the reviewer prior to taking action on the transfer data and then should take appropriate actions as indicated by the human reviewer, (e.g., reject, forward, reply, etc.) but should not allow the reviewer to circumvent any additional filtering mechanisms. Finally, the CDS should allow only authorized reviewers access to the human review mechanism.

**AC 4 10 Information Flow Enforcement**

The intent of this control enhancement is to provide CDS administrators the ability to select the filters that are executed on a specific data flow based on the type of data that is being transferred. For CDS data flows, all available filters should be applied to all data flows. However, there may be instances where a filter may not be necessary. (e.g., a message containing a single 4 byte field limited to a set of printable ASCII would not benefit from virus scanning.) The CDS should only allow privileged administrators to modify the selection of filters applied to a data flow/data type and should properly apply all of the selected filters to the proper data flows/data types.

**AC 4 11 Information Flow Enforcement**

The intent of this control enhancement is to provide authorized, privileged CDS administrators the ability to configure (enable, disable, modify) filters, such as the dirty/clean word list and the CDS malicious code filtering mechanisms according to the specific mission need of the CDS.

Only authorized, privileged CDS administrators should perform these functions. The reconfiguration of the CDS should not be allowed when the CDS is in an operational state. Any changes made to the configuration of the CDS filters must be vetted through the DAA or accreditation authority prior to implementation. The CDS malicious code/filtering mechanism will be configured to meet operational/mission requirements.

**AC 4 12 Information Flow Enforcement**

The intent of this control enhancement is to ensure that the CDS is able to properly document structured data objects intended for transfer. Identification and validation of input objects is

based on defined specifications tied to each allowed data format. This validation helps ensure proper filter operation. Also the filter mechanisms should test for consistency with respect to a defined specification (i.e., if an object departs from the defined specification, the filter will reject the object).

**AC 4 13 Information Flow Enforcement**

The intent of this control enhancement is to ensure that data objects (application layer protocols) are decomposed correctly into their constituent parts. As a minimum the CDS must understand all layers of encapsulation that may surround a given payload. The CDS should be capable of documenting the presence of embedded objects within data traffic. The ability to enforce an embedded object policy is independent of the CDS's ability to document and isolate embedded objects.

The CDS should correctly document the protocols being used and reject protocols that are invalid, unknown or disallowed by policy. The CDS should be able to fully parse embedded objects (to include checking for additional embedded objects) and handle invalid fields according to defined security policies. [e.g., reject the entire message; strip the field, etc.]

**AC 4 14 Information Flow Enforcement**

The intent of this control enhancement is to reduce the range of potential attacks against a system being protected by a CDS. Constraining data fields to the minimum essential enumeration reduces the attack surface available to malicious intent and limits the likelihood of zero-day attacks. This control ensures that the CDS applies a filter policy to the data that is being transferred through the system. The CDS must analyze and validate the field structure of the data object in addition to the data contained within each field. The CDS should analyze each field to ensure all required fields are present, occur in the proper order, and conform to length restrictions. The CDS should analyze the data to document if it conforms to a defined data specification or schema. The CDS must apply the constraint rules defined in the data specification or schema to the data received, and blocks, quarantines, or modifies (as defined by the security policy) all data objects that do not comply.

**AC 4 15 Information Flow Enforcement**

The intent of this control enhancement is to ensure that the CDS further analyzes the data contained within the data objects it receives beyond applying field and character constraints and beyond basic virus or mobile code detection capabilities. Once the determination is made that the data object is in an identifiable format and complies with the proper data specification, further analysis must be performed to ensure that unsanctioned data has not been included within the data object. Unsanctioned data in the context of this control is defined as unallowable enumerations within the explicitly allowed enumerations established by any constraints. For example, when constraining fields to alphabetic characters, the organization may wish to document JAVASCRIPT as an unsanctioned enumeration within the allowed constraints. The intent of this control [when used in conjunction with AC-4(14)] is to provide the organization with increased operational flexibility utilizing relaxed constraints, while specifically enumerating unsanctioned configurations of otherwise sanctioned field enumerations.

Unsanctioned data includes classified/sensitive information whose release from the source network could result in data leakage to untrusted recipients and executable code that could disrupt or harm the services or systems on the destination network.

**AC 4 16 Information Flow Enforcement**

The intent of this control enhancement is to ensure that the CDS has been designed considering a risk-managed CDS architecture. Selection of lower-risk architectures reduces the threat of zero-day attacks. This control allows designers to select the minimum risk architecture necessary to meet operational requirements and ensures that the implemented CDS architecture

uses solutions that enforce the defined security policy and minimizes data transfer across the border.

**AC 4 17 Information Flow Enforcement**

The intent of this control enhancement is to ensure that the CDS has a mechanism(s) to monitor incoming and outgoing data to distinguish traffic as either authorized (i.e., traffic from an authorized source or to an authorized destination) or unauthorized (unauthorized source/destination) prior to processing a transfer to the destination domain. The CDS must provide mechanisms to authenticate the source and the destination of information.

If the source and destination domains cannot be identified or authenticated or are unauthorized, the transfer shall be rejected prior to processing. Auditing of this event is included under AU-2. Source and destination domains, addresses, and individuals must be bound to data transfer at the time of creation and maintained throughout CDS processing. This may also require that the CDS strip source information/binding and rebind within the CDS prior to delivery to the destination.

**AC 5 Separation of Duties**

The intent of this control is to ensure that documentation describes how the CDS implements role separation as it relates to CDS access Mission function as it relates to CDS is defined as individuals with a need to transfer information across domains. Mission Function and the CDS Administration Function are unique and must be separated by physical and/or logical security controls as well as organization policy. For example:, the Audit Admin and Security Admin must be two separate distinct accounts where essential permissions do not overlap; And a single CDS user may not modify the IP address of the system and remove audit logs; or a user who logs in from the web cannot edit the system, but can upload documents.

**AC 6 Least Privilege**

The intent of this control is to ensure that CDS users and the CDS system itself do not have more levels of access than are needed to complete their job. All account types should have the minimum required privileges to perform their duties and each role should perform a minimal set of duties such that no role is allowed to intentionally or unintentionally perform unauthorized actions.

**AC 6 1 Least Privilege**

The intent of this control enhancement is to ensure that organizational policy is established and implemented. Corporate policy should ensure that authorized personnel are explicitly granted access to explicitly defined security/IA functions of the CDS. Such policy should include a description of the penalty for attempted unauthorized access is established such that the design of the CDS should allow granular access to security features to support site policy; review CDS security documentation (HLD, LLD, SSDD, and CONOPS).

**AC 6 2 Least Privilege**

The intent of this control enhancement is to ensure that the customer establish policy limiting use of privileged accounts to performance of duties which require access to identified security/IA functions. Implementation of such policy may prevent intentional or unintentional misuse on the CDS.

**AC 6 3 Least Privilege**

The intent of this control enhancement is to limit the exposure of CDS privilege functions over the network while not physically present at the system console. The CDS should not provide network access to privileged functions or it will be ensured that that access can be restricted according to policy. A policy will be in place which identifies privileged functions and that network access to them is prohibited. Remote CDS access should be prohibited except when there is a compelling operational need. Procedures for remote access based upon operational need should be included in the CDS documentation set.

**AC 6 4 Least Privilege**

The intent of this control enhancement as stated in the supplemental guidance: employing

virtualization techniques to allow greater privilege within a virtual machine while restricting privilege to the underlying actual machine is an example of providing separate processing domains for finer-grained allocation of user privileges.

The CDS should provide finer-grained allocation of user privileges through the use of separate distinct processing domains such as virtual machines, zones, containers, compartments, separate hardware or similar mechanisms such that greater privilege is granted the user while restricting privileges to the actual machine.

**AC 6 5 Least Privilege**

The intent of this control enhancement is to prevent intentional or unintentional misuse by limiting privileged access. The organization should establish policy that limits the number of privileged CDS accounts and that requires that privileged user accounts be distributed only to appropriately trained personnel.

**AC 6 6 Least Privilege**

The intent of this control enhancement is to ensure that only directly affiliated personnel who have an explicit trust relationship have been granted privileged access to the CDS. Site policy will exist that prohibits privileged access to the information system by non-organizational users. Organizational User is defined as contractor, guest researcher, individual detailed from another organization or individual from an allied nation.

**AC 7 7 Unsuccessful Login Attempts AC-14**

The intent of this control is to ensure that the CDS does not allow unlimited unauthorized access attempts. The CDS should automatically lock user/administrator accounts after an organization-defined number of invalid login attempts within an organization-defined time period.

**AC 7 1 Unsuccessful Login Attempts**

The intent of this control enhancement is to help ensure that the account has not been compromised by enforcing administrator intervention. The CDS vendor should ensure that the CDS has a method for locking users out after a given number of failed log-in attempts. The vendor should also ensure that the locked account will not become unlocked without the direct action of an administrator.

**AC 7 2 Unsuccessful Login Attempts**

The intent of this control enhancement is to ensure the security of mobile devices. A Mobile CDS should clear/zero/wipe its configuration/data after an organizational pre-defined number of consecutive unsuccessful login attempts or when it is removed from authorized physical control

**AC 8 System Use Notification**

The intent of this control is to ensure that all users and administrators are presented with and consent to the requirements of a system login banner prior to gaining CDS access. The banner should provide the user/administrator with specific notification of the terms and conditions of system access as well as the legal ramifications of system misuse.

**AC 9 Previous Logon (Access) Notification**

The intent of this control is to raise user awareness of potential account compromise. The CDS should provide CDS users with the date and time of previous login attempts.

**AC 9 1 Previous Logon (Access) Notification**

The intent of this control enhancement is to allow a user to know if their account has been compromised. The CDS should notify the user of previous unsuccessful login attempts.

**AC 9 2 Previous Logon (Access) Notification**

The intent of this control enhancement is to allow a user to know if their account has been compromised. The CDS should notify the user of the number of successful logins and unsuccessful login attempts.

**AC 9 3 Previous Logon (Access) Notification**

The intent of this control enhancement is to allow a user to know if their account has been compromised. The CDS should notify the user of security-related changes to the user's account.

- AC 10 Concurrent Session Control**  
 The intent of this control is to mitigate conflict in configuration. The vendor should ensure there is a method for configurable limits to the number of concurrent sessions allowed by a given user or system administrator. The default limit should be no greater than one. This will be configurable for both remote and local sessions. Organizational policy should exist which identifies how many concurrent sessions are allowed when the number exceeds one.
- AC 11 Session Lock**  
 The intent of this control is to allow users to lock the system and prevent access without losing the state of the current session. The vendor should ensure that the system has the capability to lock the user's session, without disturbing the state of the session and that this capability cannot be disabled or subverted.
- AC 11 1 Session Lock**  
 The intent of this control enhancement is to prevent unauthorized disclosure of information during a locked user session. The vendor should ensure that when a session is locked the display is hidden and that no system or user data is displayed.
- AC 14 Permitted Actions without Identification**  
 The intent of this control is to ensure that the organization has identified and documented their rationale allowing actions that can be performed on the CDS without identification or authentication. The vendor should provide documentation which shows which of these actions are configurable, the extent to which they are configurable and how they are configured by the system administrator. Only an authorized system administrator should have permissions to configure these items.
- AC 14 1 Authentication**  
 The intent of this control enhancement is to ensure that the minimal set of unauthenticated interaction is supported only for mission/business related objectives that are permitted by organizational policy. The CDS vendor should provide documentation showing all actions that can be performed without identification or authentication. The documentation should include which actions are configurable and how they are configured by the system administrator. Only an authorized system administrator should have permissions to configure these items.
- AC 16 Security Attributes**  
 The intent of this control is to reduce the risk of compromise to the confidentiality of the information processed by the CDS by ensuring that the integrity of security attributes (e.g., classification, releaseability) are not modified when processed by the CDS. The CDS should ensure that security attributes are preserved when transferring, storing, and accessing data and should ensure that security attributes of the data are maintained throughout the process.
- AC 16 1 Security Attributes**  
 The intent of this control enhancement is to prevent unintentional information disclosure as a result of mislabeled data. The CDS should ensure that the security label of the data does not change outside of the regrader and that the regrader correctly enforces the security policy.
- AC 16 2 Security Attributes**  
 The intent of this control enhancement is to ensure that only the regrader is authorized to modify security labels. The CDS should ensure that re-labeling data/object without using the regrader (e.g., setlabel, chcon, etc.) is not possible.
- AC 16 3 Security Attributes**  
 The intent of this control enhancement is to reduce the risk of compromise to the confidentiality of information handled by the CDS by ensuring that security attributes are sufficient to enable the CDS to take automated policy actions that are relevant data storage, transmission and accessibility based on the security attributes of the data.
- AC 16 4 Security Attributes**  
 The intent of this control enhancement is to ensure the CDS only allows authorized users to set classification security attributes. The CDS cannot reclassify or declassify outside of the regrader.

Classifications on the CDS should not be set by a user; only the regrader may reclassify or declassify.

**AC 16 5 Security Attributes**

The intent of this control enhancement is to reduce the risk of compromise to confidentiality of information by ensuring that all information that is output by the CDS is labeled with security attributes in such a way that personnel may discern the sensitivity of the information.

**AC 17 Remote Access**

The intent of this control is to minimize remote access to the CDS and thereby minimize organizational risk. A policy should be in place which establishes remote access restrictions.

**AC 17 1 Remote Access**

The intent of this control enhancement is to ensure compliance with remote access policy. For solutions that support remote access, ensure the CDS restricts access to only authorized subjects and monitors/audits remote access sessions.

**AC 17 2 Remote Access**

The intent of this control enhancement is to ensure that policy is in effect and enforced to protect data confidentiality and integrity during CDS remote access sessions. Remote access sessions should be encrypted using a FIPS 140-2 compliant algorithm.

**AC 17 3 Remote Access**

The intent of this control enhancement is to maintain system integrity by preventing or minimizing unauthorized access to the CDS. The CDS vendor should provide documentation on the automated mechanisms used to implement the access control policy for remote access. Documentation should include how to properly configure these mechanisms.

**AC 17 4 Remote Access**

The intent of this control enhancement is to reduce the exposure of CDS privilege functions and access to security-relevant information (firewall configurations, logs, etc.) from outside of the enclave boundary.

**AC 17 5 Remote Access**

The intent of this control enhancement is to ensure the organization can detect and correct unauthorized remote connections to the CDS and that the CDS can take corrective action. The vendor should provide documentation that shows the CDS has mechanisms to identify and take corrective action upon detection of unauthorized remote connections.

**AC 17 6 Remote Access**

The intent of this control enhancement is to prevent unauthorized disclosure of remote access capabilities of the CDS.

**AC 17 7 Remote Access**

The intent of this control enhancement is to ensure that the organization has additional mitigating controls to protect security relevant information when it is accessed remotely and access sessions are audited. The CDS vendor should ensure that a method for logging remote sessions for privileged users and system administrators, if remote access to privileged accounts is allowed by organizational policy. The CDS should be capable of providing audit trails of remote access attempts.

**AC 17 8 Remote Access**

The intent of this control enhancement is to limit exposure of the CDS and reduce the possible well-known vulnerabilities introduced by the use of organization-defined networking protocols within the CDS deemed to be non-secure.

**AC 18 Wireless Access**

The intent of this control is to ensure that organization wireless policy specifically includes references to wireless CDS. Policy statements should include usage restrictions, implementation guidance, monitoring for unauthorized access, proper authorization and authentication for wireless access, and enforcement of requirements for wireless connections of/to the CDS.

**AC 18 1 Wireless Access**

The intent of this control enhancement is to reduce the risk of unauthorized access to CDS wireless connections. Where applicable, ensure that approved FIPS 140-2 compliant encryption and authentication methods have been implemented for CDS wireless connections.

**AC 18 2 Wireless Access**

The intent of this control enhancement is to ensure that the CDS can detect and appropriately respond to unauthorized wireless access connections to the networks which interface with the CDS. Where applicable, Ensure the CDS can detect and properly respond to unauthorized connection attempts over wireless interfaces.

**AC 18 3 Wireless Access**

The intent of this control enhancement is to mitigate the threat of wireless-based attacks to the CDS by disabling embedded wireless devices and capabilities when and where their use is not needed or authorized. Where wireless communication is not supported by the CDS, the CDS should have a method for physically disabling the wireless hardware.

**AC 18 4 Wireless Access**

The intent of this control enhancement is to limit vulnerabilities introduced by intentional or unintentional misconfiguration of wireless interfaces on the CDS. Users should have no access to wireless configuration settings present on the CDS.

**AC 18 5 Wireless Access**

The intent of this control enhancement is to limit exposure of the CDS by confining its wireless network coverage to, at most, the physical perimeter of the site. The CDS vendor should ensure that CDS wireless devices have adjustable power levels, range limitations and, when they are available, secure infrared transmission capabilities.

**AC 19 Access Control for Mobile Devices**

The intent of this control is to ensure that a variety of threats to CDS via mobile devices have been mitigated through policy. Organizational policy should be in place to address the CDS access using secure mobile device technologies.

**AC 19 1 Access Control for Mobile Devices**

The intent of this control enhancement is to limit the exposure of the CDS to writable, removable media based threats (sneaker-net) by restricting use of removable media. The CDS should have the capability to prevent removable media from being mounted to the system when not a part of a configurable list of acceptable devices (white list). The CDS should not allow a device to be mounted, even when included on the white list, if the device is not encrypted in accordance with FIPS 140-2. Organizational policy should be established that restricts use of writable, removable media with the CDS.

**AC 19 2 Access Control for Mobile Devices**

The intent of this control enhancement is to limit exposure of the CDS to removable media based threats (sneaker-net) by prohibiting the use of personally owned media with the CDS. Organizational policy should be established which prohibits the use of personally owned removable media on the CDS.

**AC 19 3 Access Control for Mobile Devices**

The intent of this control enhancement is to limit exposure of the CDS to removable media based threats (sneaker-net) by prohibiting the use of media with no identifiable owner on the CDS. Organizational policy should be established which prohibits the use of removable media with no identifiable owner.

**AC 19 4 Access Control for Mobile Devices**

The intent of this control enhancement is to limit the exposure of the CDS to mobile computing device based threats by limiting their use in the same area where the CDS is deployed. Organizational policy should be established which restricts the use of mobile computing devices in close proximity to the CDS.

**AC 21 1 Sharing**

The intent of this control enhancement is to ensure the CDS has automated mechanisms to

support reliable human review (RHR). In some cases, RHR is the preferred method for application of security policies to decide upon the release of information. Due in part to the increasing number required items for review, at present, the use of artificial intelligence and natural language processing is not able to remove the human totally from the process. The CDS should have automated mechanisms for implementing access authorizations supporting information sharing/user collaboration decisions also RHR must be able to be enabled/disabled by the site. Organizational policy should be established to address information sharing. REMOVE Turned on or off optional by

**AU 1 Audit and Accountability Policy and Procedures**

The intent of this control is to ensure the creation of policy and procedures, which are required for the effective implementation of selected security controls and control enhancements in the audit and accountability family for CDS. The CDS vendor should provide documentation defining the audit/logging capabilities of the CDS and how to configure these functions. The guidance for auditing and accountability policy and procedures will be given in accordance with applicable federal laws, executive orders, directives, policies, regulations, standards, and other guidance.

**AU 2 Auditable Events**

The intent of this control is for the organization to document significant auditable events relevant to the security of the CDS; giving an overall system requirement in order to meet ongoing and specific audit needs. The CDS's configured set of audited events should match those required by applicable audit and accountability policy and should be listed in supporting CDS documentation (e.g., SSDD, CONOPS).

**AU 2 3 Auditable Events**

The intent of this control enhancement is to ensure the organization regularly reviews and updates the list of events which are relevant to the security of the CDS and, therefore, need to be audited. The list of auditable events on The CDS should not change.

**AU 2 4 Auditable Events**

The intent of this control enhancement is to improve situational awareness and to ensure that execution of privileged functions are audited by the CDS. The execution of privileged commands/functions should be capable of being audited by the system.

**AU 3 Content of Audit Records**

The intent of this control is to ensure that the CDS produces audit trail data with sufficient detail to provide individual accountability, reconstruction of events, problem monitoring, and intrusion detection. The CDS should produce audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event.

**AU 3 1 Content of Audit Records**

The intent of this control enhancement is to improve situational awareness by ensuring that the CDS is configured to provide the required level of detail for audit events, as required by organizational policy.

**AU 3 2 Content of Audit Records**

The intent of this control enhancement is to ensure that the CDS protects audit records from data security threats and prevents unauthorized access to sensitive information. The CDS should be configured to store audit records in a centrally managed database as listed in the supporting documentation (e.g. SSDD, CONOPS)

**AU 4 Audit Storage Capacity**

The intent of this control is to ensure that audit record storage capacity is not exceeded and that audit data is maintained appropriately in accordance with established organizational policy.

Organizational policy should address the maximum size and retention rate of audit logs. The

CDS audit record storage capacity should not be exceeded under normal operations. If applicable, the CDS should have the capability to buffer logs locally in the event that communication with the log management server is lost. The CDS should have the ability to store a reasonable amount of data based on the robustness of the solution and the load capability under normal conditions to allow network engineers and/or system administrator's time to re-establish communications before logs become dropped.

**AU 5 Response to Audit Processing Failures**

The intent of this control is to ensure that designated organizational officials are informed of the failure of information assurance confidence mechanisms so that corrective action can be taken to ensure audited system activity is recorded.

The CDS audit capturing mechanism should alert designated organizational officials in the event of an audit processing failure and perform corrective actions as defined in organizational security policy or other relevant documentation. The CDS should have an automated capability to notify remote designated organizational officials in the event of an audit processing failure.

**AU 5 1 Response to Audit Processing Failures**

The intent of this control enhancement is to ensure that audit information is protected from accidental loss, unauthorized access, modification, and deletion.

The CDS protects audit information from The CDS should provide a warning when the organization-defined percentage of maximum audit record storage capacity is reached. The vendor should provide documentation that shows how to properly configure this percentage.

**AU 5 2 Response to Audit Processing Failures**

The intent of this control enhancement is to ensure timely review and analysis of CDS audit records for indication of inappropriate or unusual activity so that findings can be reported to a designated organizational official in a timely manner.

The CDS should provide a real-time alert when the following audit failure events occur. The CDS will be configured to audit failure events requiring real-time alerts as required by applicable audit and accountability policy.

**AU 5 3 Response to Audit Processing Failures**

The intent of this control enhancement is to ensure audit data availability and to prevent denial of service associated with events that have the potential to exceed normal thresholds.

The CDS should throttle network traffic when thresholds representing auditing capacity for network traffic have been reached. This will ensure that the audit system maintains accountability.

**AU 5 4 Response to Audit Processing Failures**

The intent of this control enhancement is to ensure that accountability and integrity of the CDS is maintained in the event of an audit failure. The CDS should invoke a system shutdown in the event of an audit failure, as required by applicable audit and accountability policy, unless an alternative audit capability exists.

**AU 6 Audit Review, Analysis, and Reporting**

The intent of this control is to ensure that the CDS produces audit trail data with sufficient detail to provide individual accountability, reconstruction of events, problem monitoring and intrusion detection. The level of detail required should be based on a current organizational risk assessment.

The CDS should produce audit trail data that will provide sufficient detail when there is a change in risk, as listed in the supporting documentation (e.g., SSDD, CONOPS). The CDS configuration produces an audit trail data that will have sufficient detail required by applicable site audit and accountability policy.

**AU 6 1 Audit Review, Analysis, and Reporting**  
The intent of this control enhancement is to ensure that the CDS is configured appropriately to effectively and efficiently document the underlying causes of an event. Related event information will all the organization to develop and initiate control measures that will reduce the likelihood of event recurrence as well as satisfy regulatory requirements. The CDS audit review, analysis, and reporting processes will support organizational processes for investigation and response as required in established organizational policy.

**AU 6 4 Audit Review, Analysis, and Reporting**  
The intent of this control enhancement is to facilitate analysis of transactions spanning multiple components. The CDS should have an automated mechanism for centralized review and analysis.

**AU 6 5 Audit Review, Analysis, and Reporting**  
The intent of this control enhancement is to correlate attack detection events with scanning results. The CDS should integrate analysis of audit records with analysis of vulnerability scanning information, performance data, and network monitoring information as mandated by policy.

**AU 6 6 Audit Review, Analysis, and Reporting**  
The intent of this control enhancement is to enable the identification of causal, or mechanistic relationships found between CDS audit logs physical access monitoring to further enhance an organization's ability to document suspicious, inappropriate, unusual, or malevolent activity.

The organization will correlate information from audit records with information provided from monitoring physical access to enhance the ability to document suspicious, inappropriate, unusual, or malevolent activity.

**AU 6 7 Audit Review, Analysis, and Reporting**  
The intent of this control enhancement is to ensure the CDS is operating in accordance with authorized audit and accountability policy.

The CDS should execute permitted actions for each authorized information system process, role, and/or user as specified in the audit and accountability policy (e.g., SSDD, CONOPS). The CDS should take permitted actions for each authorized information system process, role, and/or user as required by applicable audit and accountability policy.

**AU 7 Audit Reduction and Report Generation**  
The intent of this control is to address ways to facilitate use of audit information for detection and damage assessment. The CDS should provide an audit reduction and report generation capability.

**AU 7 1 Audit Reduction and Report Generation**  
The intent of this control enhancement is to address protection against system disruption (denial of service) as a result of the audit function and addresses ways to facilitate use of the information for detection and damage assessment.

The CDS should not be configured to select auditable event criteria (i.e., selective auditing based on user identities, files accessed, time-of-day, etc.) The system will have the capability to automatically process audit records for events of interest based on selectable event criteria as required by applicable audit and accountability policy.

**AU 8 Time Stamps**  
The intent of this control is to ensure the CDS provides consistent / accurate time-stamps when analyzing record data. Accuracy and integrity of audit records is required in the event audit data must be used as evidence in a legal proceeding.

The CDS should use an internal system clock to generate time stamps for audit records. Where

possible the system clock should be synchronized with an NTP server (where available) to ensure consistency of records with other network devices.

**AU 8 1 Time Stamps**

The intent of this control enhancement is to provide consistence / accurate time-stamps correlating related events in separate components, and/or to show the efficacy, accuracy, and integrity of legitimate records for use as evidence.

The CDS should be capable of using NTP servers to update and ensure the accuracy of internal system clocks and allow for effective event correlation across multiple event sources. This will be utilized to prevent time differences that create communications issues between various systems and the CDS.

**AU 9 Protection of Audit Information**

The intent of this control is to address protection against unauthorized disclosure, destruction, or modification of audit data; insertion of surreptitious audit data; and unauthorized disabling of the audit trail or denial of service as a result of the audit function. The CDS should enforce access controls (MAC, DAC) on audit records, audit settings, and audit reports to prevent unauthorized access, modification, and deletion.

**AU 9 1 Protection of Audit Information**

The intent of this control enhancement is to protect audit information from unauthorized access, modification, and deletion. The CDS should export audit records on hardware-enforced, write-once media.

**AU 9 2 Protection of Audit Information**

The intent of this control enhancement is to ensure the CDS provides redundant means of storing audit data to increase availability of the information.

The CDS should back up audit records listed onto a different system or media than the system being audited as mandated in the supporting documentation (e.g., SSDD, CONOPS). The CDS should be configured for auditing to match those required by applicable audit and accountability policy.

**AU 9 3 Protection of Audit Information**

The intent of this control enhancement is to ensure the efficacy, accuracy and integrity of the audit trail. The CDS should have a means to protect the integrity of audit information and audit tools.

**AU 9 4 Protection of Audit Information**

The intent of this control enhancement is to reduce the risk of audit compromises by privileged users. The CDS audit activity should be performed on a separate information system or by using storage media that cannot be modified. Policy mandates will authorize access to management of audit functionality to only a limited subset of privileged users and enforces the protection the audit records of non-local accesses to privileged accounts and the execution of privileged functions.

**AU 10 Non-repudiation**

The intent of this control is to ensure that the content of audit records sufficiently supports the concept of non-repudiation. Audit information should be maintained in a way that preserves the source, integrity, and origin of the data.

The CDS should implement digital signatures / digital message receipts and/or hashes such that audit events cannot be repudiated by the source of the event.

**AU 10 1 Non-repudiation**

The intent of this control enhancement is to support audit requirements that provide appropriate organizational officials the means to document who produced specific information in the event of an information transfer. The CDS audit system will provide non-repudiation of origin,

submission, sending, and transport services.

**AU 10 2 Non-repudiation**

The intent of this control enhancement is to mitigate the risk that information is modified between production and review. The CDS should implement a cryptographic checksum on audit information.

**AU 10 3 Non-repudiation**

The intent of this control enhancement is to provide appropriate organizational officials the means to know who reviewed and released information and to ensure that only approved review functions are employed. The CDS should maintain reviewer/releaser identity and credentials within the established chain of custody for all information that is reviewed or released.

**AU 10 4 Non-repudiation**

The intent of this control enhancement is to mitigate the risk that information is modified between review and transfer/release. The CDS audit capability will validate the binding of user's and administrator's identity to the information at the transfer/release point prior to release/transfer from one security domain to another security domain.

**AU 10 5 Non-repudiation**

The intent of this control enhancement is to ensure that conformance testing of security requirements for cryptographic modules have been accredited to U.S. government computer security standards. The CDS should implement FIPS-validated or NSA-approved cryptography for digital signatures in accordance with established policy.

**AU 11 Audit Record Retention**

The intent of this control is to ensure the availability of audit data for detection and damage assessment. Organizational policy should establish an acceptable minimum retention period.

**AU 12 Audit Generation**

The intent of this control is to ensure the adequate storage capacity for audit data as established by corporate policy.

The CDS should generate audit records, allow designated organizational personnel to specify auditable events, and generate defined audit records. The system's capability to generate audit information should be in accordance with this control.

**AU 12 1 Audit Generation**

The intent of this control enhancement is to collect appropriate audit data for correlation of related events in different CDS components. Audit records from the CDS should be time-correlated with other events within an organization-defined tolerance.

**AU 12 2 Audit Generation**

The intent of this control enhancement is to promote interoperability and exchange of audit data between dissimilar devices and the CDS. The CDS should generate audit records normalized to a standardized format as determined by organizational policy.

**AU 14 1 Session Audit**

The intent of this control enhancement is to ensure that the CDS has mechanisms to facilitate recording and analysis of user activity upon system startup. The CDS mechanism will initiate records of user access sessions upon system startup.

**CM 1 Configuration Management Policy and Procedures**

The intent of this control is to ensure establishment of organizational policy and procedures which direct effective implementation of selected security controls and control enhancements in the configuration management family. The CDS should manage security features and assurances through control of changes made to CDS hardware, software, and firmware documentation, and test documentation throughout its life cycle and measure the CDS system configuration state.

The organization should establish configuration management policy, procedures, and other relevant documents or records, for configuration management that include purpose, scope, roles,

responsibilities, management commitment, coordination among organizational entities, and compliance. The organization should disseminate the formal documented configuration management policy to elements within the organization having associated configuration management roles and responsibilities. The organization should have configuration management procedures which facilitate implementation of the configuration management policy and associated configuration management controls. The organization should disseminate formal documented configuration management procedures to elements within the organization having associated configuration management roles and responsibilities. The organization should have a documented definition of the frequency of configuration management policies and procedures reviews/updates.

**CM 2 2 Baseline Configuration**

The intent of this control is to establish a baseline CDS configuration which captures both structure and details in a controlled manner such that the organization may reproduce the baseline system and track changes to the baseline over time.

The CDS should have mechanisms in place to support the generation of a baseline configuration in accordance with this enhancement. The organization should develop and document a baseline configuration of the CDS and maintain, under configuration control, a current baseline configuration of the CDS.

**CM 2 2 1 Baseline Configuration**

The intent of this control enhancement is to ensure that the CDS baseline reflects the latest information and/or changes during installations and upgrades. The CDS should have a mechanism in place to update the baseline configuration. A configuration management policy, configuration management plan, procedures addressing the baseline configuration of the CDS, CDS architecture and configuration documentation should be created and maintained.

**CM 2 3 Baseline Configuration**

The intent of this control enhancement is to protect CDS integrity by enabling a clean restoration after erroneous operations occur.

The organization should establish operational support for a return to previously known good/consistent state and should retain old versions of baseline configurations as necessary to support rollback.

**CM 2 4 Baseline Configuration**

The intent of this control enhancement is to reduce administration time and overhead associated with blocking undesirable applications and processes.

The CDS should have a mechanism in place to support and enforce a defined deny-by-exception software execution policy. The organization should develop and maintain a list of software programs which are not authorized and employ an allow-all, deny-by-exception authorization policy to ensure the CDS allows execution of program/process activity that is not expressly denied by policy.

**CM 2 5 Baseline Configuration**

The intent of this control enhancement is to ensure the CDS blocks all process/application activity unless expressly allowed by policy. Processes/applications should not be executed on the CDS until the associated security risk has been evaluated and authorized. The CDS should have a mechanism in place to support and enforce a defined allow-by-exception software execution policy.

**CM 3 Configuration Change Control**

The intent of this control is to apply a systematic evaluation, coordination, approval or disapproval, and implementation of all approved changes to CDS configuration  
The CDS should have a mechanism in place to control configuration changes and functions as

established by organizational policy. A configuration management policy, configuration management plan, procedures addressing CDS configuration change control, CDS architecture and configuration documentation, security plan, change control records, and CDS audit records should be created and maintained.

**CM 5 Access Restrictions for Change**

The intent of this control is to ensure physical and logical access restrictions associated with changes to the system are established.

The CDS should have the capacity to restrict changes to the security of the system. The organization should define document, approve, and enforce physical and logical access restrictions associated with changes to the CDS in accordance with established policy.

**CM 5 1 Access Restrictions for Change**

The intent of this control enhancement is to reduce the need for human intervention in the enforcement of access restrictions and auditing of enforcement actions. The CDS should maintain records of access essential for ensuring that configuration change control is being implemented as intended, that access restrictions are enforced and that the system will audit those actions in such a way that any changes can be traced back to an individual. The CDS should have automated mechanisms to implement access restrictions and to audit enforcement actions.

**CM 5 2 Access Restrictions for Change**

The intent of this control enhancement is to support after-the-fact actions should the organization become aware of an unauthorized change to the CDS and that the organization is tracking changes to the system to no unauthorized changes were made. The CDS should have a mechanism in place to audit unauthorized system changes.

**CM 5 3 Access Restrictions for Change**

The intent of this control enhancement is to ensure the integrity of software installed on the CDS and to assure others that the software will be trusted. Signed software ensures that users can verify the origin of the software, as well as ensure that the software has not been tampered with prior to its use on the CDS. The CDS system only installs software from a trusted source and that the software hasn't been modified before installation.

The CDS should enforce digital certificate authentication prior to the installation of defined critical software programs/packages. Unsigned software should not be installed.

**CM 5 4 Access Restrictions for Change**

The intent of this control enhancement is to ensure separation of duties, for critical changes to the CDS components by having more than one person required to complete the task of making changes to the CDS.

Established organizational policy and automated CDS mechanisms should require a two-person rule for CDS changes.

**CM 5 5 Access Restrictions for Change**

The intent of this control enhancement is to limit unwanted/unexpected consequences of making changes to a production/live/deployed CDS so that the developer / integrator has access only to information and resources that are essential for its legitimate purpose and controlling the ability of the people building CDS's to make rogue changes.

Documentation showing how the organization limits information system developer/integrator privileges to change hardware, software, and firmware components and CDS directly within a production environment; the organizations definition for the frequency of reviews and reevaluations of CDS developer/integrator privileges; and how the organization reviews and reevaluates CDS developer/integrator privileges in accordance with the organization-defined

frequency should be created. This documentation should also include information as to the frequency of reviews.

**CM 5 6 Access Restrictions for Change**

The intent of this control enhancement is to ensure that the code and data that provide services to independent CDS programs/processes (allowing the sharing and changing of code and data in a modular fashion) is protected from unauthorized modification and the organization controls the software libraries that will eventually be placed on the CDS.

**CM 5 7 Access Restrictions for Change**

The intent of this control enhancement is to ensure that the CDS should have a mechanism in place to limit privileges to change software libraries. Documentation showing how and to what extent the organization limits privileges to change software resident within software libraries (including privileged programs), will be created and maintained.

**CM 6 2 Configuration Settings**

The intent of this control enhancement is to ensure corrective action is taken when unauthorized changes to CDS configuration settings are detected. The CDS should have automatic mechanisms in place that respond to unauthorized changes to defined configuration settings.

**CM 6 3 Configuration Settings**

The intent of this control enhancement is to ensure that unauthorized, security-relevant configuration changes are tracked, monitored, corrected, and available for historical purposes.

**CM 6 4 Configuration Settings**

The intent of this control enhancement is to ensure the CDS is configured in accordance with security configuration guidance prior to being put in a production environment.

The CDS should show conformance to security configuration guidance (i.e., security checklists), prior to being introduced into a production environment.

**CM 7 Least Functionality**

The intent of this control is to ensure that the CDS has mechanisms that are implemented by the site to enforce the concept of least functionality, thereby only allowing essential capabilities to be leveraged by entities that may access or use the CDS. The intent of this control is to also control the scope of damage to the system in the event of compromise and reduce the risk of system exploit by limiting the system to only providing essential capabilities.

The CDS should have a mechanism in place to restrict the capabilities and functions to those that are operationally required (in accordance with organizational policy). The CDS should be implemented to only allow access to or use of capabilities and functions which are operationally required by the site.

**CM 7 1 Least Functionality**

The intent of this control enhancement is to ensure that the site (implementing the CDS) periodically reviews the implementation of the CDS to document and eliminate unnecessary functions, ports, protocols, and/or services. The CDS should have a mechanism to support the periodic review of its configuration to document and eliminate unnecessary functions, ports, protocols, and/or services.

The site should have procedures and supporting policy in place to require period reviews of the CDS configuration to document and eliminate unnecessary functions, ports, protocols, and/or services.

**CM 7 2 Least Functionality**

The intent of this control enhancement is to ensure that the CDS has mechanisms (that are also implemented by the site) to ensure that defined software installation and usage restrictions are enforced, in accordance with this enhancement.

The CDS should have a mechanism to support definable software installation and usage restrictions, in accordance with this enhancement. The CDS should enforce defined, documented software installation and usage restrictions.

**CM 7 3 Least Functionality**

The intent of this control enhancement is to ensure that the site (implementing the CDS) complies with applicable registration requirements for ports, protocols, and services.

A mechanism should exist to document the CDS open, accessible, or usable ports, protocols, and services for the purposes of registration. Procedures and supporting policies should be in place to register CDS ports, protocols, and services in accordance with applicable registration requirements.

**CM 8 1 Information System Component Inventory**

The intent of this control enhancement is to ensure the site (implementing the CDS) keeps its inventory of Information System (IS) components throughout the course of CDS component installations, removals, and updates to limit the risk that unapproved hardware is used. The CDS should be tracked as an entity in an inventory of IS components.

The CDS should have a mechanism (e.g., physical serial number, labels) for tracking its components in an inventory of IS components. The site (implementing the CDS) should have procedures and supporting policy in place requiring that the inventory of IS components is kept up to date, through the course of CDS component installations, removals, and updates.

**CM 8 3 Information System Component Inventory**

The intent of this control enhancement is to ensure the CDS has a mechanism that is implemented by the site to appropriately detect and react to the addition of unauthorized components/devices in accordance with this enhancement.

The CDS should have a mechanism which detects the addition of unauthorized components/devices. The CDS should disable/prevent network access by such components/devices or will notify designated personnel. The site should implement automated mechanisms to detect the addition of unauthorized components/devices into the CDS. The site should implement automated mechanisms to disable/prevent network access by detected unauthorized components/devices or notifies designated site personnel.

**CM 9 Configuration Management Plan**

The intent of this control is to ensure the site (implementing the CDS) develops, documents, and implements a CM plan for or which includes the CDS. Development, documentation and implementation of the CM plan is in accordance with this control. This control is intended to ensure that no system, user, or security relevant data is lost in the event of the failure of a component of the CDS. The stored data should also have mechanisms to prevent an unauthorized person from being able to read or modify the data.

Critical user and system information will be backed up. Backups will be encrypted. The CDS should have some mechanism to validate their integrity of backups. The system will create backups containing the information in the documentation. Modified backup information will not be accepted and restored to the system.

Backup procedures should be in place and testing should occur on a regular basis. On-site personnel will understand the procedures for backup and recovery of the system. The organization should store the backups in a secure location. The organization should encrypt the backups if the system does not have such a feature built in. The site will have a documented configuration management (CM) plan in place for or which includes the CDS. The CM plan will be implemented in accordance with the specific requirements stated in this control.

**CM 9 1 Configuration Management Plan**

The intent of this control enhancement is to ensure the site (implementing the CDS) maintains proper separation of duties by ensuring that the development of the CM process is assigned to personnel who are not directly involved in CDS development.

The CM process development should be assigned to site personnel who are not directly involved in CDS development.

**CP 9 Information System Backup**

This control is intended to ensure that no system, user, or security relevant data is lost in the event of the failure of a component of the CDS. The stored data should also have mechanisms to prevent an authorized person from being able to read or modify the data.

Critical user and system information should be backed up. Backups should be encrypted. The CDS should have a mechanism to validate the integrity of backups. The system should create backups containing the information in the documentation. Modified backup information should not be accepted and restored to the system.

Backup procedures should be in place and testing should occur on a regular basis. The on-site personnel should understand the procedures for backup and recovery of the system. The organization should store the backups in a secure location. The organization should encrypt the backups if the system does not have such a feature built in. The site should have a documented configuration management (CM) plan in place for or which includes the CDS. The CM plan will be implemented in accordance with the specific requirements stated in this control.

**CP 9 1 Information System Backup**

This control enhancement is meant to ensure the organization is aware of problems with the backup solution by periodically testing that it is working properly, and to ensure that the integrity of the backup information has not been intentionally or unintentionally modified.

Site documentation should detail how to store and retrieve backup information. Site documentation should detail how often the system will need to be backed up to prevent loss of logging information. The organization should document the required frequency of backups. The organization should review the audit logs of backups to validate that they occur at the required frequency. The organization should restore backups to an alternate computer and verify the integrity at the required frequency.

**CP 9 2 Information System Backup**

This control enhancement is meant to ensure the organization is made aware of problems with the backup solution by periodically restoring a piece of the backup data.

Site documentation should detail how to store and retrieve backup information. The organization should have a contingency plan. The organization should test and validate the contingency plan on a regular recurring basis.

**CP 10 Information System Recovery and Reconstitution**

The intent of this control is to ensure comprehensive and effective continuity of all system functions during a broad spectrum of emergencies or situations that may disrupt normal operations (e.g., network intrusions, power failures, damage to facilities caused by storms, fires, flooding, etc.).

Document CDS resources required for duplication of operations, including hardware, software, applications, boundary defense devices, physical and environmental infrastructure, and personnel support. Establish system description documentation that identifies and prioritizes system functions by data type, criticality, or other operational criteria. Create a copy of the most recent business impact analysis, or similar document that describes the impact of an incident on

system resources and customers. Document a listing of key personnel associated with the system administration and operations. Establish disaster recovery procedures and plans that include the CDS.

**CP 10 2 Reconstitution**

The intent of this control enhancement is to ensure that transaction-based systems (e.g., database management systems, transaction processing systems) have implemented transaction rollback and transaction journaling, or technical equivalents.

Documentation will be created with a listing of transaction-based systems utilized within CDS. Documentation with a listing of transaction-based utilities and applications that support the DoD-required transaction rollback, transaction journaling or equivalent capabilities (e.g., Oracle Database, SQL Server, SAP, and a specialized OLTP product such as IBM CICS), will be created.

System documentation that describes system characteristics and functions to ensure that CDS has implemented transaction-based systems or transaction processing systems will be created.

**CP 10 4 Reconstitution**

The intent of this control enhancement is to ensure CDS data integrity is maintained during restoration operations by using disk images and protecting those images during transfer, storage, and retrieval.

Documentation will be created defining the operating system(s) and other critical software. The CDS components will be configured to scan image media upon insertion into the component and prior to data access. The CDS should have mechanisms to verify the integrity-protected disk images. The CDS should verify integrity-protected disk images prior to reimage. Policy mandating organization-defined time-periods required for CDS components to be reimaged will be created. Site policy mandating that the CDS disk images are configuration-controlled and integrity-protected will be created.

The site will configure the CDS to integrity-check image media prior to reimage, as defined by site policy. The CDS components will have integrity-check mechanisms in place during restoration. The organization's system security documentation will identify the type and location of physical assets (e.g., locked metal containers, rooms or spaces with lockable restricted-access doors, etc.) protecting backup and restoration assets. The organization will provide the capability to reimage information system components within organization-defined time-periods.

**CP 10 6 Reconstitution**

The intent of this control enhancement is to ensure that procedures are in place to assure the appropriate physical and technical protection of the backup and restoration hardware, firmware, and software.

The hardware, software, or firmware used for back up of data and all other CDS assets should be protected and ensured. A system security document that identifies the technical security controls (e.g., cryptographic key management, role-based access controls, etc.) used to protect backup, restoration assets, and media should be created.

**IA 2 3 Identification and Authentication**

The intent of this control enhancement is to ensure that CDS is capable of supporting multifactor authentication for local access to privileged accounts. Multifactor authentication is defined as two or more of the following types: something you know (e.g., password), something you have (e.g., CAC), something you are (e.g., biometric). Multifactor authentication does not include two factors of the same type (e.g., two passwords). From a CDS perspective, since this control is focused on local privileged user access, the privileged user should have two factors of

authentication to access the CDS via the console. See the comment section for the relationship to network based access (to/through the CDS).

The CDS should support multifactor authentication for local access by privileged accounts. The CDS should be configured to support the multifactor types of authentication that are required for privileged accounts. The CDS should enforce two different types of authentication factors for multifactor authentication of privileged accounts. The CDS should require multifactor authentication for local access to privileged accounts.

**IA 2 4 Identification and Authentication**

The intent of this control enhancement is to ensure that the CDS is capable of supporting multifactor authentication for local access to non-privileged accounts. Multifactor authentication is defined as two or more of the following types: something you know (e.g., password), something you have (e.g., CAC), something you are (e.g., biometric). Multifactor authentication does not include two factors of the same type (e.g., two passwords). From a CDS perspective, since this control is focused on local non-privileged user access, the privileged user should have two factors of authentication to access the CDS via the console. See the comment section for the relationship to network based access (to/through the CDS).

The CDS should support multifactor authentication for local access by non-privileged accounts. The CDS should be configured to support the multifactor types of authentication that are required for non-privileged accounts. The CDS should enforce two different types of authentication factors for multifactor authentication of non-privileged accounts. The CDS should require multifactor authentication for local access to non-privileged accounts.

**IA 2 5 Identification and Authentication**

The intent of this control enhancement is to ensure that the CDS does not allow for any type of group authentication at initial login. When the CDS allows for the use of group authenticators for roles (e.g., sysadmin, secadmin), the user must authenticate via their individual user account prior to assuming the role, which requires the group authenticator. For CDSs, group authentication does not apply outside of the defined roles that are associated with specific users (i.e., group authentication should never be used for user accounts).

A user should not be allowed to perform an initial logon to the system using a group authenticator. The CDS should force the user to authenticate to the system with their individual authenticator, prior to using the group authenticator to assume a role. The CDS should be configured to prevent console logon privileges to group accounts (roles). Site policy should prohibit the use of group accounts and the sharing of user IDs and passwords for the CDS. The CDS should be configured to associate only one role per user account.

**IA 2 8 Identification and Authentication**

The intent of this control enhancement is to ensure that network access to the CDS by enclave managed privileged accounts (e.g., remote management) or network access to privileged accounts resident on the CDS (e.g., remote logon) on the CDS is protected such that an attacker cannot capture authentication sessions and replay the sessions to gain unauthorized access to the CDS.

The CDS should not allow the replay of authentication sessions for privileged accounts that occur over the network. The CDS should implement mechanisms to protect the authentication credentials of privileged accounts sent over the network, when they are reused [not one-time authenticators]. The CDS privileged account protection mechanisms should effectively protect privileged account authenticators sent over the network. The CDS should provide multiple mechanisms to protect and prevent replay of privileged account authenticators sent over the network. The CDS should be configured to support site specific mechanisms to protect and

prevent replay of privileged account authenticators sent over the network.

**IA 2 9 Identification and Authentication**

The intent of this control enhancement is to ensure that on a CDS, non-privileged accounts should not remotely access the CDS directly; therefore, this control focuses on non-privileged user accounts in the enclave accessing the CDS over the network for the purposes of sending information through the CDS. The intent of this control is that this network access to the CDS by enclave managed non-privileged accounts is protected such that an attacker cannot capture authentication sessions and replay the sessions to gain unauthorized access to the CDS (for the purposes of sending information through the CDS).

The CDS should not allow the replay of authentication sessions for non-privileged accounts that occur over the network. The CDS should implement mechanisms to protect the authentication credentials of non-privileged accounts sent over the network, when they are reused [Not one-time authenticators]. The CDS non-privileged account protection mechanisms should effectively protect non-privileged account authenticators sent over the network. The CDS should provide multiple mechanisms to protect and prevent replay of non-privileged account authenticators sent over the network. The CDS should be configured to support site specific mechanisms to protect and prevent replay of non-privileged account authenticators sent over the network.

**IA 3 Device Identification and Authentication**

The intent of this control enhancement is to ensure that the CDS limits communication with devices to those devices that are authorized to communicate with it. For CDSs, a list of devices should be defined that are authorized to communicate with the CDS, along with the corresponding unique identification and authentication information. For example, if the CDS is an email CDS, the CDS should authenticate the email server to ensure it is authorized prior to allowing the connection from the server. Authentication should occur via IP address and an associated server certificate. In other instances, it may be required that the CDS is capable of uniquely documenting and authenticating external devices that are authorized to connect to it to , for instance, that the USB is an authorized USB device prior to reading data from the device or using the device (e.g., USB keyboard).

The CDS should provide the capability to define a list of authorized devices with which it should communicate. The CDS should associate unique identification and authentication information with each device. The CDS should correctly identify and authenticate each device before allowing further communication with the device.

**IA 3 1 Device Identification and Authentication**

The intent of this control enhancement is to ensure that the CDS allows for bidirectional authentication between devices when that connection is made remotely or wirelessly. The understanding is that the term remote implies that the device is not located on the local enclave; that the communication must traverse the wide area network. The CDS must be able to support cryptographic-based authentication with network devices prior to establishing a communication session with the device. This control is specific to network devices such as LDAP, email, or other such servers to which the CDS does not have a physical connection. In addition, some CDSs may require remote authentication to end user devices (e.g., tactical) that use the CDS to access information from various networks or transfer information across the CDS.

The CDS should support cryptographic authentication with network devices. The CDS should support bi-directional authentication with network devices. The CDS enforces the use of cryptographic authentication with network devices. The CDS should enforce bi-directional authentication with network devices.

**IA 3 2 Device Identification and Authentication**

The intent of this control enhancement is to ensure that the CDS allows for bidirectional authentication between devices located on the wired local enclave. The CDS must be able to support cryptographic-based authentication with network devices prior to establishing a communication session with the device. Essentially, this control and IA-3(1) should be tested the same as both controls involve network communication, whether remote, local, wireless, or wired.

The CDS should support cryptographic authentication with network devices. The CDS should support bi-directional authentication with network devices. The CDS should enforce the use of cryptographic authentication with network devices. The CDS should enforce bi-directional authentication with network devices. The CDS should be configured to require cryptographic authentication with network devices and to require bi-directional authentication with network devices.

**IA 4 4 Identifier Management**

The intent of this control enhancement is to ensure that the CDS is capable of distinguishing between users depending upon the organization's defined characteristics, if necessary. The CDS shall be capable of supporting organizationally generated unique user identifiers. For CDSs, the CDS shall also be able to distinguish between users and administrators (system administrators, security administrators, audit administrators).

The CDS should be capable of supporting organizationally generated unique user identifiers and distinguishing between users and administrators. The site should define the unique characteristics used to document users within their site policy. The site should have policies and procedures in place for establishing unique identifiers for CDS users.

**IA 5 Authenticator Management**

The intent of this control is to ensure that the CDS is capable of supporting and protecting user/device authenticators. Protection includes defined policies and procedures, revocation, changing default passwords upon installation, changing authenticators and protecting stored authenticators from unauthorized access. The details of those authenticators are covered in the control enhancements. The site should have policy and procedures in place that define the process for assigning, distributing, receiving and revoking authenticators.

The site policy and procedures should define the characteristics of the initial authenticator content for the CDS. The site policy and procedures should define the password complexity requirements that the CDS must be configured to enforce. The site policy and procedures should define the administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators. The site policy and procedures should require the CDS to be configured to require a user to change the content of their default/initial authenticator upon first logon. The site policy and procedures should define the minimum and maximum lifetime restrictions and reuse conditions for authenticators that the CDS must be configured to enforce. The site policy and procedures should define the time period at which authenticators must be changed. The site policy and procedures should provide instructions for users to follow to protect their authenticator from unauthorized disclosure and modification.

**IA 5 1 Authenticator Management**

The intent of this control enhancement is to ensure that when the CDS requires the use of a password for authentication, it applies strict guidelines on the passwords that should be used. The CDS should be configurable to enforce site policy for password complexity requirements and password update requirements (complexity, history, and frequency). The CDS must ensure that the passwords are stored and transmitted in an encrypted/protected form.

The CDS should be configurable to support complex passwords to include the use of upper-case, lower-case, numbers and special characters. The CDS should be capable of enforcing a minimum number of upper-case, lower-case, numbers and special characters for every password. The CDS should be configurable to support password establishment parameters to include restrictions against password reuse, the minimum and maximum lifetime of a password, and ensure the minimum number of characters that must be changed. The CDS should store all passwords in an encrypted/protected form. The CDS should encrypt all passwords prior to transmission to an external system/host.

**IA 5 2 Authenticator Management**

The intent of this control enhancement is to ensure that when the CDS requires the use of a certificate for PKI authentication, it validates, protects, and maps that certificate. The CDS should ensure that the certificate is associated with the corresponding user account that is attempting to authenticate. In addition, the CDS should ensure that the certificate is still valid (i.e., not expired, revoked, or marked invalid); ensure the certificate path is from an accepted trust point and that any intermediary trust points (sub certificate authorities) are valid. In cases where the CDS is responsible for storing private keys, the CDS must ensure the protection of the private key(s).

**IA 5 6 Authenticator Management**

The intent of this control enhancement is to ensure that the CDS stores authenticators in a location, and with the appropriate mandatory access controls (e.g., labels or type enforcement), of the classification in which the authenticator is used by the CDS. The site should have policy and procedures in place to instruct users/administrators on how to protect their authenticators.

The CDS should apply mandatory access controls to files/directories containing authenticators in accordance with the classification of information processed by the CDS and that users/administrators of the CDS are aware of the guidelines identified in site policy for protecting their authenticators. Also policy and procedures exist that provide instruction for the protection of user authenticators.

**IA 5 7 Authenticator Management**

The intent of the control enhancement is to ensure that authenticators used or validated by the CDS are not stored in an unencrypted or unprotected form on the CDS (either in configuration files, database stores, etc.). CDS applications or functions that use unencrypted authenticators must require that the authenticator be provided externally (outside of the application or function). In addition, the CDS must not use the encrypted form of the credential when performing authentication services, but rather, require the unencrypted credential to be communicated over a secure channel.

**IA 6 Authenticator Feedback**

The intent of this control is to ensure that the CDS should obscure feedback of authenticators for local and remote login.

**PE 3 4 Physical Access Control**

The intent of this control enhancement is to ensure that an unauthorized person cannot easily manipulate the physical hardware of the CDS. The documentation should clearly state the environments in which the system is expected be deployed also state that the system is to be placed in a lockable case. The case should not be easily opened without a token (e.g., a key). The token should be stored in a secure location (e.g., make sure the key is not taped to the top of the case). On site personnel should understand the procedures to lock and unlock the casing, including any audits that must be performed and where to retrieve and store the token. The CDS system should not be open to physical modification.

**PE 3 5 Physical Access Control**

The intent of this control enhancement is to ensure that an unauthorized person cannot easily manipulate the physical hardware of the CDS and that the CDS detects/reacts when the

hardware has been tampered with. The system shall stop processing data in the event that the hardware has been tampered with. The system should have tamper tape. The system should fail to process data if a piece of hardware, such as the network card, has been replaced.

**PE 5 Access Control for Output Devices**

The intent of this control is to ensure that CDS's when deployed the output devices shall be placed into secure areas that should prevent unauthorized access. Appropriate on site personnel should be aware of where all output devices are located. All output devices should be located where the organizational documentation states they should be. All of the systems physical output devices should be included in the system documentation.

**PL 2 2 System Security Plan**

The intent of this control enhancement is to document all internal interfaces, the information being exchanged, and the protection mechanisms associated with each interface from a functional architecture perspective. This control is intended to ensure sufficient information is provided to allow for testing the CDS functionality (transfer, access, and multi-level).

The vendor/site shall create the appropriate documentation that identifies the system architecture (including site specific architecture) and provides detailed security-related information, documentation that identifies system user roles required for access control, access privileges assigned to each role, and all unique system security requirements (e.g., encryption of data at rest) each category of sensitive information processed or stored by the system application, and its specific protection plan.

**RA 2 Security Categorization**

The intent of this control is to ensure that a specific relationship between the confidentiality, integrity, and availability, and the network that the CDS resides as well as the data processed by the CDS (subjects and objects) have been ascertained and are more readily recognized, differentiated and understood.

A security CONOPS, risk assessment policy, procedures addressing security categorization of organizational information and CDS, security planning policy and procedures, security plan, other relevant documents or records should be created and the Risk Assessment and/or Threat Analysis should contain security categorization. The organization should categorize information and the CDS in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The security categorization should be consistent with FIPS 199 and considers the provisional impact levels and special factors in NIST Special Publication 800-60. A security CONOPS or related documentation should be created ensuring the organization considers in the security categorization of the information system, potential impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level impacts. The organization should include supporting rationale for impact-level decisions as part of the security categorization.

The organization conducting the security categorization of the information system as an organization-wide exercise should include the involvement of senior-level officials including, but not limited to, authorizing officials, information system owners, chief information officer, senior agency information security officer, and mission/information owners. The designated, senior-level organizational official should review and approve the security categorizations. The authorizing official or authorizing official designated representative should review and approve the security categorization decision.

**RA 5 Vulnerability Scanning**

The intent of this control is to ensure the CDS is assessed on a regular basis and when necessary, for weaknesses. The CDS should have a documented and validated risk assessment policy,

procedures addressing vulnerability scanning, risk assessment, security plan, vulnerability scanning results, patch and vulnerability management records, and other relevant documents or records that mandate the frequency for conducting routine vulnerability scans. The CDS should have documented and validated software and hardware versioning information on the CDS. The CDS should be cross-referenced with known vulnerabilities. The CDS should have mechanisms in place to assess and mitigate weaknesses described by vulnerabilities and these should be documented. CDS's should have periodic vulnerability scans run against them and any issues identified must be addressed accordingly. On-site IA personnel should be trained in the use and maintenance of vulnerability scanning tools and techniques in order to conduct these scans appropriately.

**SA 4 6 Acquisitions**

The intent of this control enhancement is to ensure that this control should only be applied to cryptography within a CDS.

**SA 5 Information System Documentation**

The intent of this control is to ensure that the organization maintains documentation that describes the implementation and maintenance of information system security and that this information is readily available to authorized users. In addition, the intent of this control is to ensure that the organization is in compliance with the DoD Information Assurance Vulnerability Management (IAVM) program and that a written and signed compliance policy is put into effect. This control is intended to ensure that a comprehensive set of procedures are developed and used to test all patches, upgrades, and new AIS applications prior to deployment.

The CDS should have a documented and validated vulnerability management policy and/or standard operating procedures, administration documentation, user documentation, CM plan and/or SOPs that describe procedures for testing and implementing patches, updates, and new AIS applications, and SOPs for implementing security features for the CDS. The CDS should have documented system change requests and approvals readily available in accordance with site policy. Documentation distributed to users should be safeguarded. Logs of patching, troubleshooting and testing should be created and maintained.

**SA 5 1 Information System Documentation**

The intent of this control enhancement is to document the characteristics and capabilities of all of the protection mechanisms used in the CDS architecture and to ensure sufficient information is provided to allow for testing the CDS functionality (transfer, access, and multi-level). The CDS should have a documented and validated system architecture including detailed security-related information. There should also be procedure in place for testing CDS functionality.

**SA 5 2 Information System Documentation**

The intent of this control enhancement is to document the security-relevant external interfaces, the information being exchanged, and the protection mechanisms associated with each CDS interface from a functional architecture perspective. This control is intended to ensure sufficient information is provided to allow for testing the CDS functionality (transfer, access, and multi-level). The CDS should have a documented and validated system architecture including detailed security-related information. There should also be procedure in place for testing CDS functionality.

**SA 5 3 Information System Documentation**

The intent of this control enhancement is to document all external interfaces, the information being exchanged, and the protection mechanisms associated with each CDS interface from a functional architecture perspective. This control is intended to ensure sufficient information is provided to allow for testing the CDS functionality (transfer, access, and multi-level).

The CDS should have a documented and validated system architecture including detailed security-related information. The CDS should have validated documentation that identifies

system user roles required for access control, access privileges assigned to each role, all unique system security requirements (e.g., encryption of data at rest) each category of sensitive information processed or stored by the system application, and its specific protection plan (e.g., Privacy Act, HIPAA). There should also be procedure in place for testing CDS functionality.

**SA 5 4 Information System Documentation**

The intent of this control enhancement is to document all internal interfaces, the information being exchanged, and the protection mechanisms associated with each interface from a functional architecture perspective. This control is intended to ensure sufficient information is provided to allow for testing the CDS functionality (transfer, access, and multi-level).

The CDS should have a documented and validated system architecture including detailed security-related information. There should also be procedure in place for testing CDS functionality.

**SA 5 5 Information System Documentation**

The intent of this control enhancement is to ensure that all access to source code libraries is controlled to protect privileged programs and to prevent the introduction of unauthorized code. This control is intended to ensure that all required software development life cycle documentation is current and approved, and it reflects the use of code reviews and/or accepted software quality control practices that ensure the security of software source code.

The CDS should have a documented and validated CM plan which addresses software configuration management. It should include a list of software development life cycle documentation and DoD guidelines for documentation standards or content requirements. It should document the approval authority and approval requirements for the system documentation as well as the approval for the test plans that are identified by the IAM. The CDS should have documented the latest application test plans that address the security requirements specified in the referenced requirements document.

**SA 7 User-Installed Software**

The intent of this control is to ensure the on a CDS non-privileged users cannot install any software on the system.

**SA 10 Developer Configuration Management**

The intent of this control is to ensure that change controls for software development are in place to prevent unauthorized programs or modifications to programs from being implemented and ensure that change requests are subject to a review and approval process. Change controls for software development also include technical system features to assure that changes are executed by authorized personnel and are properly implemented.

The CDS should have a documented and validated CM plan and procedures and/or SOPs that describe procedures for testing and implementing patches, updates, and new AIS applications. The local terminology should be in the configuration management documentation. It should include a listing of development servers and a listing of active developer accounts; as well as a listing of developer accounts and their system access (i.e., access to tested and approved production code). Sample copies of system change requests and approvals should also be included as attachments to the plan. The IAM/IAO/ISSO should be defined, with contact information, within this documentation.

**SA 10 1 Developer Configuration Management**

The intent of this control enhancement is to ensure that the CDS has a documented list of current DoD information system hardware and software within the accreditation boundary. This should include the operating systems used.

**SA 11 Developer Security Testing**

The intent of this control is to ensure that the organization is in compliance with the DoD

Information Assurance Vulnerability Management (IAVM) program and that a written and signed compliance policy is put into effect. The CDS should have documented and validated vulnerability management policy and/or standard operating procedures.

**SA 11 3 Developer Security Testing**

The intent of this control enhancement is to ensure that all required software development life cycle documentation is current and approved, and it reflects the use of code reviews and/or accepted software quality control practices that ensure the security of software source code.

The CDS should have software development life cycle documentation and DoD guidelines for documentation standards or content requirements. The documentation should include the approval authority and approval requirements for the system documentation.

**SC 5 1 Denial of Service Protection**

The intent of this control enhancement is to ensure the system limits the ability of a compromised system service from disrupting any other system on the network using a denial of service attack.

The system should deny processes access to the network if the access is not explicitly required for functionality, e.g., use of a firewall, or by limiting a process's access rights. The system should only allow a user to execute programs with network access if explicitly required. Users should not have the ability to create executable scripts on the system unless explicitly needed for their role. The CDS should have documented and validated policy that ensures the system does have mechanisms to restrict DoS attacks.

**SC 5 2 Denial of Service Protection**

The intent of this control enhancement is to ensure the CDS is able to perform any required network functionality even in the event that the system is flooded with information over the network.

The CDS should have documented and validated policy ensuring that The system should load balance multiple connections on each interface.

**SC 7 12 Boundary Protection**

The intent of this control enhancement is to ensure that all capable components in the CDS architecture have protection mechanisms, such as firewalls, access control lists, and system networking configurations, in use to reduce ability of an external system from compromising the system.

The CDS firewall should be active at system start up. The firewall should only allow input on the ports and/or protocols necessary to meet the system objectives. The firewall should only allow output on the ports and/or protocols necessary to meet the system requirements.

**SC 7 15 Boundary Protection**

The intent of this control enhancement is to ensure all traffic is audited to assist with after the fact investigation in the event of a process failure or compromise, and to limit the ability of any privileged process from unrestricted communications with an external network.

The system should have a dedicated interface for management. Only the dedicated interface should be used for management. The user should not modify the system to allow one of the other interfaces to be used for management. Access to the management interface should be audited.

**SC 7 16 Boundary Protection**

The intent of this control enhancement is to ensure the CDS has mechanisms in place to limit the ability of an attacker to discover components and/or devices that are part of the management interface. As part of defense in depth, this enhancement provides another restriction that an

attacker must overcome in order to discover information that could lead to system compromise.

The system should not publish the hostnames of its managed interfaces to a network naming service. The system should not publish service information to the network regarding its management interface(s). The system should conduct periodic changes to the IP addresses in order to counter spillages and leaks as to the IP. All ports on the system that can be used to document functions should be closed to systems on the network. The required network services should not relay any more information than necessary to unauthenticated entities. The system should not respond to ICMP requests unless explicitly required.

**SC 7 17 Boundary Protection**

The intent of this control enhancement is to ensure that an organization has mechanisms in place to help reduce the risk that a system on the internal network could be compromised and to reduce the ability of a compromised node from passing data outside of the network by enforcing a strict protocol format that should be validated. To ensure the system only allows traffic that is correctly formatted egress.

The system should use a protocol with a strict format. The system should use only the validated and approved formats. The organization should have the technology to validate the formats used by the system. The mechanisms used to enforce format adherence should in use at all times during production and testing. The site administrative or IA personnel should understand how to configure the system to use only the allowed formats.

**SC 7 18 Boundary Protection**

The intent of this control enhancement is to ensure the CDS has mechanisms enabled to deny unauthorized access and to prevent external information exchange in the event of a system failure, and to ensure the system fails secure in the event of system failure.

The system should stop processing data if the firewall stops or is shutdown also it should have documented and validated policy for boundary devices to ensure that in the event of failure It should not be exposed to unfiltered traffic. The site administrative or IA personnel should understand how to properly configure the boundary devices. The site administrative or IA personnel should understand what messages or alerts to look for to know that a boundary device has failed.

**SC 8 Transmission Integrity**

The intent of this control is to ensure the CDS has mechanisms in place to prevent external modification of data when exchanged between systems.

The system should validate the integrity of all information transmitted to and from the system. The CDS should also have documented and validated policy ensuring the system uses integrity measures on data exchanges. The network topology of the network and The system should be deployed in a manner that ensures the measures used are acceptable for the risk of that environment.

**SC 9 Transmission Confidentiality**

The intent of this control is to ensure the CDS has mechanisms in place to prevent an external device from reading data exchanged between the systems. The system should be deployed in a trusted environment. It should encrypt all information transmitted to and from the system. It should not accept unencrypted data. Also to validate that there is a functional cryptographic key management program.

The CDS should have documented and validated that ensures the systems uses confidentiality measures on data exchanges. The network topology of the network and The system should be deployed in a manner that ensures the measures used are acceptable for the risk of that

environment.

**SC 13 Use of Cryptography**

The intent of this control is to ensure the crypto system properties and the secrecy and authenticity requirements protect the CDS in compliance with federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

- i) Crypto system properties : de/encryption transformations must be efficient, system is easy to use, the security of the system should depend only on the secrecy of the de/encryption transformations
- ii) Secrecy requirements: if both plaintext and cipher text are known, it should be computationally infeasible [present and future] to document the deciphering algorithm; it should be computationally infeasible to systematically document plaintext from intercepted cipher text
- iii) Authenticity requirements: if cipher text and plain text are known, it should be computationally infeasible to document the enciphering algorithm; it should be computationally infeasible to find valid cipher text

**SC 13 1 Use of Cryptography**

The intent of this control enhancement is to protect government information that does not have a Restricted, Confidential, Secret, or Top Secret classification that is processed by the CDS.

The CDS should have documented and validated policy that mandates, at a minimum, uses FIPS-validated cryptography to protect unclassified information on the CDS.

**SC 13 2 Use of Cryptography**

The intent of this control enhancement is to protect government information that has a Restricted, Confidential, Secret, or Top Secret classification and that is processed by the CDS.

The CDS should employ NSA-approved cryptography to protect classified information and have documented and validated security related documents mandating use of NSA-approved cryptography.

**SC 13 3 Use of Cryptography**

The intent of this control enhancement is to ensure information in processed by the CDS at the same classification level, but which must be separated for need-to-know reasons, is encrypted, at a minimum, and meets requirements specified in FIPS 140-2 cryptography.

The CDS should have documented and validated security related documents mandating FIPS-validated cryptography to protect information when such information must be separated from individuals who have the necessary clearances yet lack the necessary access approvals

**SC 13 4 Use of Cryptography**

The intent of this control enhancement is to state that NIST FIPS 140-2 validated cryptography (e.g., DoD PKI class 3 or 4 token) is used to implement digital signatures (e.g., ECDSA, DSA, RSA) on the CDS.

The CDS should have documented and validated security related documents mandating use FIPS-validated and/or NSA-approved cryptography to implement digital signatures.

**SC 15 Collaborative Computing Devices**

The intent of this control is to ensure that collaborative computing technologies interacting with the CDS incorporate security capabilities (e.g., I&A, access control, auditing). The collaborative computing technologies should not allow a user to see and hear another user's workstation area, or to read, modify, and delete any information on or accessible to a user's workstation.

The CDS should have documented and validated security related documents to ensure that the

organization prohibits remote activation of collaborative computing devices, excluding the organization-defined exceptions where remote activation is to be allowed.

**SC 15 1 Collaborative Computing Devices**

The intent of this control enhancement is to ensure that collaborative computing devices should be easily disconnected from the CDS.

**SC 15 2 Collaborative Computing Devices**

The intent of this control enhancement is to document if the CDS or supporting environment blocks both inbound and outbound traffic between instant messaging clients that are independently configured by end users and external service providers. The CDS should have validated security related documents.

**SC 15 3 Collaborative Computing Devices**

The intent of this control enhancement is to document if the organization defines the secure work areas where collaborative computing devices are prohibited; and the organization disables or removes collaborative computing devices from information systems in organization-defined secure work areas.

**SC 16 Transmission of Security Attributes**

The intent of this control is to ensure the transmission of security attributes with data processed by the CDS. Security Parameters is defined as the highest classification and all appropriate associated security markings of the information processed.

The CDS should have automated mechanisms supporting reliable transmission of security parameters between information systems. The CDS should automatically and reliably associate security attributes with information that is exchanged between itself and other systems.

**SC 16 1 Transmission of Security Attributes**

The intent of this control enhancement is to ensure the CDS implements parity checks and cyclic redundancy checks (CRCs) for incoming and outgoing files, assures the integrity of all transmitted information including labels and security parameters and detects/prevents the hijacking of a communication session (e.g., covert communication channels). The CDS should automatically and reliably validate the integrity of security attributes that are associated with the information that it exchanges with the organization's other systems.

**SC 17 Public Key Infrastructure Certificates**

The intent of this control is to ensure the certificate should be used to ensure that a public key belongs to an individual/organization.

The CDS should have documented and validated security related documents that define a certificate policy for issuing public key certificates, and that the organization issues public key certificates under the organization-defined certificate policy or provides public key certificates under a certificate policy from an approved service provider.

**SC 18 Mobile Code**

The intent of this control is to ensure that policy and procedures related to mobile code address preventing the development, acquisition, or introduction of unacceptable mobile code within the CDS.

**SC 18 1 Mobile Code**

The intent of this control enhancement is to address the security concerns with regard to mobile code (executable content) by reliable executable content scanning detection and correction. This should include the use of mobile code that is digitally signed (document the author), constrained by the browser so that the privileges granted to the mobile code would be based on who signed the code/content and tools to search for signatures of known malicious mobile code (analogous to anti-viral software).

The CDS should have reliable executable content scanning detection and monitoring capabilities

for mobile code authorization. The system should have the capability to implement detection and inspection mechanisms to document unauthorized mobile code and the takes corrective action when unauthorized mobile code is identified. The CDS should have a documented and validated system and communications protection policy, procedures addressing the authorization, monitoring, and control of mobile code within the CDS, other relevant documents or record.

**SC 18 2 Mobile Code**

The intent of this control enhancement is to address the security concerns when acquiring developing or using mobile code or executable content on the CDS by preventing hostile mobile code or executable content from introducing malicious code, modifying/corrupting data, allowing unauthorized access to a system, or denying service.

The CDS should have a documented and validated system and communications protection policy, procedures addressing the organization defined requirements for the acquisition, development and/or use of mobile code.

**SC 18 3 Mobile Code**

The intent of this control enhancement is to prevent hostile mobile code or executable content by ensuring that only authorized mobile code or executable content by use of, for example, digitally signed code and/or tools that search for signatures of known malicious mobile code. The CDS should have automated mechanisms preventing download and execution of prohibited mobile code (e.g., digital signatures).

The CDS should have a documented system and communications protection policy, procedures addressing mobile code, mobile code usage restrictions, mobile code implementation policy and procedures, CDS design documentation, CDS configuration settings and associated documentation; CDS audit records, other relevant documents or records.

**SC 18 4 Mobile Code**

The intent of this control enhancement is to ensure the CDS prevent the downloading of mobile code or executable content where there is no operational need. The CDS should implement automated mechanisms preventing mobile code execution.

The CDS should have a documented and validated system and communications protection policy, procedures addressing mobile code, mobile code usage restrictions, CDS design documentation, CDS configuration settings and associated documentation, list of applications for which automatic execution of mobile code must be prohibited, list of actions required before execution of mobile code, other relevant documents or records.

**SC 19 Voice Over Internet Protocol**

The intent of this control is to establish VoIP policy to mitigate potential damage to the CDS if VoIP is maliciously exploited.

The CDS should have a documented and validated system and communications protection policy, procedures addressing VoIP, VoIP usage restrictions, other relevant documents or records.

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

The intent of this control is to ensure the origin authentication of DNS data, data integrity and authenticated denial of existence. This should include cryptographic keys and digital signatures for the verification of the authenticity and integrity of its data. Add support for cryptographically signed responses and support securing zone transfer information.

The CDS should provide automated mechanisms implementing secure name/address resolution service (authoritative source). The CDS should have a documented and validated system and

communications protection policy, procedures addressing secure name/address resolution service (authoritative source), CDS design documentation, CDS configuration settings and associated documentation.

**SC 20 1 Secure Name /Address Resolution Service (Authoritative Source)**

The intent of this control enhancement is to ensure the CDS identifies the signing key of a delegated zone and when the CDS has securely provided a public key high in the DNS hierarchy. It should follow the chain to data in child zones so that the integrity of DNS data is protected.

The CDS should have automated mechanisms implementing child subspace security status indicators and chain of trust verification for resolution services. The CDS should have a documented and validated system and communications protection policy, procedures addressing secure name/address resolution service (authoritative source), CDS design documentation, CDS configuration settings and associated documentation, other relevant documents or records.

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

The intent of this control is to limit exposure of spoofing attacks that try to induce the name server to cache false resource records, and could lead unsuspecting users to unsavory sites. If the resolving server were to be compromised or its cache-poisoned, the advertising server's authoritative zone information would be unaffected, thus limiting the potential damage.

The CDS should have automated mechanisms implementing data origin authentication and integrity verification for resolution services. The CDS should have a documented and validated system and communications protection policy, procedures addressing secure name/address resolution service (recursive or caching resolver), CDS design documentation, CDS configuration settings and associated documentation, other relevant documents or records.

**SC 21 1 Secure Name /Address Resolution Service (Recursive or Caching Resolver)**

The intent of this control enhancement is to maintain chain of trust between both the recursive name servers and the communication channels between itself and those name servers (e.g., SIG(0), TSIG, or IPsec).

The CDS should have automated mechanisms implementing data origin authentication and integrity verification for resolution services. The CDS should have a documented and validated system and communications protection policy, procedures addressing secure name/address resolution service (recursive or caching resolver), CDS design documentation, CDS configuration settings and associated documentation, other relevant documents or records.

**SC 22 Architecture and Provisioning for Name/Address Resolution Service**

The intent of this control is to improve availability by eliminating single points of failure and to enhance redundancy while ensuring that the CDS only processes name/address resolution.

The CDS should have a documented and validated the system and communications protection policy, procedures addressing architecture and provisioning for name/address resolution service, access control policy and procedures, CDS design documentation, assessment results from independent, testing organizations, CDS configuration settings and associated documentation, other relevant documents or records.

**SC 23 Session Authenticity**

The intent of this control is to establish grounds for confidence at each end of a communications session in the ongoing identification of the other participants and to validate the information being transmitted.

The CDS should have automated mechanisms implementing session authenticity. Parity checks / cyclic redundancy checks (CRCs) mechanisms should be in place on the CDS to assure the

integrity of all transmitted information (including labels and security parameters) and to detect or prevent the hijacking of a communication session (e.g., encrypted or covert communication channels). The CDS should have a documented and validated system and communications protection policy, procedures addressing session authenticity, CDS design documentation, CDS configuration settings and associated documentation; other relevant documents or records.

**SC 23 1 Session Authenticity**

The intent of this control enhancement is to prevent the CDS from being used to impersonate a legitimate user/process and perform actions on their behalf allowing an attacker to view or alter data, and to perform unauthorized actions.

The CDS should have automated mechanisms implementing session identifier invalidation upon session termination (e.g., cookie expiration). The CDS should have a documented and validated system and communications protection policy, procedures addressing session authenticity, CDS design documentation, CDS configuration settings and associated documentation, other relevant documents or records.

**SC 23 2 Session Authenticity**

The intent of this control enhancement is to ensure the authentication processes is easily terminated to prevent a user/process from successfully masquerading as another and thereby gaining unauthorized access.

The CDS should have automated mechanisms implementing logout capability for web pages requiring user authentication.

**SC 23 3 Session Authenticity**

The intent of this control enhancement is to document the current interaction session.

The CDS should have automated mechanisms generating and monitoring unique session identifiers. The CDS should have a documented and validated system and communications protection policy, procedures addressing session authenticity, CDS design documentation, CDS configuration settings and associated documentation, other relevant documents or records.

**SC 23 4 Session Authenticity**

The intent of this control enhancement is to ensure the stochasticity of CDS identifiers protection against brute-force attacks. The CDS should have automated mechanisms generating unique session identifiers. The CDS should have a documented and validated system and communications protection policy, procedures addressing session authenticity, CDS design documentation, CDS configuration settings and associated documentation, other relevant documents or records for organization defines requirements for randomly generating unique session identifiers.

**SC 24 Fail in Known State**

The intent of this control is to ensure the integrity of the system state is protected by preventing a loss of confidentiality, integrity, and availability in the event of a failure of the CDS or a component of the system.

The CDS should have automated mechanisms implementing fail-in-known-state capability. The CDS should have a documented and validated system and communications protection policy; procedures addressing CDS failure, CDS design documentation, CDS configuration settings and associated documentation, list of failures requiring the CDS to fail in a known state, state information to be preserved in system failure, other relevant documents or records.

**SC 25 Thin Nodes**

The intent of this control is to reduce the need to secure every user endpoint, and to reduce the exposure of information, the CDS, and services to a successful attack.

The CDS should have a documented and validated system and communications protection policy, procedures addressing use of thin nodes, CDS design documentation, CDS configuration settings and associated documentation, other relevant documents or records.

**SC 26 Honeypots**

The intent of this control is to detect, deflect, and analyze malicious attacks on the CDS.

The CDS may include components specifically designed to be the target of malicious attacks for the purpose of detecting, deflecting, and analyzing such attacks. The CDS should have a documented and validated system and communications protection policy, procedures addressing use of honeypots, CDS design documentation, CDS configuration settings and associated documentation, other relevant documents or records.

**SC 26 1 Honeypots**

The intent of this control enhancement is to ensure the CDS poses as a client and interacts with servers to examine whether an attack has occurred.

The CDS should have automated mechanisms proactively seeking Web-based malicious code. Document and review system and communications protection policy, procedures addressing use of honeypots, access control policy and procedures, boundary protection procedures, CDS design documentation, CDS configuration settings and associated documentation, other relevant documents or records.

**SC 27 Operating System-Independent Applications**

The intent of this control is to promote portability and reconstitution on different platform architectures, increasing the availability for critical functionality within an organization while the CDS with a given operating system is under attack.

The CDS should include an organization-defined operating system-independent processes document and review system, as well as a communications protection policy, procedures addressing operating system-independent applications, CDS design documentation, CDS configuration settings and associated documentation, and a list of operating system-independent applications.

**SC 28 Protection of Information at Rest**

The intent of this control is to maintain the confidentiality and integrity protections of non-mobile CDS devices provided by primary data storage onto secondary storage devices.

The CDS should have automated mechanisms implementing confidentiality and integrity protections for information on secondary storage devices. The CDS should have a documented and validated system and communications protection policy, procedures addressing protection of information at rest, CDS design documentation, CDS configuration settings and associated documentation, cryptographic mechanisms and associated configuration documentation, and a list of information at rest requiring confidentiality and integrity protections.

**SC 28 1 Protection of Information at Rest**

The intent of this control is to ensure cryptography is used to protect stored information within the CDS.

The CDS should have cryptographic mechanisms implementing confidentiality and integrity protections for information at rest (e.g., hash, encryption). The CDS should have a documented and validated system and communications protection policy, procedures addressing protection of information at rest, CDS design documentation, CDS configuration settings and associated documentation, and cryptographic mechanisms with associated configuration documentation.

**SC 31 Covert Channel Analysis**

The intent of this control is to ensure unauthorized information does not flow across security

domains. The CDS developers/integrators should perform a covert channel analysis.

**SC 32 Information System Partitioning**

The intent of this control is to provide system integrity through logical/physical isolation.

The CDS should be partitioned into components residing in separate physical domains (or environments) as deemed necessary by relevant documents or records. The CDS should have a documented and validated system and communications protection policy, CDS design documentation; CDS configuration settings and associated documentation, CDS architecture; list of CDS physical domains (or environments), CDS facility diagrams, other relevant documents or records.

**SC 33 Transmission Preparation Integrity**

The intent of this control is to protect the CDS from malicious and/or unintentional modification at information aggregation or protocol transformation points.

The CDS should enforce transmission integrity capability. The CDS should have a documented and validated system and communications protection policy, procedures addressing transmission integrity, CDS design documentation and CDS configuration settings with associated documentation.

**SC 34 Non-Modifiable Executable Programs**

The intent of this control is to provide non-modifiable storage to ensure the integrity of the CDS from the point of creation of the read-only image.

The CDS should load and execute the operating environment from hardware-enforced, read-only media and applications from hardware-enforced, read-only media.

**SC 34 1 Non-Modifiable Executable Programs**

The intent of this control enhancement is to eliminate the possibility of malicious code insertion via persistent, writable storage within the designated information system component.

The CDS should not have removable writable storage that is persistent across component restart or power on/off.

**SC 34 2 Non-Modifiable Executable Programs**

The intent of this control enhancement is to protect the integrity of information to be placed onto read-only media and to control the media after information has been recorded through a combination of prevention and detection/response measures.

The CDS should have a combination of protection measures, that provide both prevention and detection/response, that protects the integrity of information placed onto read-only media and controlling the media after information has been recorded onto the media.

**SI 3 Malicious Code Protection**

The intent of this control applies to both the transfer of malicious code and the ability of each CDS component to self-protect itself from malicious code. This control states that the CDS and its components protect themselves and the networks they connect to from malicious code. Protection of the networks that CDS connect to requires that the data being passed between networks is free from malicious code. The malicious code mechanism that the CDS engine uses must be kept up to date so that it should detect newly defined malicious code. The vendor must provide procedures so that the site should update the CDS.

The CDS must scan all data (or at a minimum, depending upon the system, data that traverses from the low to the high domain) as part of the data filtering path. [This includes malicious code within messages and attachments.] In addition, the CDS components must periodically scan the resident data (files, processes, etc). The CDS must block and/or quarantine or remove any

data that contains malicious code in addition to alerting administrators. The CDS must be capable of monitoring its processing for malicious code to the CDS so that the CDS is not overwhelmed or reaches its threshold when processing malicious code which may indicate a denial of service attempt or attempts to overload the CDS and bypass the malicious code scan.

The CDS procedures defined by the vendor should be effective in correctly updating the CDS malicious code definition files. The CDS should continue to scan the data as configured when the malicious code definition files have been updated. The CDS should be able to block, quarantine, and/or remove data containing malicious code. (both on each component and data traversing) The CDS should alert administrators when malicious code is detected in a data transfer. The CDS should monitor its processing threshold to detect abnormalities in malicious code processing.

**SI 3 1 Malicious Code Protection**

The intent of this control enhancement is to ensure the organization has a central management structure for malicious code mechanisms and that the organization includes the CDS in the central management policy/structure. The organization should have policies and procedures in place to manage and maintain the CDS malicious code protections. The organization is the site.

The site should have policies and procedures in place to manage and maintain the CDS malicious code protections. The site should have policies and procedures that define the conditions under which malicious code mechanism updates should be applied to the CDS (Note: procedures should include definition of the appropriate C&A approval process requirements prior to application of any update).

**SI 3 2 Malicious Code Protection**

The intent of this control enhancement is to ensure that automatic updates to the CDS malicious code signature/definition files are verified (i.e., from a valid source and the integrity of the data) prior to application on the CDS and that they are correctly applied to the CDS. For a CDS, automatic updates of the agent code should not occur. Verification of the malicious code signature definition files should include testing and validation. For a CDS, it is important that automatic updates are provided by a trusted source operating in the high side or controlling domain and that these updates are provided over a protected channel (e.g., encrypted). Site policy must also dictate that CDS malicious code protection signature/definition file updates be validated prior to placement on the high side trusted source and ultimate use by the CDS.

The CDS should reject automatic malicious code updates from invalid sources and validate the integrity of the automatic malicious code updates prior to applying the updates. The CDS should communicate with the malicious code update source via a protected channel. The CDS should not allow automatic updates of the malicious code agents.

**SI 3 3 Malicious Code Protection**

The intent of this control enhancement is to ensure users are not able to shut off or alter the configuration of malicious code mechanisms that are used by the CDS or resident on CDS components. This control applies to both the malicious code mechanisms used to check for the transfer of miscode and the self-protection malicious code mechanisms resident on the CDS components. This includes the ability to directly shut down malicious code scanning processes. Certain data paths may not be required to perform malicious code scanning. In these instances, it would be considered a configuration item that must be performed by an authorized administrator.

The CDS should restrict access to the configuration of its malicious code mechanisms used in the data filtering path to authorized administrators. The CDS components should restrict access

to the configuration of self-scanning malicious code mechanisms to authorized administrators. The CDS should not allow malicious code mechanisms and processes used in the data path to be shut off and the CDS components should protect self-scanning malicious code mechanisms and processes from being shut off.

**SI 3 4 Malicious Code Protection**

The intent of this control enhancement is to ensure that, when the CDS malicious code definition files are updated, they are updated by authorized administrators only. Updates to the virus definition files are the only allowable update. New versions of the scanning software would need to be included in updated CDS releases and vetted through the appropriate C&A process. The CDS virus definition files, used during data flow filtering, should only be updated by an authorized administrator.

**SI 3 5 Malicious Code Protection**

The intent of this control enhancement is to protect the CDS from malicious code that may be present on the removable media. This control implies that the CDS should protect itself from the introduction of removable media as a means of protection. Users should not be allowed to connect/insert removable media. Administrators may connect/insert removable media as necessary to administer the CDS. However, the CDS and its components should not auto mount/execute removable media.

The CDS components should restrict the mounting of media to only authorized administrators. The CDS components should restrict the execution of code on removable media to only authorized administrators. The CDS components should require human interaction to mount removable media when introduced to the system. (no auto mount) The CDS components should require human interaction to execute code on removable media when introduced to the system. (no auto execute) The CDS components should perform a scan of removable media upon insertion in to the component and prior to data access.

**SI 3 6 Malicious Code Protection**

The intent of this control enhancement is to ensure the CDS is capable of detecting malicious code in both transfers through the system and on the CDS components. This control also covers the alerting of detected benign malicious code. The control specifically focuses on benign mechanism, which is generally a consideration in the operational environment, where malicious code could cause undo harm to the system and propagate throughout the site's enclave.

The CDS should have a mechanism to scan data that passes through the CDS for malicious code. The CDS should detect malicious code and shell code in all low to high domain data transfers. [This includes malicious code within messages and attachments.] The CDS should detect malicious in all high to low domain data transfers [this includes malicious code within messages and attachments.] The CDS should have a mechanism to self-scan, on a periodic basis, the components making up the CDS for malicious code, mobile code and unauthorized shell code. The CDS components should detect malicious code that is resident on each component. The CDS should block, quarantine, and/or remove data containing malicious code. (both on each component and data traversing) The CDS should alert administrators when malicious code is detected in a data transfer. The CDS's configuration for malicious code detection should be enabled for all data flows. The CDS components should be configured to self-scan for malicious code at regular intervals according to the site scanning policy.

**SI 4 Information System Monitoring**

The intent of this control is to alert on detected activity related to the modification of all security mechanisms within the CDS. This is a very broad set of events that the system needs to monitor. For each mechanism that should be modified within the CDS, SI-4 is responsible for monitoring that mechanism and alerting when a modification or an attempt to modify has occurred. The intent of this control is to ensure that the CDS is capable of monitoring for

activity that would indicate an attack against the CDS and its components. This includes remote or local attacks. Attacks should be unauthorized attempts to access or use the system.

The CDS should monitor the integrity of security-related files and processes [e.g., virus scanning, dirty word filters, identification and authentication, etc. Note: this list must be based on the SRTM for the system that maps the mechanisms to the controls.] The CDS should notify security personnel when a security-related event occurs [e.g., user accounts have been locked due to unsuccessful logon attempts]. The CDS should alert security personnel of modifications to the security mechanisms [e.g., iptables Configuration, Access Control Lists, CDS filters configurations, etc.]. The CDS should notify security personnel when security mechanisms are disabled.

**SI 4 1 Information System Monitoring**

The intent of this control enhancement is to ensure that the CDS is comprehensively covered with respect to monitoring and alerting, such that each component within the CDS implements intrusion detection. In addition, the CDS implementation uses common protocols to ensure integration and analysis where necessary not only between CDS components, but with enclave solutions.

The CDS intrusion detection mechanisms should use standard, non-proprietary protocols, to communicate intrusion events within the CDS. The CDS intrusion detection mechanisms should use standard, non-proprietary protocols, to communicate intrusion events to enclave aggregation systems. The CDS should not provide CDS sensitive information to enclave systems, in accordance with defined security policy. Each CDS component should implement and enable intrusion detection mechanisms. The CDS should not provide CDS information to the low-side enclave.

**SI 4 2 Information System Monitoring**

The intent of this control enhancement is to ensure the CDS provides the necessary tools to interpret event data. This control also covers the gathering and potentially centralizing of data (internally and/or externally) to support further analysis.

The CDS components should provide mechanisms for administrators to read and interpret event data. [e.g., CDSs should provide a capability to read trusted operating system audit data. Depending upon the CDS, this could also apply to other mechanisms that capture event data.] The CDS components should provide a capability to search event data based on specified event information [e.g., date, time, subject, object, event, result, etc.] This should be used to correlate data and conduct data mining by incident responder/SOC/CIRT/auditor personnel. The CDS should provide mechanisms to centrally collect event data, in near real-time, from its components. The CDS provides mechanisms to centrally review, in near real-time, event data from its components. The CDS should provide event data to enclave systems, when permitted by security policy. The CDS should not provide CDS sensitive information to enclave systems, in accordance with defined security policy. The administrators should be trained to use the CDS mechanisms provided to read and interpret event data. The administrators should be trained to use the CDS mechanisms provided to locate specified event information within the log files. The CDS should be configured to centrally collect event data, in near real-time, from its components. This should be done through the use of a SIEM/SIM tool, when possible. The CDS should be configured to centrally review, in near real-time, event data from its components. This should be done through the use of a SIEM/SIM tool, when possible. The CDS components should be configured to send their event data to a centrally managed location. The CDS should be configured to provide event data to the enclave [excluding sensitive information], when permitted by security policy.

**SI 4 3 Information System Monitoring**

The intent of this control enhancement is to ensure the CDS provides the ability for its security mechanisms to communicate and interact with each other. The intrusion detection mechanism employed by the CDS should be able to interact with the mechanisms responsible for performing access control and flow control processing of the communications/data attempting to traverse the CDS. This interaction among security mechanisms should make it possible for the CDS to accurately recognize and respond to attempts to attack the CDS or the connected enclaves. In the case of CDS, the CDS may shut down a specific flow if an attack is detected. For CDS, the reconfiguration allows disabling of data flows, but not a partial reconfiguration of the data flow, depending upon policy.

The CDS should be designed and configured to allow the security mechanisms [e.g., access control and flow control] to interact with the intrusion detection mechanism. The CDS's intrusion detection mechanism should be able to document attacks based on alerts provided by the CDS security mechanisms. The CDS's security mechanisms should respond to alerts provided by the intrusion detection mechanisms in accordance with the security policy. The CDS's intrusion detection mechanism configuration should be modifiable only by authorized administrators. The inter-process communication between the security mechanisms and the intrusion detection system should be protected. The inter-process communication from the intrusion detection system should be validated prior to execution of a response. The CDS should be capable of and configured to disable data flows, per site policy. The CDS should be configured to alert administrators in the case of a data flow shutdown. The site policy should define the response procedures to be executed by administrators in the event of an alert.

**SI 4 4 Information System Monitoring**

The intent of this control enhancement is to ensure that the CDS has a screening mechanism(s) to monitor the incoming and outgoing data on all of its network communication interfaces. The mechanism should be able to distinguish traffic as authorized (i.e., allowable traffic from an authorized source or to an authorized destination) or unauthorized (unallowable traffic and/or unauthorized source/destination). The CDS should ensure that only allowable protocols over allowable ports are permitted. The CDS should also implement a threshold to protect against repeated attack attempts. In the case of certain monitoring, such as for malicious code, the monitoring should occur before the network traffic is allowed to traverse the CDS. The prevention of CDS traversal implies that the Malcode scans occur before the network traffic is regraded by the trusted subject.

The CDS should document incoming network traffic as being from an authorized source. The CDS should document the source of incoming network traffic and ensure that it is from an unauthorized source. The CDS should document the destination of outgoing network traffic and ensure that it is an authorized destination [host/enclave/etc.]. The CDS should document outgoing network traffic as being destined for an unauthorized destination [host/enclave/etc.]. The CDS should be capable of documenting and restricting inbound communications to only allowed ports and protocols, as defined by policy. The CDS should be capable of documenting and restricting outbound communications to only allowed ports and protocols, as defined by policy. The CDS should document network traffic that contains malicious code, and should prevent it from traversing the CDS. The CDS should not insert malicious code into an incoming/outgoing data flow. The CDS should document outgoing traffic that is not authorized for release to destination host/domain, and should prevent it from being sent to the destination. The CDS should implement a mechanism to monitor the number of unauthorized activities to ensure that it should detect when actions have exceeded the allowed threshold. The screening mechanism should only be modified by an authorized, privileged user.

**SI 4 5 Information System Monitoring**

The intent of this control enhancement is to ensure that the CDS implements mechanisms that

provide alerts when the security functions (such as authentication, access control, virus scanning, content checking, etc.) encounter results that could signify potential compromise, or attempts to compromise, the CDS itself or the connected networks. With respect to communication, alerting should be provided for not only data flows, but also for inter-process communications. The mechanism may provide alerts by logging audit events to the log file for review by an administrator, sending messages directly to the console, invoking an audible tone to signal a problem, or by shutting down processes or services to prevent further compromise of the system.

The CDS should provide alert mechanisms for all security mechanisms that trigger when an indicator is detected. The CDS should provide the ability to configure the defined set of compromise indicators. The CDS should provide the ability to configure alert mechanism to react to specific indicators for all of the security mechanisms in place. The CDS should generate alerts for indicators from all security mechanisms in place. The CDS should protect the configuration of the defined set of indicators from modification by unauthorized administrators and users. The CDS should protect the configuration of the alerting mechanism from modification by unauthorized administrators and users. The CDS should be configured to alert when security-related events, in accordance with site policy, are detected. The CDS should be configured to alert the appropriate security administrator when a security-related event occurs.

**SI 4 6 Information System Monitoring**

The intent of this control enhancement is to ensure that non-privileged users should not bypass intrusion detection and prevention mechanisms implemented within the CDS. This includes a user's ability to send traffic through the system and to remotely or locally access the system. The CDS must ensure that all traffic is routed through the intrusion detection and prevention mechanisms before it is processed by the CDS. In addition, access requests to the system should be routed through the intrusion detection and prevention mechanisms prior to being sent to the access control mechanisms.

Actions performed by all users (privileged and non-privileged) shall be monitored by intrusion detection and prevention mechanisms. However, defined privileged users should be provided the capability to alter the configuration of the CDSs intrusion detection and prevention mechanisms. Non-privileged users should not be allowed to alter the configuration of the CDS's intrusion detection mechanisms. The CDS protects the configuration of its intrusion detection mechanisms from unauthorized access by non-privileged users.

The CDS should route all traffic, high to low, through its intrusion detection mechanism before processing the traffic any further. The CDS should route all traffic, low to high, through its intrusion detection mechanism before processing the traffic any further. The CDS should route all remote access requests through the intrusion detection mechanisms prior to processing by the access control mechanisms. The CDS should route all local access requests through the intrusion detection mechanisms prior to processing by the access control mechanisms. The CDS should not provide the ability to turn off the intrusion detection mechanism. The CDS should allow traffic from only authorized users/hosts to proceed beyond the intrusion detection mechanism. The CDS should protect the configuration of the intrusion detection mechanism to only authorized, privileged users.

**SI 4 7 Information System Monitoring**

The intent of this control enhancement is to ensure that the CDS provides a mechanism to notify required personnel of suspicious events. The notification may be the CDS sending an email to the required personnel, providing a visual console alert, or invoking an audible tone to signal an issue. The suspicious events may include identification of network attacks (such as syn flood, message replay), multiple unauthorized attempts to access CDS security mechanisms, etc. The

intent of this control also covers the CDSs ability to react to a suspicious event in an automated, least disruptive, manner. These reactions may include the graceful shutdown of processes or services to prevent compromise of the system, with or without human interaction. The list of events, reactions, and personnel shall be configurable only by authorized, privileged users.

The CDS should provide alerting mechanisms to notify personnel when a suspicious event occurs. The CDS alert mechanism should notify defined personnel [via email, visual, or audible means] when specific events occur, as defined by policy. Visual alert notifications should be presented and remain visual until an authorized privileged user acknowledges the notification. Audible notifications are presented and remain audible until an authorized privileged user acknowledges the notification. The CDS should be capable of automatically executing the defined action when a suspicious event occurs. The CDS should react (as defined by the configuration) when a suspicious event occurs. The CDS should restrict the configuration of defined suspicious events to only authorized, privileged users. The CDS should restrict the configuration of defined reactions to suspicious events to only authorized, privileged users. The CDS should restrict the configuration of notified personnel to only authorized, privileged users. The CDS should be configured to alert the appropriate security administrator when a security-related incident occurs.

**SI 4 8 Information System Monitoring**

The intent of this control enhancement is to ensure that the CDS applies access control restrictions to the intrusion detection/monitoring log files/reports and alerting mechanisms. Only authorized administrators and processes should be able to access, modify and/or delete the log files/reports and alerts associated with the intrusion detection/monitoring mechanism. Tests conducted on behalf of this control should test various methods of attempted access, modification, or deletion. For example, processes in different domains on the CDS shall not write to the same log files/reports; unauthorized users shall not be allowed to write reports or cause false alerts; unauthorized users and processes shall not delete reports/log files or acknowledge alerts, etc.

The CDS should restrict access to the intrusion detection log files/reports to only authorized administrators through the use of access control privileges. The CDS should restrict access to the intrusion detection alerts to only authorized administrators through the use of access control privileges. The CDS should restrict the ability to modify and/or delete the intrusion detection logs files/reports to only authorized, privileged users. The CDS should restrict the ability to modify and/or delete the intrusion detection alerts to only authorized, privileged users. The site should have policy and procedures that define how output from the CDS intrusion monitoring tools should be protected external to the CDS.

**SI 4 9 Information System Monitoring**

The intent of this control enhancement is to ensure that the CDS-connected enclaves detect, respond, and recover to perceived or actual attacks against them. This control is concerned with the organizations testing intrusion monitoring capabilities to ensure they are up to date and working as expected. It is also concerned with the organizational policies and procedures that govern the testing process, to include the frequency.

The organization should have defined procedures to test intrusion monitoring tool to ensure that the tools are up to date and working as expected. The organizational intrusion monitoring policies should define the methodology for testing and frequency of execution for the intrusion monitoring tools within the organization's enclave.

**SI 4 10 Information System Monitoring**

The intent of this control enhancement is to ensure that encrypted traffic is not sent straight through the CDS without monitoring by the CDS. The CDS must decrypt the traffic so that the

system's monitoring tools are able to accurately document and monitor the traffic/data. As defined by site policy, when the CDS decrypts the traffic, it is responsible for re-encrypting the data prior to sending data to the destination domain. From a site perspective, it is important that the site monitoring tools be able to access the data as needed to perform monitoring functions.

The CDS should block all encrypted data it receives that it is unable to decrypt. The CDS should decrypt all encrypted data received before processing the data (i.e., sending the data through the inspection processes). The CDS should re-encrypt data, as defined by policy, after completing inspection, but prior to transfer to another domain. The CDS should not be configured to allow encrypted data to be sent directly through the CDS (i.e., bypassing the inspection processes). The CDS should restrict access to configuration of encryption mechanisms to only authorized, privileged users. [for example, some channels may require that outgoing communications be re-encrypted, while others may not] The site policy and procedures should define how the organization should handle encrypted communications to ensure they are monitored. The site components responsible for decryption/encryption of the data flow should be configured to send only unencrypted traffic to the CDS and to re-encrypt data received from the CDS. The CDS should re-encrypt data, if required by policy, prior to transfer to another domain.

**SI 4 11 Information System Monitoring**

The intent of this control enhancement is to ensure that the site is monitoring the communications within their local enclave and at their enclave boundary to ensure that traffic destined for an external enclave/host is valid and authorized. The site should monitor on a periodic basis (at a minimum), the resources within their enclave for anomalous, suspicious activity (such as long-term persistent connections, or unusual or unauthorized protocol activity, to destinations beyond the local enclave). The expectation is that, at a minimum, intrusion detection occurs at the boundary and on components within the enclave (e.g., network and host based intrusion detection). For example, for CDSs, any enclave authentication database used to authenticate to or through the CDS should implement host based intrusion detection.

The site should have policy and procedures in place to routinely monitor communication channels at the local enclave boundary that are destined for devices/host on an external enclave. The organization should implement intrusion detection capabilities at the enclave boundary. The site should implement network-based intrusion detection within their local enclave. The organization should implement host based intrusion detection on systems hosting security-relevant functions.

**SI 4 12 Information System Monitoring**

The intent of the control enhancement is to ensure that the CDS has a mechanism that should trigger an alert upon specific activities occurring. The list of activities that should trigger an alert from the CDS should be focused on events that should affect the security of the CDS itself or one of its mechanisms responsible for enforcing security controls on the data flow.

The CDS should provide an alert mechanism for all security mechanisms when unusual or inappropriate activity is detected. The CDS should provide the capability to configure the defined set of unusual or inappropriate activity. The CDS should generate alerts for unusual or inappropriate activity from the security mechanisms it is configured to monitor. The CDS should protect the configuration of the defined set of unusual or inappropriate from modification by unauthorized administrators and users. The CDS should protect the configuration of the alerting mechanism from modification by unauthorized administrators and users. The CDS should be configured to trigger an alert when unusual or inappropriate activities occur (as defined by site policy).

**SI 5 Security Alerts, Advisories, and Directives**

The intent of this control is to ensure that the site has policy and procedures in place that address providing and distributing security alerts, advisories and directives to the required individuals within the organization. The policy and procedures should dictate, 1) who is responsible for providing security alerts, advisories and directives, 2) where the security alerts, advisories and directives should be provided from, and 3) who the security alerts, advisories, and directives should be distributed to within the organization. The policy and procedures should also document who within the organization is responsible for generating security alerts, advisories or directives authored by the site.

The site should also have policy and procedures in place to address how security alerts, advisories and directives that affect the CDS should be handled. The policy and procedures should document the proper process that should be followed prior to altering the CDS software and/or configuration to ensure that the CDS certification and accreditation are not compromised.

The site policy and procedures should define how and from whom security alerts, advisories and directives should be provided and disseminated within the organization. The site policy and procedures should define how and to whom security alerts, advisories and directives that originate within the organization should be generated and disseminated. The site policy and procedures should define the proper process for handling security alerts, advisories and directives that directly affect the CDS. The site policy and procedures should define organizational roles and responsibilities for the handling of security alerts, advisories, and directives.

**SI 5 1 Security Alerts, Advisories, and Directives**

The intent of this control enhancement is to ensure that the site uses automated mechanisms whenever possible to provide and distribute security alert and advisory information. The automated mechanism may include registration to an external alert advisory database that automatically notifies an individual within the organization when a new alert or advisory is released. The individual within the organization may also setup auto-forward rules for alerts and advisories received from the registered site so that they are automatically distributed throughout the organization.

The site policy and procedures should define a process to automate the receipt of published security alerts and advisories to required individuals. The site policy and procedures should define a process to automate the distribution of security alerts and advisories received throughout the organization.

**SI 6 Security Functionality Verification**

The intent of this control is to ensure that the CDS has a mechanism that should monitor the status and execution of security processes to ensure they are configured and functioning correctly. The mechanisms should execute periodically while the CDS is in an operational state. The frequency of the execution is configurable, based on policy, and should only be configured by an authorized, privileged user. In addition, the mechanism shall be able to be executed upon command by an authorized, privileged administrator. The mechanisms should also execute upon transition back to an operational state. When the CDS detects that a security function is not operating properly, the CDS shall take the appropriate action(s), based on policy. Examples of monitoring functions for CDS should be integrity checkers or process monitoring (to ensure that expected processes are running).

The CDS should detect when security functions/processes are started and stopped. The CDS should monitor the operation of security functions/processes to ensure they are configured and functioning correctly. The monitoring of the security functions/processes should occur on a periodic basis while the system is in an operational state. The monitoring of the security

functions/processes should be executed upon transition to an operational state. The execution of security function/process monitoring should only be initiated by an authorized, privileged user. The CDS should react, as defined by policy, when it identifies a security function/process that is not operating as desired. The CDS should be configured to monitor a defined set of security functions/processes. The frequency of monitoring execution should be configured to execute monitoring functions. The configuration of the CDS monitoring function should only be performed by authorized, privileged users. The defined set of actions, when a function/process is not operating/configured as expected, should only be configurable by only authorized, privileged users.

**SI 6 1 Security Functionality Verification**

The intent of this control enhancement is to ensure that the CDS provides the ability to notify system administrators when scheduled self-tests and/or security tests encounter a failure. Self-tests should include startup tests run against the hardware and/or software of the CDS. For a CDS, automated security tests should include integrity checkers or process monitors (as defined in the parent control). It should also include virus scanning of the system itself.

The CDS should provide the ability to notify security personnel of the results of failed self-tests and/or security-related tests. The CDS should alert security personnel of failed security tests. The CDS should be configured to notify security personnel when self-tests or security-related tests fail, in accordance with site policy. The CDS system administrator's address should be stored in the CDS for alert notifications regarding security test failures.

**SI 7 Software and Information Integrity**

The intent of this control is to ensure that the CDS has a validated mechanism that should detect unauthorized changes to the CDS software and information resident on the system. Information going through. This control includes unauthorized changes to CDS software such as the OS and application. Information includes items such as the configuration files for the security mechanisms it employs. For a CDS, the information (configuration files, etc) to monitor for unauthorized changes should only be configured by authorized, privileged users.

The CDS should provide the capability to detect changes in software and configuration files while in an operational state. The CDS should provide the capability to detect changes in software and configuration files at startup. The CDS should detect unauthorized changes to the CDS operating system and application. The CDS should detect unauthorized changes to the security mechanisms' configuration files. The CDS should be configured to detect unauthorized changes in a defined set of security functions/processes. The configuration of the CDS monitoring for unauthorized changes to the CDS software and information should only be performed by authorized, privileged users. The CDS should provide the capability to alert administrators when a file or piece of software fails the integrity verification. The CDS should have an alert mechanism to notify administrators when a file or piece of software fails the integrity verification. The CDS should ensure the integrity of software and configuration files at startup. The CDS should run integrity checking mechanisms periodically during normal operations, as defined by site policy. The list of files/software that the CDS is configured to monitor should include all security-related files and software on the CDS itself. The CDS should be configured to alert administrators when a file or piece of software fails the integrity verification.

**SI 7 1 Software and Information Integrity**

The intent of this control enhancement is to ensure that the CDS has a mechanism that should monitor the integrity of the system software and information resident on the system (i.e., CDS). See SI-7 for additional details on the definition of software and information as it pertains to this control. In addition, this integrity scan should execute on a periodic basis while the system is in an operational state.

The CDS should provide a mechanism to validate the integrity of the CDS software and information. The CDS should validate the integrity of the CDS's operating system and applications. The CDS should validate the integrity of the CDS's configuration files. The CDS's integrity validation mechanisms should execute on a periodic basis while the system is in an operational state. The CDS's integrity validation mechanism should execute upon transition to an operational state. The CDS's integrity validation mechanism should be configured to validate a defined set of security functions/processes. The configuration of the CDS's integrity validation mechanism should only be performed by authorized, privileged users. The execution of the integrity validation mechanism should only be initiated by an authorized, privileged user. The configuration of the frequency of integrity validation executions should be performed by only authorized, privileged users.

**SI 7 2 Software and Information Integrity**

The intent of this control enhancement is to ensure that the CDS is configured to allow an automated notification to be sent to a specific individual(s) whenever the CDS identifies a file or software module whose integrity should not be verified or that fails verification.

This control directly relates to SI-7, which tests the CDS's capability to monitor and alert on integrity verification.

The CDS configuration should contain the correct address of the security administrator to which integrity failure notifications are to be sent and The CDS should be configured to automatically alert security administrators when a failure occurs.

**SI 7 3 Software and Information Integrity**

The intent of this control enhancement is to ensure that the site has implemented a mechanism within their enclave to centrally manage tools that are used to verify the integrity of the IA components used within their enclave. Many CDSs do not provide a means to send integrity status to a central device. In the case of CDS, the site should have a centrally managed policy in place that defines procedures for validating the integrity of the devices on their enclave. The site must have a mechanism (i.e., device or policy) in place to centrally manage the integrity of the components within their enclave.

**SI 7 4 Software and Information Integrity**

The intent of this control enhancement is to ensure that the CDS vendor employs some form of tamper protection on the CDS components when they are shipped from the vendor site to the customer site. This should allow the detection of potential modifications to the hardware during shipping on arrival at the customer site. In addition, this control covers the detection of tampering once the CDS is placed at the customer site. Tamper evident packaging should include tamper tape, locked cases, etc.

All CDS components should be shipped in tamper-evident packaging. The originating organization that creates and maintains the source code and the hardware components should be provided to the customer by the vendor along with country of origin information. The CDS components should have tamper-evident mechanisms in place during transit to the site (i.e., delivery mechanisms). The CDS components should have tamper-evident mechanisms in place during operations.

**SI 8 Spam Protection**

The intent of this control enhancement applies to both the transfer of spam and the ability of each CDS component to self-protect itself from spam (limits the waste of available resources). Many CDS components should not be concerned with spam protection; however, there may be instances where a component of the CDS is responsible for the receipt/hosting of applications which may be susceptible.

The CDS should have a mechanism to scan data that passes through the CDS for spam messages. The CDS should detect spam in all low to high domain data transfers. The CDS should detect spam in all high to low domain data transfers. The CDS should have a mechanism to scan messages destined for CDS components for spam. The vendor documentation must include procedures for updating spam definition files. The procedures defined by the vendor should be effective in correctly updating the CDS spam definition files. The CDS should continue to scan the data as configured when the spam definition files have been updated. The CDS should have the capability to block, quarantine, and/or remove data containing spam. (on each component and data traversing) The CDS should alert administrators when spam is detected in a data transfer and The CDS should monitor its processing threshold to detect abnormalities in spam processing.

**SI 8 1 Spam Protection**

The intent of this control enhancement is to ensure that the site is aware of the impact that spam should have on their network resources and that the site has mechanisms in place to block spam inbound to, and outbound from, their local enclave. The site's ability to detect and protect, to include updating the spam protection mechanisms, their network resources from unsolicited communications should help protect the site's CDS from attack (i.e., defense in depth posture). The site should have mechanisms within their local enclave that detect and block unsolicited communications from entering and exiting their local enclave and have policy and procedures in place to define the process, to include frequency, for updating spam mechanisms.

**SI 8 2 Spam Protection**

The intent of this control enhancement is to ensure that the CDS will only automatically update its signature definitions from the network of highest classification that it is connected to.

**SI 9 Information Input Restrictions**

The intent of this control is to ensure that input of information directly on to the CDS is restricted to authorized users. (input sent through the CDS is covered in AC-4) Restrictions shall be based on the user's role/responsibilities. In addition, the site should have policy and procedures in place that define who is authorized to input data directly on to the CDS and what type of data may be directly inputted to the CDS. For example, the site policy should defined who is authorized to configure the dirty word list (i.e., input the defined dirty words) on the CDS, and the proper process to follow to that the dirty word list has been vetted and approved through the appropriate channels prior to entering the information in the CDS configuration.

The CDS should authenticate users prior to allowing them to input information on to the system. The CDS should use authorization information to document a user's ability to input information on to the CDS. The site should have policy and procedures in place that document the individual(s) authorized to enter information directly on to the CDS. The site should have policy and procedures in place that document the type of information that is authorized to be inputted to the CDS.

**SI 10 Information Input Validation**

The intent of this control is to ensure that input to the CDS is validated by the CDS prior to being accepted by the system. (input sent through the CDS is covered in AC-4) Since the Information flow controls should validate input transferred through the CDS (or in the case of multi-level solutions, data that must go through verification and the regrader function prior to being input in to the MLS solution), this control is only focused on information used locally by the CDS. For example, if the local CDS user/administrators are required to have email addresses associated with their user names, the CDS should validate the format and content of the email address prior to accepting the address and associating it with the administrator account.

In regard to the ability to prescreen data to interpreters properly handle the data; this could be

defined as a filtering function. For the purposes of all CDSs, content filtering should be handled in the AC-4 controls. This control was written for single-level database functions that do not provide separate content filtering and regrading functions and for free-form text input that occurs during the configuration of the CDS.

The CDS should validate data inputs used to locally configure the CDS based upon expected input parameters. [e.g., user/administrator account data, firewall rules, interface addresses, etc.] The CDS should validate both gui-driven and command-line data inputs. The CDS should reject invalid data inputs. The CDS should provide visual notification to privileged users when data inputs are invalid. The CDS administrators at the site must be made aware of the restrictions mandated by the CDS for free-form data input on to the CDS itself.

**SI 11 Error Handling**

The intent of this control is to ensure that the CDS correctly identifies error conditions that are important to the overall security posture of the CDS and the transactions it processes. It also ensures that CDSs do not provide extraneous information within error messages/logs that could facilitate an attack against the system or provide a means for a user to circumvent the security controls on the system. For CDS, authorized personnel could be (depending upon policy) users that send messages to the CDS and administrators. This includes error messages that are provided back to users and/or administrators who submit messages or data to the CDS for processing. For a CDS, authorized personnel and the amount of information in those messages should depend upon policy [both policy within the community and site policy]. For example, some sites may allow users to receive error messages with very limited detail. Other sites may restrict these messages to only privileged personnel or provide privileged personnel messages with additional information. In some instances, community policy dictates that the messages to users shall not indicate that the system is a CDS or the configuration of the filtering mechanisms. The community policy should be based upon the connected security domains.

The CDS should identify error conditions related to security events that occur while processing data transferring through the CDS. The CDS should log information regarding all security related-errors. The CDS should not send error messages to non-privileged users that reveal sensitive information about the CDS's configuration. The CDS should not send error messages to non-privileged users that reveal sensitive information about the CDS's processing capabilities. The CDS should not send error messages to non-privileged users that reveal sensitive information about the connected enclaves. The CDS error messages sent to privileged users should contain only enough detail to allow corrective action to be taken without revealing sensitive information about the CDS.

**SI 12 Information Output Handling and Retention**

The intent of this control is to ensure that the information within the CDS is maintained in accordance with applicable laws and requirements. For example, a CDS shall not overwrite data within the system until the information has been backed up or off-loaded from the system. The extent of the tests that need to occur should depend upon policy. For example, there may be an operational requirement that the system automatically off-load data every 24 hours. For CDS, this would need to be tested for specifically defined information types and their retention requirements. This control relates to CP-9 and .AU-5 such that AU-5 needs to define, for CDS that audit data not be overwritten prior to being backed-up.

The CDS should provide the capability to backup/off-load information for retention purposes. [Note: for CDS the backup is generally to external media or an alternate server; however, that does not necessarily have to be the case for all data. In some instances the back-up may be to a different partition on the system.] The CDS should back up/offload information to alternate storage that is the same security domain as the information being backed-up/offloaded. The

CDS backup/offload procedures should be well defined and function as expected. The CDS should provide the capability to automate the backup/off-load of defined information. The CDS must provide the ability to configure the frequency of automated information backup/off-loads and must not overwrite information prior to backup/off-loading. The site should identify the necessary federal laws, executive orders, directives, etc. that they must comply with regarding the retention of their information with, and output from, the components within their information system. The site policy should identify which components within their information system require information to be retained, how long the information must be retained, details on the type of information that must be retained from those components, and where this retained information is to be stored. The site procedures should describe how to offload/backup the information that must be retained for each component that provides mitigations to CDS vulnerabilities and the site policy must define how CDS backups/offloaded data shall be handled.

**SI 13 4 Predictable Failure Prevention**

The intent of this control enhancement is to ensure the CDS system is capable of either rolling over to another system upon critical failure or shutting down to prevent further compromise or damage. In the case where a CDS is capable of automatically rolling over to another system, this functionality should be transparent to the user and provide notification to the administrator that the roll-over occurred. Many CDSs do not provide automatic roll over functionality. If the CDS does not provide an automatic roll over capability but provides instruction on the configuration and procedures for performing a manual swap, those procedures should be tested and that the end results of the swap is a fully functional system. In the case where a CDS is capable of shutting down components, when a critical failure is detected, the CDS should be capable of either shutting down the specific channel associated with the failure, or in cases where the failure warrants, shutting down the entire CDS. Configuration of the time-period allowed for the rollover shall be tested. For CDS, critical failure is a failure in a security function/component which affects the CDS's ability to enforce the security policy. The CDS rollover capability should only be configured by an authorized, privileged user. The CDS shutdown capability should only be configured by an authorized, privileged user. The CDS should be configured to shut down the appropriate components (i.e., entire system or individual components) upon identification of a critical failure.

## 6. Specific Value Parameters

There are no unique parameter values for cross domain solutions.

## 7. Regulatory/Statutory Controls

The following are regulatory or statutory controls that directly/indirectly apply to cross domain solutions.

- DCID 6/3
- OMB Memorandum 06-16
- NIST Special Publications 800-12, 800-30, 800-39, 800-46, 800-48, 800-60, 800-63, 800-73, 800-76, 800-77, 800-78, 800-92, 800-94, 800-97, 800-100, 800-113, 800-114, 800-121, 800-124
- OMB Memorandum 04-04
- FIPS Publication 201. 199, 140-2
- DoD Instruction 8500.2, February 6, 2003

## 8. Tailoring Considerations

For cross domain solutions, start with *CNSS Instruction No. 1253, July 2011 Revision* and then apply this Cross Domain Solution Overlay. Care should be taken that security controls are not removed without a thorough understanding of the system, mission, environment and network. Removing one security control can affect different aspects of the cross domain solution and jeopardize certification and accreditation.

## 9. Duration

This overlay uses the NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009 with May 2010 errata updates and CNSS Instruction No. 1253, July 2011 Revision, *Security Controls and Control Selections for National Security Systems*, Draft July 2011. When either document is finalized or edited, this CDS Overlay will need to be revisited.

## 10. Definitions

Please see CNSSI 4009 ([http://www.cnss.gov/Assets/pdf/cnssi\\_4009.pdf](http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf))