Insider Threat Overlays

1. Identification

The *Insider Threat Overlays* identifies security control specifications needed to protect against insider threats and establishes an organizational Insider Threat Program for IT enterprises with national security systems (NSS).

In 2011, Executive Order (EO) 13587 required the establishment of Insider Threat Programs for deterring, detecting, and mitigating insider threats, including the safeguarding of classified information from exploitation, compromise, or other unauthorized disclosure.

Then in 2012, the White House Memorandum, *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*, required agencies to monitor and audit user activity on classified networks.

Thereafter in 2014, the White House Memorandum, *Near-term Measures to Reduce the Risk of High-Impact Unauthorized Disclosures* required the implementation of corrective measures for classified computer networks to improve business practices, enhance the security culture across the workforce, and reduce the unique risks associated with privileged users.

The *Insider Threat Overlays* correlates and applies the insider threat related requirements established in these regulatory and statutory references, along with insider threat related policies, guidelines, and best practices from Committee for National Security Systems (CNSS), Intelligence Community (IC), Department of Defense (DoD), and National Institute of Standards and Technology (NIST) issuances, to the security controls specified in NIST Special Publication (SP) 800-53 (Revision 4).

The intended audience for this document includes, Information System Owners and System Security Engineers, Enterprise Security Service Providers, Insider Threat Program Management, Security Incident Responders, Security Control Assessors, and Authorizing Officials, who will use the information contained in this document to understand the insider threat related aspects of the security controls specified by the overlays.

The following documents were used to create these overlays:

- EO 13526, *Classified National Security Information*, 5 January 2010
- EO 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, 7 October 2011
- EO *Amending the Civil Service Rules, Executive Order 13488, and Executive Order 13467 to Modernize the Executive Branch-Wide Governance Structure and Processes for Security Clearances, Suitability and Fitness for Employment, and Credentialing, and Related Matters*, 17 January 2017
- White House Memorandum, November 2012, Subject: *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*
- White House Memorandum, February 2014, Subject: *Near-term Measures to Reduce the Risk of High-Impact Unauthorized Disclosures*
- Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01B, Cyber Incident Handling Program, 10 July 2012

- CNSS Directive (CNSSD) 504, *Directive on Protecting NSS from Insider Threat*, 4 February 2014
- CNSS Instruction (CNSSI) 1001, *National Instruction on Classified Information Spillage*, February 2008
- CNSSI 4009, *Committee on National Security Systems (CNSS) Glossary*, 6 April 2015.
- CNSSI 1015, *Enterprise Audit Management Instruction for National Security Systems* (NSS), September, 2013
- CNSSI 1253, *Security Categorization and Control Selection for National Security Systems*, 27 March 2014
- CNSSI 1253 Appendix F Attachment 3, *CDS Overlay*, 24 April 2016
- CNSSI 1253 Appendix F Attachment 5, *Classified Information Overlay*, 9 May 2014
- CNSSI 1253 Appendix F Attachment 6, *Privacy Overlay*, 20 April 2015
- CNSS Policy (CNSSP) 11, *National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products*, 10 June 2013
- CNSSP 15, *National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information among National Security Systems*, 1 October 2012
- CNSSP 17, *Policy on Wireless Systems*, January 2014
- CNSSP 25, *National Policy for Public Key Infrastructure in National Security Systems*, March 2009
- DoD Directive (DoDD) 5205.16 *The DoD Insider Threat Program*, 30 September 2014
- Title 32, Code of Federal Regulations (CFR), Part 310, DoD Privacy Program
- Department of Defense (DoD) Insider Threat Management and Analysis Center (DITMAC) System of Records Notice (SORN), 17 October 2016
- ICS 502-01, *Intelligence Community Computer Incident Response and Computer Network Defense*, 20 December 2013
- Intelligence Community Enterprise Audit Conceptual Framework, June 2011
- National Defense Authorization Act (NDAA) for Fiscal Year 2017
- NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, December 2014
- NIST SP 800-161 Supply Chain Risk Management, April 2015
- Office of the Secretary of Defense Insider Threat Mitigation, 12 July 2013
- The Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, and Breach Rules, at 45 C.F.R. Parts 160 and 164 (2013)
- The Privacy Act of 1974, as amended, (P.L. 93-579), 5 U.S.C. §552a

These overlays should be reviewed and updated, as necessary, when new regulatory or statutory direction is issued that impacts the designation or application of insider threat-related security controls or upon the publication of a revision to NIST SP 800-53, CNSSI 1015, or CNSSI 1253.

2. Overlay Characteristics

The *Insider Threat Overlays* applies to NSS that store, process, or transmit classified, national security, or controlled unclassified information and to the enterprise security solutions and Insider Threat Programs that support those systems.

The *Insider Threat Overlays* provides guidance for information access, encryption, anonymization, redaction, disclosure, retention, disposal and disposal techniques of Personally Identifiable Information (PII) and Protected Health Information (PHI). Information sharing and safeguarding covered by this document includes but is not limited to, foreign contact information, foreign travel information, personnel security information, financial disclosure information, in addition to relevant databases and files, personnel security files, polygraph examination reports, facility access records, security violation files, travel records, foreign contact reports, and financial disclosure filings.

This document contains four overlays (IT System, Enterprise, Insider Threat System, and Insider Threat Program). These overlays in unison reflect enterprise-wide insider threat detection and mitigation activities and the shared responsibilities of service providers and system owners that comprise an enterprise insider threat solution.

Figure 1 presents an enterprise level overview of the interrelationships among the various components of an insider threat program.[1] The IT System and Enterprise Overlays refer to components and functions external to the Centralized Hub (Private Enclave) and the Insider Threat System and Insider Threat Program Overlays refer to components and functions internal to the Centralized Hub (Private Enclave).

The IT System Overlay is based on a system categorization of Low Confidentiality, Low Integrity, and Low Availability and specifies security controls applicable to all systems regardless of system categorization. When a control that is specified only at a higher level (e.g., Moderate or High) is addressed in the overlay, then such specification is clearly cited in the Justification for Selection.

The Enterprise Overlay contains common and hybrid security controls that are inherited by one or more organizational information systems. The controls specified in the Enterprise Overlay are based on providing support to systems categorized with Low Confidentiality, Low Integrity, and Low Availability. When a control that is specified only at a higher level (e.g., Moderate or High) is addressed in the overlay, then such specification is clearly cited in the Justification for Selection.

[1] Figure 1 is based on Figure 1 in the NITTF 2014 Guide To Accompany the National Insider Threat Policy and Minimum Standards.

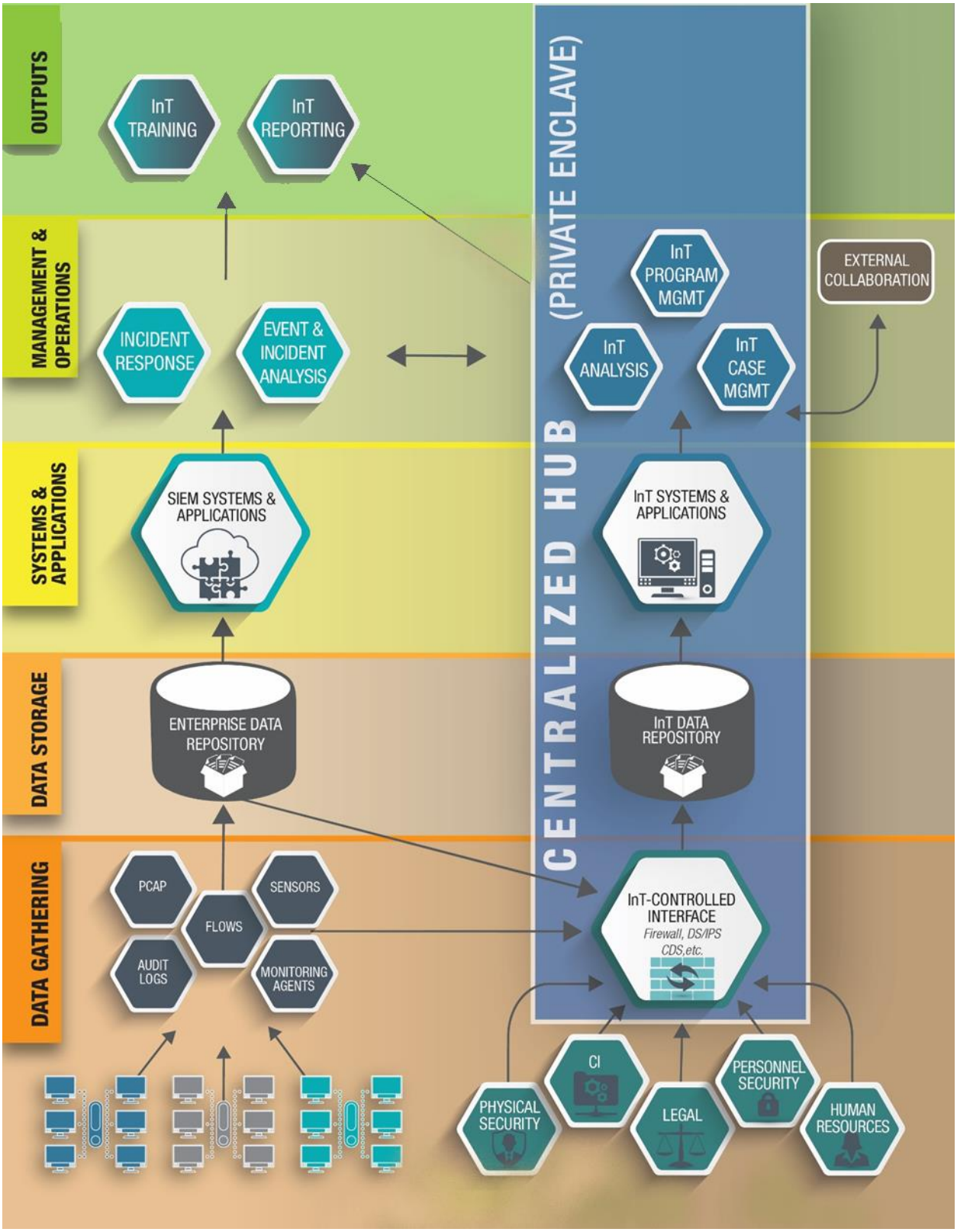

Figure 1 – Insider Threat Program: Enterprise View

The Insider Threat System Overlay specifies security controls for IT systems that directly support the Insider Threat Program. The Insider Threat System Overlay is based on a system categorization of High Confidentiality, High Integrity, and Moderate Availability. The Insider Threat System Overlay also includes security and privacy controls based on the Personally Identifiable Information (PII) Confidentiality Impact Level High and Protected Health Information (PHI) Privacy Overlays.

The Insider Threat Program Overlay contains common and hybrid security controls specifically implemented by the Insider Threat Program, which are then inheritable by the enterprise. The Insider Threat Program Overlay is based on a system categorization of High Confidentiality, High Integrity, and Moderate Availability. The Insider Threat Program Overlay also includes security and privacy controls based on the PII Confidentiality Impact Level High and PHI Privacy Overlays.

The assumptions that underlie the security control selections and serve as the basis to justify the allocation of controls in the *Insider Threat Overlays* include:

- The IT System and Enterprise overlays were developed without differentiation for a particular classification or sensitivity of the information. These overlays are intended to be universally applicable to all classification and sensitivity levels, to include Top Secret/SCI, Top Secret Collateral, Secret, Confidential, and Controlled Unclassified Information (CUI) (e.g., Law Enforcement, PII/PHI, For Official Use Only (FOUO), Limited Distribution (LIMDIS)).
- The Insider Threat System and Insider Threat Program overlays were developed to provide the requisite level of protection for, up to, Top Secret/SCI and all Privacy (e.g., PII High/PHI) information.
- The Insider Threat System overlay was developed with the basis that there are no wireless or remote (external to the local network) accesses to Insider Threat Systems (i.e., systems that directly support the Insider Threat Program).
- All Insider Threat overlays were developed without differentiation between NSS organizations (e.g., IC, DoD, Executive Branch). Best practice policies and guidelines were universally included and consolidated from all organizational communities without limitation to the community from which they were established.

3. Applicability

Use the following questions to determine the applicability of the *Insider Threat Overlays*:

a. *Is your organization required to establish an Insider Threat Program per EO 13587?* If the answer is no, the *Insider Threat Overlays* do not apply. If the answer is yes, continue through the additional questions below to determine which of the *Insider Threat Overlays* applies.
b. *Are the security controls being applied to an individual IT system?* If the answer is yes, then follow the guidance for the IT System overlay.
c. *Are the security controls being implemented by an enterprise solution for inheritance by one or more IT systems?* If the answer is yes, then follow the guidance for Enterprise overlay.

d. *Are the security controls being applied to an IT system that directly supports the Insider Threat Program?* If the answer is yes, then follow the guidance for Insider Threat System overlay.
e. *Are the security controls being implemented by the organization's centralized Insider Threat Program?* If the answer is yes, then follow the guidance for Insider Threat Program overlay.

4. Overlay Summary

The table below contains a summary of the security control specifications as they apply in the *Insider Threat Overlay*. The symbols used in the table are as follows:

- The letter "B" indicates the control is a CNSSI 1253 baseline control using a Confidentiality = Low, Integrity = Low, and Availability = Low baseline for all IT systems and a Confidentiality = High, Integrity = High, and Availability = Moderate for Insider Threat Systems.
- The letter "P" indicates the control is a PII Moderate and/or PHI Privacy Overlay baseline control.
- A plus sign ("+") indicates the control is to be selected.
- Two dashes ("--") indicates the control is not to be selected.
- The letter "E" indicates there is a control extension.
- The letter "G" indicates there is supplemental guidance, including specific tailoring guidance if applicable, for the control.
- The letter "V" indicates the overlay defines a value for an organizational-defined parameter for the control. (The parameter value may be from CNSSI 1253, the DoD Specific Assignment Values (DSPAV), or created specifically for this overlay.)
- The letter "R" indicates there is at least one regulatory/statutory reference that requires the control selection or that the control helps to meet the regulatory/statutory requirements.
- Absence of any symbol (i.e., a blank cell) indicates the security control or enhancement does not apply to that overlay.

Table 1: Insider Threat Overlays Security Controls

Control ID	Control Name	IT System	Enterprise	Insider Threat System	Insider Threat Program
AC-2	Account Management	BGVR	BGVR	BGVR	
AC-2(1)	Account Management | Automated System Account Management		GR		
AC-2(2)	Account Management | Removal of Temporary / Emergency Accounts			BV	
AC-2(3)	Account Management | Disable Inactive Accounts			BV	

Control ID	Control Name	IT System	Enterprise	Insider Threat System	Insider Threat Program
AC-2(4)	Account Management | Automated Audit Actions	BGV	BGV	BGV	
AC-2(5)	Account Management | Inactivity Logout	BGV	BGV	BGV	
AC-2(7)	Account Management | Role Based Schemes	BGVR	BGVR	BGVR	
AC-2(9)	Account Management | Restrictions On Use of Shared Groups / Accounts	BGV	BGV	--PG	
AC-2(10)	Account Management | Shared / Group Account Credential Termination	BG	BG	--	
AC-2(11)	Account Management | Usage Conditions			BGV	
AC-2(12)	Account Management | Account Monitoring / Atypical Use		BGV	BGV	BGV
AC-2(13)	Account Management | Disable Accounts for High Risk Individuals	BGV	BGV	BPV	
AC-3	Access Enforcement	BEG		BPEG	
AC-3(2)	Access Enforcement | Dual Authorization	+GVR		+GVR	
AC-3(4)	Access Enforcement | Discretionary Access Control	BGV		BGV	
AC-3(9)	Access Enforcement | Controlled Release			PV	
AC-3(10)	Access Enforcement | Audited Override of Access Control Mechanisms			PV	
AC-4	Information Flow Enforcement			BPV	
AC-4(4)	Information Flow Enforcement | Content Check Encrypted Information	+GV	+GV	+GV	
AC-4(15)	Information Flow Enforcement | Detection of Unsanctioned Information			PV	
AC-4(17)	Information Flow Enforcement | Domain Authentication			PV	
AC-4(18)	Information Flow Enforcement | Security Attribute Binding			PV	
AC-5	Separation of Duties	BGVR		BPGVR	

Control ID	Control Name	IT System	Enterprise	Insider Threat System	Insider Threat Program
AC-6	Least Privilege	BEGR		BPEGR	
AC-6(1)	Least Privilege | Authorize Access to Security Functions	BGV		BPGV	
AC-6(2)	Least Privilege | Non-Privileged Access for Nonsecurity Functions	BGV	BGV	BPGV	
AC-6(3)	Least Privilege | Network Access to Privileged Commands			BV	
AC-6(5)	Least Privilege | Privileged Accounts	BGV		BPGV	
AC-6(7)	Least Privilege | Review of User Privileges	BGVR	BGVR	BPGVR	
AC-6(8)	Least Privilege | Privilege Levels for Code Execution	BGV		BGV	
AC-6(9)	Least Privilege | Auditing Use of Privileged Functions	BG		BPG	
AC-6(10)	Least Privilege | Prohibit Non-Privileged Users From Executing Privileged Functions	BG		BPG	
AC-7	Unsuccessful Logon Attempts	BGV		BGV	
AC-8	System Use Notification	BGVR		BGVR	
AC-9	Previous Logon (Access) Notification	+GR		+GR	
AC-9(1)	Previous Logon (Access) Notification | Unsuccessful Logons	+GR		+GR	
AC-10	Concurrent Session Control	+GVR		BGVR	
AC-11	Session Lock	BGV		BPGV	
AC-11(1)	Session Lock | Pattern-Hiding Displays	BG		BG	
AC-12	Session Termination			BPV	
AC-12(1)	Session Termination | User-Initiated Logouts / Message Displays			BV	
AC-14	Permitted Actions Without Identification Or Authentication			BV	
AC-16	Security Attributes			BPV	

Control ID	Control Name	IT System	Enterprise	Insider Threat System	Insider Threat Program
AC-16(3)	Security Attributes | Maintenance of Attribute Associations by Information System			PV	
AC-16(6)	Security Attributes | Maintenance of Attribute Association by Organization			BV	
AC-17	Remote Access			BP	
AC-17(1)	Remote Access | Automated Monitoring / Control	BG		BG	
AC-17(2)	Remote Access | Protection of Confidentiality / Integrity Using Encryption			BP	
AC-17(3)	Remote Access | Managed Access Control Points			BV	
AC-17(4)	Remote Access | Privileged Commands / Access			BV	
AC-17(6)	Remote Access | Protection of Information			B	
AC-17(9)	Remote Access | Disconnect / Disable Access			BGV	
AC-18(4)	Wireless Access | Restrict Configurations by Users	BG	BG		
AC-20	Use of External Information Systems			BP	
AC-20(2)	Use of External Information Systems | Portable Storage Devices	BGV	BGV		
AC-20(3)	Use of External Information Systems | Non-Organizationally Owned Systems / Components / Devices	BGV	BGV		
AC-21	Information Sharing			BPV	
AC-22	Publicly Accessible Content	BEGVR	BEGVR		
AC-23	Data Mining Protection	BGVR			
AT-2	Security Awareness			BPV	
AT-2(2)	Security Awareness | Insider Threat		BGR		BGR
AT-3	Security Training			BPV	
AT-3(2)	Role-Based Security Training | Physical Security Controls		BGV		

Control ID	Control Name	IT System	Enterprise	Insider Threat System	Insider Threat Program
AT-3(4)	Role-Based Security Training | Suspicious Communications and Anomalous System Behavior		BGV		
AT-4	Security Training Records			BPV	
AU-1	Audit and Accountability Policy and Procedures		BGVR		BPGVR
AU-2	Audit Events	BGVR	BGVR	BPGVR	BPGVR
AU-2(3)	Audit Events | Reviews and Updates		BGV		BGV
AU-3	Content of Audit Records	BG		BGP	
AU-3(1)	Content of Audit Records | Additional Audit Information	BGVR		BGVR	
AU-3(2)	Content of Audit Records | Centralized Management of Planned Audit Record Content	+GVR	+GVR	BGVR	
AU-4	Audit Storage Capacity	BGVR	BGVR	BPGVR	
AU-4(1)	Audit Storage Capacity | Transfer to Alternate Storage	BGVR	BGVR	BGVR	
AU-5	Response to Audit Processing Failures	BGVR		BGVR	
AU-5(1)	Response to Audit Processing Failures | Audit Storage Capacity	BGV		BGV	
AU-5(2)	Response to Audit Processing Failures | Real-Time Alerts	GVR		GVR	
AU-6	Audit Review, Analysis, and Reporting	BEGVR	BEGVR	BPEGVR	BPEGVR
AU-6(1)	Audit Review, Analysis, and Reporting | Process Integration		BGR	BGR	BGR
AU-6(3)	Audit Review, Analysis, and Reporting | Correlate Audit Repositories		BGR	BPGR	BPGR
AU-6(4)	Audit Review, Analysis, and Reporting | Central Review and Analysis		BGR	BGR	
AU-6(5)	Audit Review, Analysis, and Reporting | Integration / Scanning and Monitoring Capabilities		+GVR	BGVR	BGVR

Control ID	Control Name	IT System	Enterprise	Insider Threat System	Insider Threat Program
AU-6(6)	Audit Review, Analysis, and Reporting | Correlation with Physical Monitoring		+GR	BGR	BGR
AU-6(8)	Audit Review, Analysis, and Reporting | Full Text Analysis of Privileged Commands			+GR	+GR
AU-6(9)	Audit Review, Analysis, and Reporting | Correlation with Information From Nontechnical Sources				+GR
AU-6(10)	Audit Review, Analysis, and Reporting | Audit Level Adjustment	BG	BG	BPG	BPG
AU-7	Audit Reduction and Report Generation		GR	BPGR	
AU-7(1)	Audit Reduction and Report Generation | Automatic Processing		GVR	BPGVR	
AU-7(2)	Audit Reduction and Report Generation | Automatic Sort and Search		+GVR	PGVR	
AU-8	Time Stamps	BGV		BGV	
AU-8(1)	Time Stamps | Synchronization with Authoritative Time Source	BGVR	BGVR	BGVR	
AU-9	Protection of Audit Information	BGR	BGR	BGR	
AU-9(2)	Protection of Audit Information | Audit Backup on Separate Physical Systems / Components	+GVR		BPGVR	
AU-9(3)	Protection of Audit Information | Cryptographic Protection	+GR	+GR	BPGR	
AU-9(4)	Protection of Audit Information | Access by Subset of Privileged Users	BEGVR	BEGVR	BEGVR	BEGVR
AU-9(6)	Protection of Audit Information | Read Only Access	+GVR	+GVR	+GVR	+GVR
AU-10	Non-Repudiation	GVR		BPGVR	
AU-10(1)	Non-Repudiation | Association of Identities			PV	

Control ID	Control Name	IT System	Enterprise	Insider Threat System	Insider Threat Program
AU-10(3)	Non-Repudiation | Chain of Custody				+ER
AU-11	Audit Record Retention		BGVR		BGVR
AU-11(1)	Audit Record Retention | Long-Term Retrieval Capability		BGV		BGV
AU-12	Audit Generation	BEGVR		BPEGVR	
AU-12(1)	Audit Generation | System-Wide / Time-Correlated Audit Trail	BGV	BGV	BGV	
AU-12(3)	Audit Generation | Changes by Authorized Individuals	BGV	BGV	BPGV	BPGV
AU-14	Session Audit	BGR	BGR	BGR	BGR
AU-14(1)	Session Audit | System Start-Up	BG	BG	BG	
AU-14(2)	Session Audit | Capture/Record and Log Content	BGR	BGR	BGR	BGR
AU-14(3)	Session Audit | Remote Viewing / Listening	BG		BG	BG
AU-16	Cross-Organizational Auditing		+GVR	+GVR	+GVR
AU-16(1)	Cross-Organizational Auditing | Identity Preservation		+GR		+GR
AU-16(2)	Cross-Organizational Auditing | Sharing of Audit Information		+GVR		PGVR
CA-2	Security Assessments			BPV	
CA-2(1)	Security Assessments | Independent Assessors		BGV		
CA-2(2)	Security Assessments | Specialized Assessments		GVR		
CA-3	System Interconnections			BPV	
CA-3(2)	System Interconnections | Unclassified Non-National Security System Connections			+V	
CA-3(3)	System Interconnections | Unclassified Non-National Security System Connections			PV	
CA-3(5)	System Interconnections | Restrictions On External System Connections			BPV	
CA-5	Plan of Action and Milestones			BV	
CA-6	Security Authorization			BPV	

Control ID	Control Name	IT System	Enterprise	Insider Threat System	Insider Threat Program
CA-7	Continuous Monitoring		BGVR	BPVR	BPGVR
CA-7(3)	Continuous Monitoring | Trend Analysis		+GR	+GR	+GR
CA-8	Penetration Testing			BPV	
CA-9	Internal System Connections			BPV	
CA-9(1)	Internal System Connections | Security Compliance Checks			P	
CM-2	Baseline Configuration			B	
CM-2(1)	Baseline Configuration | Reviews and Updates			BV	
CM-2(2)	Baseline Configuration | Automation Support for Accuracy / Currency			B	
CM-2(3)	Baseline Configuration | Retention of Previous Configurations			BV	
CM-3	Configuration Change Control			BV	
CM-3(1)	Configuration Change Control | Automated Document / Notification / Prohibition of Changes			BV	
CM-3(2)	Configuration Change Control | Test / Validate / Document Changes			B	
CM-3(4)	Configuration Change Control | Security Representative			BV	
CM-3(5)	Configuration Change Control | Automated Security Response			BV	
CM-3(6)	Configuration Change Control | Cryptography Management	BGV	BGV	BPGV	
CM-4	Security Impact Analysis			BP	
CM-4(1)	Security Impact Analysis | Separate Test Environments			BP	
CM-4(2)	Security Impact Analysis | Verification Of Security Functions			P	
CM-5	Access Restrictions for Change	BG		BG	
CM-5(1)	Access Restrictions for Change | Automated Access Enforcement / Auditing	G		BG	

Control ID	Control Name	IT System	Enterprise	Insider Threat System	Insider Threat Program
CM-5(2)	Access Restrictions for Change | Review System Changes	GV		BGV	
CM-5(3)	Access Restrictions for Change | Signed Components			BV	
CM-5(5)	Access Restrictions for Change | Limit Production / Operational Privileges	BGVR		BGVR	
CM-5(6)	Access Restrictions for Change | Limit Library Privileges	BG		BG	
CM-6	Configuration Settings			BGV	
CM-6(1)	Configuration Settings | Automated Central Management / Application / Verification	BGV		BGV	
CM-6(2)	Configuration Settings | Respond to Unauthorized Changes			BV	
CM-7	Least Functionality			BV	
CM-7(1)	Least Functionality | Periodic Review	BGV	BGV	BGV	
CM-7(2)	Least Functionality | Prevent Program Execution	BGV		BGV	
CM-7(3)	Least Functionality | Registration Compliance	BGV	BGV	BGV	
CM-7(4)	Least Functionality | Unauthorized Software / Blacklisting	+GV	+GV	+GV	
CM-7(5)	Least Functionality | Authorized Software / Whitelisting	BGVR	BGVR	BGVR	
CM-8	Information System Component Inventory			BV	
CM-8(1)	Information System Component Inventory | Updates During Installations / Removals			BP	
CM-8(2)	Information System Component Inventory | Automated Maintenance	BGR	BGR	BGR	

Control ID	Control Name	IT System	Enterprise	Insider Threat System	Insider Threat Program
CM-8(3)	Information System Component Inventory | Automated Unauthorized Component Detection		BGV		
CM-8(4)	Information System Component Inventory | Accountability Information			BV	
CM-9	Configuration Management Plan			B	
CM-10	Software Usage Restrictions			B	
CM-10(1)	Software Usage Restrictions | Open Source Software			BV	
CM-11	User-Installed Software	BGV	BGV	BGV	
CM-11(1)	User-Installed Software | Alerts for Unauthorized Installations	+GV	+GV	BGV	
CM-11(2)	User-Installed Software | Prohibit Installation without Privileged Status	BG		BG	
CP-2	Contingency Plan			BPV	
CP-2(1)	Contingency Plan | Coordinate with Related Plans			B	
CP-2(3)	Contingency Plan | Resume Essential Missions / Business Functions			BV	
CP-2(8)	Contingency Plan | Identify Critical Assets			BP	
CP-3	Contingency Training			BV	
CP-4	Contingency Plan Testing			BPV	
CP-4(1)	Contingency Plan Testing | Coordinate with Related Plans			B	
CP-6	Alternate Storage Site			B	
CP-6(1)	Alternate Storage Site | Separation from Primary Site			B	
CP-6(3)	Alternate Storage Site | Accessibility			B	
CP-7	Alternate Processing Site			BPV	
CP-7(1)	Alternate Processing Site | Separation From Primary Site			B	
CP-7(3)	Alternate Processing Site | Priority of Service			B	
CP-9	Information System Backup			BPV	

Control ID	Control Name	IT System	Enterprise	Insider Threat System	Insider Threat Program
CP-9(1)	Information System Backup | Testing for Reliability / Integrity			BV	
CP-9(5)	Information System Backup | Transfer to Alternate Storage Site			BV	
CP-10	Information System Recovery and Reconstitution			BP	
CP-10(2)	Information System Recovery and Reconstitution | Transaction Recovery			B	
CP-10(4)	Information System Recovery and Reconstitution | Restore within Time Period			BV	
IA-2	Identification and Authentication (Organizational Users)	BEGR		BPEGR	
IA-2(1)	Identification and Authentication (Organizational Users) | Network Access to Privileged Accounts	BGR		BGR	
IA-2(2)	Identification and Authentication (Organizational Users) | Network Access to Non-Privileged Accounts	BGR		BGR	
IA-2(3)	Identification and Authentication (Organizational Users) | Local Access to Privileged Accounts	+GR		BGR	
IA-2(4)	Identification and Authentication (Organizational Users) | Local Access to Non-Privileged Accounts	GR		BGR	
IA-2(5)	Identification and Authentication (Organizational Users) | Group Authentication	BG		BG	
IA-2(6)	Identification and Authentication (Organizational Users) | Network Access to Privileged Accounts - Separate Device			PV	

Control ID	Control Name	IT System	Enterprise	Insider Threat System	Insider Threat Program
IA-2(7)	Identification and Authentication (Organizational Users) | Network Access to Non-Privileged Accounts - Separate Device			PV	
IA-2(8)	Identification and Authentication (Organizational Users) | Network Access to Privileged Accounts – Replay Resistant			B	
IA-2(9)	Identification and Authentication (Organizational Users) | Network Access to Non-Privileged Accounts - Replay Resistant			B	
IA-2(11)	Identification and Authentication (Organizational Users) | Remote Access - Separate Device			BPV	
IA-2(12)	Identification and Authentication (Organizational Users) | Acceptance of PIV Credentials			B	
IA-3	Device Identification and Authentication	BGV		BPGV	
IA-3(1)	Device Identification and Authentication | Cryptographic Bidirectional Authentication	GVR		BGVR	
IA-4	Identifier Management	BGV		BPGV	
IA-4(4)	Identifier Management | Identify User Status	BGV	BGV	BGV	
IA-5	Authenticator Management	BGV	BGV	BPGV	
IA-5(1)	Authenticator Management | Password-Based Authentication	BGV	BGV	BGV	
IA-5(2)	Authenticator Management | PKI-Based Authentication	+BG	+BG	BG	
IA-5(3)	Authenticator Management | In-Person or Trusted Third-Party Registration			BV	

Control ID	Control Name	IT System	Enterprise	Insider Threat System	Insider Threat Program
IA-5(4)	Authenticator Management | Automated Support for Password Strength Determination	BGV	BGV	BGV	
IA-5(7)	Authenticator Management | No Embedded Unencrypted Static Authenticators			B	
IA-5(8)	Authenticator Management | Multiple Information System Accounts	BGV		BGV	
IA-5(11)	Authenticator Management | Hardware Token-Based Authentication			BV	
IA-5(13)	Authenticator Management | Expiration of Cached Authenticators			BV	
IA-5(14)	Authenticator Management | Managing Content of PKI Trust Stores			B	
IA-6	Authenticator Feedback			BP	
IA-7	Cryptographic Module Authentication			BP	
IA-8	Identification and Authentication (Non-Organizational Users)	BGR		BGR	
IA-10	Adaptive Identification and Authentication	GV	GV	BGV	
IA-11	Re-authentication			BV	
IR-1	Incident Response Policy and Procedures		BGV		BPGV
IR-2	Incident Response Training	BGV	BGV	BPGV	BPGV
IR-2(1)	Incident Response Training | Simulated Events			B	
IR-2(2)	Incident Response Training | Automated Training Environments			B	
IR-3	Incident Response Testing		BGV		BGV
IR-3(2)	Incident Response Testing | Coordination with Related Plans		G		G
IR-4	Incident Handling	BG	BG	BPG	BPG

Control ID	Control Name	IT System	Enterprise	Insider Threat System	Insider Threat Program
IR-4(1)	Incident Handling | Automated Incident Handling		G	BG	
IR-4(3)	Incident Handling | Continuity of Operations	GVR	GVR	GVR	GVR
IR-4(4)	Incident Handling | Information Correlation		BG		BG
IR-4(6)	Incident Handling | Insider Threats - Specific Capabilities		BGR		BGR
IR-4(7)	Incident Handling | Insider Threats - Intra-Organization Coordination		BGVR		BGVR
IR-4(8)	Incident Handling | Correlation with External Organizations		BGV		BGV
IR-5	Incident Monitoring		BG		BPG
IR-5(1)	Incident Monitoring | Automated Tracking / Data Collection / Analysis		G	BG	BG
IR-6	Incident Reporting		BGV		BPGV
IR-6(1)	Incident Reporting | Automated Reporting		G	BG	BG
IR-6(2)	Incident Reporting | Vulnerabilities Related to Incidents		BGV		BGV
IR-7	Incident Response Assistance		BG		BPG
IR-7(1)	Incident Response Assistance | Automation Support for Availability of Information / Support		+G	BG	
IR-7(2)	Incident Response Assistance | Coordination with External Providers		BG		BG
IR-8	Incident Response Plan		BGV		BPGV
IR-9	Information Spillage Response			BV	
IR-9(3)	Information Spillage Response | Post-Spill Operations			BV	
IR-9(4)	Information Spillage Response | Exposure to Unauthorized Personnel				BV
IR-10	Integrated Information Security Analysis Team		G		BPG
MA-1	System Maintenance Policy and Procedures			BPV	

Control ID	Control Name	IT System	Enterprise	Insider Threat System	Insider Threat Program
MA-2	Controlled Maintenance			BPV	
MA-2(2)	Controlled Maintenance | Automated Maintenance Activities			B	
MA-3	Maintenance Tools	BG	BG	BG	
MA-3(1)	Maintenance Tools | Inspect Tools			B	
MA-3(2)	Maintenance Tools | Inspect Media	BG	BG	BG	
MA-3(3)	Maintenance Tools | Prevent Unauthorized Removal			BV	
MA-4(1)	Nonlocal Maintenance | Auditing and Review	GV			
MA-4(3)	Nonlocal Maintenance | Comparable Security / Sanitization			B	
MA-5	Maintenance Personnel			BP	
MA-6	Timely Maintenance			BV	
MP-1	Media Protection Policy and Procedures		BGVR		
MP-2	Media Access	BEGVR	BEGVR	BPEGVR	
MP-3	Media Marking	GVR	GVR	BPGVR	
MP-4	Media Storage	GVR	GVR	BPGVR	
MP-5	Media Transport			BPV	
MP-5(4)	Media Transport | Cryptographic Protection			BP	
MP-6	Media Sanitization			BPV	
MP-6(1)	Media Sanitization | Review / Approve / Track / Document / Verify			BP	
MP-6(2)	Media Sanitization | Equipment Testing			BV	
MP-6(3)	Media Sanitization | Nondestructive Techniques			BV	
MP-6(8)	Media Sanitization | Remote Purging / Wiping of Information			BPV	
MP-7	Media Use	BEGVR	BEGVR	BPEGVR	
MP-7(1)	Media Use | Prohibit Use Without Owner			BP	
MP-8	Media Downgrading			PV	

Control ID	Control Name	IT System	Enterprise	Insider Threat System	Insider Threat Program
MP-8(3)	Media Downgrading | Controlled Unclassified Information			PV	
PE-2	Physical Access Authorizations			BPV	
PE-2(1)	Physical Access Authorizations | Access By Position / Role			P	
PE-3	Physical Access Control		BGVR	BPGVR	
PE-3(1)	Physical Access Control | Information System Access		BGV	BGV	
PE-5	Access Control for Output Devices			BP	
PE-6	Monitoring Physical Access			BPV	
PE-8	Visitor Access Records			BPV	BPV
PE-8(1)	Visitor Access Records | Automated Records Maintenance / Review			B	
PE-18	Location of Information System Components			PV	
PL-1	Security Planning Policy and Procedures			BPV	
PL-2	System Security Plan			BPV	
PL-2(3)	System Security Plan | Plan / Coordinate with Other Organizational Entities			BV	
PL-4	Rules of Behavior	BGVR	BGVR	BPGVR	
PL-8	Information Security Architecture			BPV	
PS-1	Personnel Security Policy and Procedures			BPV	BPV
PS-2	Position Risk Designation			BPV	BPV
PS-3	Personnel Screening		BGVR	BPGVR	BPGVR
PS-3(3)	Personnel Screening | Information with Special Protection Measures			BPV	BPV
PS-4	Personnel Termination	BGVR	BGVR	BPGVR	BPGVR
PS-4(2)	Personnel Termination | Automated Notification			BV	
PS-5	Personnel Transfer		BGVR	BPGVR	BPGVR
PS-6	Access Agreements		BGVR	BPGVR	BPGVR

Control ID	Control Name	IT System	Enterprise	Insider Threat System	Insider Threat Program
PS-6(3)	Access Agreements | Post-Employment Requirements			B	B
PS-7	Third-Party Personnel Security		BGVR	BPGVR	BPGVR
PS-8	Personnel Sanctions		BGVR	BPGVR	BPGVR
RA-2	Security Categorization			BP	
RA-3	Risk Assessment			BPV	
RA-5	Vulnerability Scanning	BGVR	BGVR	BGVR	
RA-5(1)	Vulnerability Scanning | Update Tool Capability	BG	BG	BG	
RA-5(2)	Vulnerability Scanning | Update by Frequency / Prior to New Scan / When Identified	BGV	BGV	BGV	
RA-5(4)	Vulnerability Scanning | Discoverable Information	BGV	BGV	BGV	
RA-5(5)	Vulnerability Scanning | Privileged Access	BGV	BGV	BGV	
RA-5(10)	Vulnerability Scanning | Correlate Scanning Information			B	
SA-2	Allocation of Resources			BP	
SA-3	System Development Life Cycle			BPV	
SA-4	Acquisition Process			BP	
SA-4(1)	Acquisition Process | Functional Properties of Security Controls			B	
SA-4(2)	Acquisition Process | Design / Implementation Information for Security Controls			B	
SA-4(3)	Acquisition Process | Development Methods / Techniques / Practices			BV	
SA-4(5)	Acquisition Process | System / Component / Service Configurations			BV	
SA-4(7)	Acquisition Process | NIAP-Approved Protection Profiles			B	
SA-4(9)	Acquisition Process | Functions / Ports / Protocols / Services in Use			B	
SA-4(10)	Acquisition Process | Use of Approved PIV Products			B	

Control ID	Control Name	IT System	Enterprise	Insider Threat System	Insider Threat Program
SA-5	Information System Documentation			BV	
SA-8	Security Engineering Principles			BP	
SA-9	External Information System Services			BV	
SA-10	Developer Configuration Management			BV	
SA-10(1)	Developer Configuration Management | Software / Firmware Integrity Verification			B	
SA-11	Developer Security Testing and Evaluation			BPV	
SA-11(5)	Developer Security Testing and Evaluation | Penetration Testing			PV	
SA-12	Supply Chain Protection			BV	
SA-12(1)	Supply Chain Protection | Acquisition Strategies / Tools / Methods			BV	
SA-12(9)	Supply Chain Protection | Operations Security			BV	
SA-14	Criticality Analysis			BV	
SA-15	Development Process, Standards, and Tools			BV	
SA-15(3)	Development Process, Standards, and Tools | Criticality Analysis			BV	
SA-15(4)	Development Process, Standards, and Tools | Threat Modeling / Vulnerability Analysis			BV	
SA-15(7)	Development Process, Standards, and Tools | Automated Vulnerability Analysis			BV	
SA-15(9)	Development Process, Standards, and Tools | Incident Response Plan			BP	
SA-16	Developer-Provided Training			BV	

Control ID	Control Name	IT System	Enterprise	Insider Threat System	Insider Threat Program
SA-17	Developer Security Architecture and Design			BP	
SA-19	Component Authenticity			BV	
SA-21	Developer Screening			PV	
SA-22	Unsupported System Components			B	
SC-1	System and Communications Protection Policy and Procedures			BV	
SC-2	Application Partitioning			BP	
SC-3	Security Function Isolation			B	
SC-4	Information in Shared Resources	GR		BPGR	
SC-5(1)	Denial of Service Protection | Restrict Internal Users		BGV		
SC-5(2)	Denial of Service Protection | Excess Capacity / Bandwidth / Redundancy		G		
SC-5(3)	Denial of Service Protection | Detection / Monitoring			BV	
SC-7(5)	Boundary Protection | Deny by Default / Allow by Exception	BGR		BGR	
SC-7(9)	Boundary Protection | Restrict Threatening Outgoing Communications Traffic	BG	BG	BG	
SC-7(10)	Boundary Protection | Prevent Unauthorized Exfiltration		BGR	BGR	
SC-7(11)	Boundary Protection | Restrict Incoming Communications Traffic			BV	
SC-7(12)	Boundary Protection | Host-Based Protection			BV	
SC-7(13)	Boundary Protection | Isolation of Security Tools / Mechanisms / Support Components		BGV		
SC-7(14)	Boundary Protection | Protects Against Unauthorized Physical Connections			BPV	
SC-7(15)	Boundary Protection | Route Privileged Network Accesses	+GR	+GR	+GR	

Control ID	Control Name	IT System	Enterprise	Insider Threat System	Insider Threat Program
SC-7(18)	Boundary Protection | Fail Secure			B	
SC-7(21)	Boundary Protection | Isolation of Information System Components			BV	
SC-8	Transmission Confidentiality and Integrity			BPV	
SC-8(1)	Transmission Confidentiality and Integrity | Cryptographic or Alternate Physical Protection			BPV	
SC-8(2)	Transmission Confidentiality and Integrity | Pre / Post Transmission Handling			BPV	
SC-10	Network Disconnect	GVR		BGVR	
SC-12	Cryptographic Key Establishment and Management			BPV	
SC-13	Use of Cryptography			BPV	
SC-15	Collaborative Computing Devices			BV	
SC-17	Public Key Infrastructure Certificates			BV	
SC-18	Mobile Code			B	
SC-18(1)	Mobile Code | Identify Unacceptable Code / Take Corrective Actions			BV	
SC-18(2)	Mobile Code | Acquisition / Development / Use			BV	
SC-18(3)	Mobile Code | Prevent Downloading / Execution			BV	
SC-18(4)	Mobile Code | Prevent Automatic Execution			BV	
SC-20	Secure Name/Address Resolution Service (Authoritative Source)			B	
SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver)			B	
SC-22	Architecture and Provisioning for Name/Address Resolution Service			B	

Control ID	Control Name	IT System	Enterprise	Insider Threat System	Insider Threat Program
SC-23	Session Authenticity			B	
SC-23(1)	Session Authenticity | Invalidate Session Identifiers at Logout			B	
SC-23(3)	Session Authenticity | Unique Session Identifiers with Randomization			BV	
SC-23(5)	Session Authenticity | Allowed Certificate Authorities			BV	
SC-24	Fail in Known State			BV	
SC-28	Protection of Information at Rest			BPV	
SC-28(1)	Protection of Information at Rest | Cryptographic Protection	BGVR		BPGVR	
SC-38	Operations Security	BGV	BGV	BGV	
SC-39	Process Isolation			B	
SC-42	Sensor Capability and Data	+GV		+GV	
SC-42(3)	Sensor Capability and Data | Prohibit Use of Devices		+GV		
SI-1	System and Information Integrity Policy and Procedures			BV	
SI-2	Flaw Remediation			BV	
SI-2(2)	Flaw Remediation | Automated Flaw Remediation Status			BV	
SI-2(6)	Flaw Remediation | Removal of Previous Versions of Software / Firmware			BV	
SI-3	Malicious Code Protection	BEGVR		BPEGVR	
SI-3(2)	Malicious Code Protection | Automatic Updates			B	
SI-4	Information System Monitoring	BGV	BGV	BPGV	BPGV
SI-4(1)	Information System Monitoring | System-Wide Intrusion Detection System		BG		
SI-4(2)	Information System Monitoring | Automated Tools for Real-Time Analysis		GR	BGR	BGR

Control ID	Control Name	IT System	Enterprise	Insider Threat System	Insider Threat Program
SI-4(4)	Information System Monitoring | Inbound and Outbound Communications Traffic		BGV	BGV	BGV
SI-4(5)	Information System Monitoring | System-Generated Alerts		BGV		
SI-4(10)	Information System Monitoring | Visibility of Encrypted Communications		GV		
SI-4(11)	Information System Monitoring | Analyze Communications Traffic Anomalies		BGV		BGV
SI-4(12)	Information System Monitoring | Automated Alerts		BGV		
SI-4(14)	Information System Monitoring | Wireless Intrusion Detection		BGR		
SI-4(15)	Information System Monitoring | Wireless to Wireline Communications		BGR		
SI-4(16)	Information System Monitoring | Correlate Monitoring Information		BG		BG
SI-4(19)	Information System Monitoring | Individuals Posing Greater Risk				BV
SI-4(20)	Information System Monitoring | Privileged User				BGVR
SI-4(22)	Information System Monitoring | Unauthorized Network Services			BV	
SI-4(23)	Information System Monitoring | Host-Based Devices	BGV	BGV	BGV	
SI-5	Security Alerts, Advisories, and Directives			BPV	
SI-6	Security Functionality Verification			BV	
SI-6(3)	Security Function Verification | Report Verification Results			BV	

Control ID	Control Name	IT System	Enterprise	Insider Threat System	Insider Threat Program
SI-7	Software and Information Integrity			BPV	
SI-7(1)	Software, Firmware, and Information Integrity | Integrity Checks			BV	
SI-7(2)	Software, Firmware, and Information Integrity | Automated Notifications of Integrity Violations			BV	
SI-7(5)	Software, Firmware, and Information Integrity | Automated Response to Integrity Violations			BV	
SI-7(6)	Software, Firmware, and Information Integrity | Cryptographic Protection			P	
SI-7(7)	Software, Firmware, and Information Integrity | Integration of Detection and Response			BV	
SI-7(8)	Software, Firmware, and Information Integrity | Auditing Capability for Significant Events	+GV		BGV	
SI-7(14)	Software, Firmware, and Information Integrity | Binary or Machine Executable Code			B	
SI-10	Information Input Validation			BPV	
SI-10(3)	Information Input Validation | Predictable Behavior			B	
SI-11	Error Handling			BPV	
SI-12	Information Handling and Retention			BP	
SI-16	Memory Protection			BV	
PM-11	Mission/Business Process Definition			BP	
PM-12	Insider Threat Program		BEGR		BPEGR
PM-15	Contacts with Security Groups and Associations		BGR		BGR
PM-16	Threat Awareness Program		BGR		BGR
AP-1	Authority to Collect				P
AP-2	Purpose Specification				P

Control ID	Control Name	IT System	Enterprise	Insider Threat System	Insider Threat Program
AR-2	Privacy Impact and Risk Assessment				P
AR-3	Privacy Requirements for Contractors and Service Providers				P
AR-5	Privacy Awareness and Training				PV
AR-7	Privacy-Enhanced System Design and Development			P	
AR-8	Accounting of Disclosures				P
DM-1(1)	Minimization of Personally Identifiable Information | Locate / Remove / Redact / Anonymize PII			+	+
DM-2	Data Retention and Disposal			PV	PV
DM-3	Minimization of PII Used in Testing, Training, and Research			P	P
DM-3(1)	Minimization of PII Used in Testing, Training, and Research | Risk Minimization Techniques			P	P
IP-1	Consent				PGR
IP-2	Individual Access				PGR
IP-3	Redress				--R
IP-4	Complaint Management				PGR
SE-2	Privacy Incident Response		PGR	PGR	PGR
UL-1	Internal Use				P
UL-2	Information Sharing with Third Parties				P

5. Detailed Overlay Control Specifications

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

AC-2 Account Management

- Justification to Select: AC-2 is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program. Office of the Secretary

of Defense Insider Threat Mitigation, 12 July 2013 requires that tier 3 privileged user assignment be reviewed and validated on a quarterly basis.

Supplemental Guidance: Elements of AC-2 are implemented at both the system and enterprise levels. If a system or the organization does not properly or fully implement account management, then the enterprise will not be able to control and monitor access by insiders to information systems, networks, and restricted information.

Organizations should provide an inventory of all validated privileged Users and their authorized accesses and privileges to internal security and counterintelligence (CI) offices. This inventory shall be reviewed, validated and provided to personnel security, the Insider Threat Program, and CI Program on at least a quarterly basis for Tier 3 Privileged Users (e.g., Network and Domain Administrators) and on at least an annual basis for all other Privileged Users. The inventory will enable personnel security, Insider Threat, and CI specialists to review, track and evaluate any security or other reportable events by a Privileged User, such as a change in employment status, position, or organization. Any revocation or expansion of a Privileged User's access shall be reported immediately (within 1 business day) to personnel security, Insider Threat, and CI offices.

Parameter Value(s): The organization:

a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: *at least: General User Accounts; Privileged User Accounts; Group Accounts; Temporary/Emergency Accounts; and System Accounts*;
b. Assigns account managers for information system accounts;
c. Establishes conditions for group and role membership;
d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
e. Requires approvals by *ISSM or ISSO* for requests to create information system accounts;
f. Creates, enables, modifies, disables, and removes information system accounts in accordance with *an existing process or by developing and implementing processes that include the requirement for each user to complete annual security awareness and privacy training, or the account shall be disabled whenever the specified conditions are not met*;
g. Monitors the use of information system accounts;
h. Notifies account managers:
    1. When accounts are no longer required;
    2. When users are terminated or transferred; and
    3. When individual information system usage or need-to-know changes;
i. Authorizes access to the information system based on:
    1. A valid access authorization;
    2. Intended system usage; and
    3. Other attributes as required by the organization or associated missions/business functions;

j. Reviews accounts for compliance with account management requirements *at least quarterly for Tier 3 privileged user accounts and annually for all other general user and privileged accounts*.
k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

Regulatory/Statutory Reference(s): Office of the Secretary of Defense Insider Threat Mitigation, 12 July 2013.

AC-2(1) Account Management | Automated System Account Management

Justification to Select: AC-2(1) is selected in the CNSSI 1253 baseline categorized Moderate or High for Confidentiality or Integrity. CNSSI 1015 requires that Departments and Agencies configure and implement audit management capabilities to effectively protect and defend NSS and they must implement, at a minimum, automated management and technical security capabilities for EAM, as outlined in Annex A of CNSSI 1015. CNSSI 1015 Annex A Element T2.4 directs Departments and Agencies automate procedures to enable or disable audit accounts.

Supplemental Guidance: Typically, the automated mechanisms to support the management of information system accounts would be implemented by an organization using a standardized enterprise solution. If the organization does not implement automated system account management, then the disabling of accounts will be more difficult and take more time, creating an opportunity for an insider threat to compromise and misuse an account that should have been disabled.

Regulatory/Statutory Reference(s): CNSSI 1015 Annex A, Element T2.4.

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

Justification to Select: AC-2(2) is selected in the CNSSI 1253 baseline categorized Moderate or High for Confidentiality or Integrity and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The information system automatically *disables* temporary and emergency accounts after *a period not to exceed 72 hours*.

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

Justification to Select: AC-2(3) is selected in the CNSSI 1253 baseline categorized Moderate or High for Confidentiality or Integrity and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The information system automatically disables inactive accounts after *a period of inactivity not to exceed:*
a. NIPRNet and SIPRNet: 35 days;
b. TS Network: 90 days;
c. Cross-Domain Systems: 30 days; or
d. A shorter period if so specified in the applicable STIG(s).

AC-2(4) Account Management | Automated Audit Actions

Justification to Select: AC-2(4) is selected in the CNSSI 1253 baseline for all systems, including systems that directly support the Insider Threat Program.

Supplemental Guidance: If a system or the organization does not automatically audit account creation, modification, enabling, disabling, and removal actions and notify the designated individuals, then an insider threat could perform such actions without detection.

Parameter Value(s): The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies *the System Administrator, Security Administrator, and ISSO*.

AC-2(5) Account Management | Inactivity Logout

Justification to Select: AC-2(5) is selected in the CNSSI 1253 baseline for all systems, including systems that directly support the Insider Threat Program.

Supplemental Guidance: If a user does not log out of the system at the end of the work period or when leaving the facility, then an insider threat could attempt to use the system to gain access using other authorized users' accounts.

Parameter Value(s): The organization requires that users log out *at the end of the user's standard work period, or when the user leaves the physical premises, unless otherwise defined in formal organizational policy and, for cross-domain systems, when required CDS actions are complete*.

AC-2(7) Account Management | Role Based Schemes

Justification to Select: AC-2(7) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program. CNSSD 504 establishes the use of role based access controls (RBAC) for privileged users as a best practice.

Supplemental Guidance: If a system or the organization does not properly manage privileged user accounts in accordance with AC-2(7), then an insider threat may be able to use privileges they should not have access to.

Organizations will identify and implement procedures to enable or disable privileged user accounts. When an individual whose position and duties no longer require such access and privileges organizations shall confirm that accesses and privileges have been revoked. Organizations will provide an inventory of all validated privileged users and their authorized accesses and privileges to the Insider Threat Office. Any revocation or expansion of a Privileged User's access shall be reported immediately to the Insider Threat Office. A complete updated copy of the inventory shall be provided on at least a quarterly basis for Tier 3 Privileged Users (e.g., Network and Domain Administrators) and on at least an annual basis for all other Privileged Users. The inventory will enable Insider Threat specialists to review, track and evaluate any security or other reportable events by a Privileged User, such as a change in employment status, position, or organization.

Parameter Value(s): The organization:
(a) Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles;
(b) Monitors privileged role assignments; and
(c) Takes *action to revoke and disable privileged role assignments and user accounts* when privileged role assignments are no longer appropriate *and all system administrator accounts that cannot currently enforce User Based Enforcement (UBE) will be configured to expire at least every 60 days*.

Regulatory/Statutory Reference(s): CNSSD 504, Section A.2.b.; CNSSI 1015 Annex A, Elements M1.4 and T1.4; and Office of the Secretary of Defense Insider Threat Mitigation, 12 July 2013.

AC-2(9) Account Management | Restrictions on use of Shared Groups / Accounts

Justification to Select: AC-2(9) is selected in the CNSSI 1253 baseline for all systems and centrally managed group accounts. However, the Privacy Overlay prohibits the use of shared/group accounts for providing access to PII. Therefore, AC-2(9) would be deselected for systems that directly support the Insider Threat Program.

Supplemental Guidance: The use of shared/group accounts (for systems other than those containing PII, including systems that directly support the Insider Threat Program) must be used in conjunction with prior unique authentication in order to mitigate the insider threat risk by associating the use of the shared/group account to an individual user. If a system or the organization does not require initial identification and authentication prior to the use of group accounts, then insider threat related activities executed using a group user account would not be traceable to a specific individual.

Parameter Value(s): The organization only permits the use of shared/group accounts that meet:
(a) A unique authenticator for initial identification and authentication prior to using a group account, and
(b) Use of group accounts/authenticators shall be explicitly authorized only by the AO (or formally designated representative)
(c) Any decision to authorize shared/group accounts must be based on a compelling need with adequate justification with such details fully documented in the SSP.

AC-2(10) Account Management | Shared / Group Account Credential Termination

Justification to Select: AC-2(10) is selected in the CNSSI 1253 baseline for all systems.

Supplemental Guidance: If a system or the organization does not terminate shared/group account credentials when members leave the group, then an insider threat may be able to use shared/group account credential privileges they should not have access to and any insider threat related activities executed using the group user account would not be traceable to the specific individual.

AC-2(11) Account Management | Usage Conditions

Justification to Select: AC-2(11) is selected in the CNSSI 1253 baseline categorized High for Confidentiality or Integrity, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: An example of restricting usage to certain times of the day, days of the week, or specific duration of time is to restrict user access to only those hours an individual is assigned to work (e.g., "core hours").

Parameter Value(s): The information system enforces *expected circumstances and/or usage conditions (e.g., restricting usage to certain times of the day, days of the week, or specific duration of time)* for *all general and privileged user account*.

AC-2(12) Account Management | Account Monitoring / Atypical Use

Justification to Select: AC-2(12) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: AC-2(12) is implemented in a centralized manner for the enterprise. Such implementation would involve account monitoring by the Insider Threat Program through the use of systems that directly support the Insider Threat Program. If the organization does not monitor information system accounts for atypical use, then an insider threat could perform unusual or unauthorized activities without detection.

Parameter Value(s): The organization:
(a) Monitors information system accounts for *atypical use (e.g., unusual or unauthorized activities or conditions such as accessing information systems at certain times of the day and from locations that are not consistent with the normal usage patterns of individual users) to include account lock-outs, requests for user identification codes (userids) or passwords, loss of desktop control (remote administration), and unexplained loss of files.*; and
(b) Reports atypical usage of information system accounts to, *at a minimum, the Security Administrator and ISSO*.

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

Justification to Select: AC-2(13) is selected in the CNSSI 1253 baseline for all systems and in the Privacy Overlay for all Privacy Impact Levels and PHI. AC-2(13) is therefore applicable to systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system or the organization does not promptly disable accounts for individuals posing a significant risk, then the user could use their account to exfiltrate information or cause damage to the system or network.

Parameter Value(s): The organization disables accounts of users posing a significant risk within *30 minutes* of discovery of the risk. This control involves both enterprise and system level measures.

AC-3 Access Enforcement

Justification to Select: AC-3 is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program. The White House Memorandum, Near-term Measures to Reduce the Risk of High-Impact Unauthorized Disclosures, requires information sharing portals hosted on classified computer networks requires authentication.

Supplemental Guidance: If a system does not enforce only approved authorizations, then an insider threat may gain access to systems, applications, or information without proper authorization.

AC-3(2) Access Enforcement | Dual Authorization

Justification to Select: Although AC-3(2) is not selected in the CNSSI 1253 baseline or an overlay, AC-3(2) is commonly implemented for all transfers of data from a classified computer network to removable media. White House Memorandum, Near-Term Measures to Reduce the Risk of High-Impact Unauthorized Disclosures, requires the implementation of two-stage controls (review and concurrence of a second person) for all transfers of data from a classified computer network to removable media, if the transfer is not part of an approved internal use process such as encrypted back-ups. Dual authorization, also referred to as two-person integrity, provides a means to minimize the insider threat.

Supplemental Guidance: Two-stage controls shall be implemented for all transfers of data from a classified computer network to removable media or to a network of lower classification. If a system does not implement dual authorizations and two-stage controls for all transfers of data from a classified computer or network to removable media, then an insider threat could use removable media to exfiltrate classified and sensitive data.

Parameter Value(s): The information system enforces dual authorization for *all transfers of data from a classified computer or network to removable media*. A second person serving to meet the two-stage control requirement should be: assigned in writing; specifically trained in their responsibilities, and the review and transfer procedures; and knowledgeable of the information being transferred to make an informed decision of the appropriateness of the transfer.

Regulatory/Statutory Reference(s): White House Memo - Near-Term Measures to Reduce the Risk of High-Impact Unauthorized Disclosures, Section D-1.

AC-3(4) Access Enforcement | Discretionary Access Control

Justification to Select: AC-3(4) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system does not enforce discretionary access controls, then an insider threat may have access to classified and sensitive information for which they do not have a need-to-know.

Parameter Value(s): The information system enforces *discretionary access control policy* over defined subjects and objects where the policy specifies that a subject that has been granted access to information can do one or more of the following:
(a) Pass the information to any other subjects or objects;
(b) Grant its privileges to other subjects;
(c) Change security attributes on subjects, objects, the information system, or the information system's components;
(d) Choose the security attributes to be associated with newly created or revised objects; or
(e) Change the rules governing access control.

AC-3(9) Access Enforcement | Controlled Release

Justification to Select: AC-3(9) is selected in the Privacy Overlay for Privacy Impact Levels of Medium or High, and for PHI. AC-3(9) is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The information system does not release information outside of the established system boundary unless:
(a) The receiving *organization, information system, or system component* provides *adequate protections for the information being released to it, such as security and privacy controls commensurate with the information sensitivity and classification (including PII Privacy Impact Level or PHI) being received*; and
(b) *Technical safeguards (e.g., file type checking, content filtering), Appendix J of NIST SP 800-53, and controls UL-1 and UL-2* are used to validate the appropriateness of the information designated for release.

AC-3(10) Access Enforcement | Audited Override of Access Control Mechanisms

Justification to Select: AC-3(10) is selected in the Privacy Overlay for all Privacy Impact Levels and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization employs an audited override of automated access control mechanisms under *situations where access control mechanisms are overridden for information systems containing PII under the Privacy Act*.

AC-4 Information Flow Enforcement

Justification to Select: AC-4 is selected in the CNSSI 1253 baseline categorized Moderate or High for Confidentiality or Integrity, and in the Privacy Overlay for Privacy Impact Levels of Moderate or High, and for PHI. AC-4 is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on *NIST 800-47 and ICS 503-1*.

AC-4(4) Information Flow Enforcement | Content Check Encrypted Information

Justification to Select: Although AC-4(4) is not selected in the CNSSI 1253 baseline or an overlay, AC-4(4) is commonly implemented to detect obfuscated data exfiltration by insider threat.

Supplemental Guidance: If a system or the organization does not prevent encrypted information from bypassing content-checking mechanisms, then an insider threat could encrypt information prior to exfiltration as a potential method to bypass system and network boundary protections. Mitigations to this exfiltration methodology include system level inspection prior to encryption and transmission and/or network boundary encryption proxying that enable the communication to be decrypted, inspected, and re-encrypted or blocked at the boundary.

Parameter Value(s): The information system prevents encrypted information from bypassing content-checking mechanisms by *decrypting the information, blocking the flow of the encrypted information, or terminating communications sessions attempting to pass encrypted information*.

AC-4(15) Information Flow Enforcement | Detection of Unsanctioned Information

Justification to Select: AC-4(15) is selected in the CNSSI 1253 baseline in the Privacy Overlay for Privacy Impact Levels of Moderate or High and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The information system, when transferring information between different security domains, examines the information for the presence of *any unsanctioned information* and prohibits the transfer of such information in accordance with the *security policy as approved by the AO and clearly documented in the System Security Plan*.

AC-4(17) Information Flow Enforcement | Domain Authentication

Justification to Select: AC-4(17) is selected in the Privacy Overlay for Privacy Impact Levels of Moderate or High and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The information system uniquely identifies and authenticates source and destination points by *the applicable organization, system, application, or individual* for information transfer.

AC-4(18) Information Flow Enforcement | Security Attribute Binding

Justification to Select: AC-4(18) is selected in the Privacy Overlay for Privacy Impact Levels of Moderate or High, and for PHI, and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The information system binds security attributes to information using *approved binding techniques* to facilitate information flow policy enforcement.

AC-5 Separation of Duties

Justification to Select: AC-5 is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: Organizations should establish mechanisms for appropriate separation of duties among those Privilege Users with the highest accesses so that accesses and privileges are distributed across the user population and no such individuals are able to perform all privileged actions for sensitive systems or applications. As an example, Systems Administrators with extensive access shall not also server as ISSOs and/or DTOs.

Organizations should institute separate administrator user accounts that tailor privileged access for particular users to the specific tasks at hand, to include separate roles for network or database administration from other sensitive functions such as cryptographic key management, hardware management, cross domain and removable media data transfer, system security management, or access to particularly sensitive information.

If a system does not adequately separate privileged user roles, then an insider threat could perform malicious activity without oversight or detection.

Parameter Value(s): The organization:

a. Separates *at a minimum:*

(1) Mission functions and distinct information system support functions are divided among different individuals/roles;

(2) Different individuals perform information system support functions (e.g., system management, systems programming, configuration management, quality assurance and testing, database management, network security);

(3) Different administrator accounts for different roles, e.g., system administration, security administration, database administration;

(4) Administration of access control functions from administration of audit functions;

(5) At a minimum, system administrators shall not also perform security audit administration functions; and

(6) Exceptions to the requirement for separation of duties must be documented in the SSP and approved by the AO or designee.

b. Documents separation of duties of individuals; and

c. Defines information system access authorizations to support separation of duties.

Regulatory/Statutory Reference(s): Office of the Secretary of Defense Insider Threat Mitigation, 12 July 2013; and White House Memo - Near-Term Measures to Reduce the Risk of High-Impact Unauthorized Disclosures, Section C-2.

AC-6 Least Privilege

Justification to Select: AC-6 is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Control Extension: The organization shall increase separation of duties and the application of "least privilege" through automation of systems administration, use of two-stage controls, and other means to reduce the need for privileged users or for such users to exercise their privileges in manual ways.

Supplemental Guidance: Organizations should restrict Information Technology (IT) Administrator (e.g., system administrators, help desk personnel, application administrators, etc.) access to information systems and data within the scope of what they are authorized to know and manage.

Organizations should enforce "least privileged" access and limited or defined duration principles to limit Privileged User access and ensure users are only provided with the minimum access necessary to perform their authorized function.

If a system does not properly implement least privilege, then an insider threat could misuse their privileged access beyond that for which they have been authorized.

Regulatory/Statutory Reference(s): CNSSD 504, Section A.2.b; White House Memo - Near-Term Measures to Reduce the Risk of High-Impact Unauthorized Disclosures, Section C-3; and Office of the Secretary of Defense Insider Threat Mitigation, 12 July 2013.

AC-6(1) Least Privilege | Authorize Access to Security Functions

Justification to Select: AC-6(1) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system does not explicitly authorize access to security functions, then an insider threat could misuse those functions to gain unauthorized access to the system or information.

Parameter Value(s): The organization explicitly authorizes access to *all functions not publicly accessible (e.g., all security functions (deployed in hardware, software, and firmware) and all security-relevant information not publicly available).*

AC-6(2) Least Privilege | Non-privileged Access for Nonsecurity Functions

Justification to Select: AC-6(2) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: The organization should establish both privileged and non-privileged accounts, with separate credentials, for users with privileged roles. Additionally, organizations should implement a policy that privileged user credentials be used only when performing privileged functions.

If a system or the organization does not require privileged users use non-privileged accounts when performing non-privileged functions, then the privileged accounts would be more exposed to compromise by an insider threat.

Parameter Value(s): The organization requires that users of information system accounts, or roles, with access to *any privileged functions (e.g., security functions such as establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters, system programming, system and security administration) or security relevant information,* use non-privileged accounts or roles, when accessing nonsecurity functions.

AC-6(3) Least Privilege | Network Access to Privileged Commands

Justification to Select: AC-6(3) is selected in the CNSSI 1253 baseline categorized High for Confidentiality or Integrity and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization authorizes network access to *privileged accounts and any privileged command (e.g., creation of a new chain of trust, deletion of audit logs, and access to removable media) or PII* only for *compelling operational needs necessary to accomplish the assigned responsibilities, as approved by the AO* and documents the rationale for such access in the security plan for the information system.

AC-6(5) Least Privilege | Privileged Accounts

Justification to Select: AC-6(5) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system does not restrict privileged accounts to specific personnel or roles, then an insider threat could gain unauthorized access to privileged information/functions.

Parameter Value(s): The organization restricts privileged accounts on the information system to *personnel or roles as defined in the System Security Plan.*

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

Justification to Select: AC-6(7) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system or the organization does not regularly review the privileges assigned to users and privileged accounts, then an insider threat could misuse privileges which are no longer valid for their role or assignment.

Organizations should periodically conduct a review of all privileged user roles and minimize their number, scope of privilege (“least privilege”), and breadth of privilege (“separation of duties”). Separate roles for network or database administration from other sensitive functions, such as cryptographic key management, hardware management, cross domain and removable media data transfer, system security management, or access to particularly sensitive information.

Organizations should also periodically conduct a review of all privileged users to ensure they have a continuing need for privileged capabilities or access, ensure they have current security clearances, and minimize any granted exceptions.

Parameter Value(s): The organization:
(a) Reviews *at a minimum, annually* the privileges assigned to *all roles and classes of users* and, *at a minimum, quarterly* the privileges assigned to *individuals with access to privileged accounts* to validate the need for such privileges; and
(b) Reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs.

Regulatory/Statutory Reference(s): White House Memo - Near-Term Measures to Reduce the Risk of High-Impact Unauthorized Disclosures, Sections A-1 and C-1.

AC-6(8) Least Privilege | Privilege Levels for Code Execution

Justification to Select: AC-6(8) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system does not limit the execution of software to the level of the user, then an insider threat could circumvent system protections and elevate their privileges beyond what is authorized for them.

Parameter Value(s): The information system prevents *all software* from executing at higher privilege levels than users executing the software.

AC-6(9) Least Privilege | Auditing Use of Privileged Functions

Justification to Select: AC-6(9) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system does not audit the execution of privileged functions, then malicious actions executed by an insider threat would not be detected.

AC-6(10) Least Privilege | Prohibit Non-Privileged Users from Executing Privileged Functions

Justification to Select: AC-6(10) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system does not prevent non-privileged users from executing privileged functions, then an insider threat could misuse the privileged functions to gain access to systems or functions for which they have not been authorized.

AC-7 Unsuccessful Logon Attempts

Justification to Select: AC-7 is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system does not limit invalid logon attempts, then an insider threat could use a brute force exploit to gain access using an identity or credential for which they have not been issued.

Parameter Value(s): The information system:

a. Enforces a limit of *three* consecutive invalid logon attempts by a user during a *time period of 15 minutes, regardless of whether the login attempt occurs via a local or network connection*; and

b. Automatically *locks an account/node for at least 15 minutes or until released by an administrator or through identity authentication software* when the maximum number of unsuccessful attempts is exceeded, *regardless of whether the login attempt occurs via a local or network connection*.

AC-8 System Use Notification

Justification to Select: AC-8 is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: Information resources should display a standard banner that provides notice of, and obtains user consent to, the collection and monitoring of all user activities. Classified and unclassified network banners should inform users that their activity on the network is being monitored for lawful United States Government-authorized purposes and can result in criminal or administrative actions against the user. This standard banner shall be implemented in coordination with legal counsel as well as with civil liberties and privacy officials, to ensure legal, civil rights, civil liberties and privacy issues are appropriately addressed and should be approved by the Senior Official(s) in consultation with legal counsel.

Additionally, standard mandatory notice and consent provisions will be included in all user agreements in accordance with applicable security controls and implementation procedures.

If a system does not display a Notice and Consent Banner, then an organization might not be able to hold an insider threat accountable for their malicious activities.

Parameter Value(s): The information system:

a. Displays to users *a Standard Mandatory DoD Notice and Consent Banner* before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that:

1. Users are accessing a U.S. Government information system;
2. Information system usage may be monitored, recorded, and subject to audit;
3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and
4. Use of the information system indicates consent to monitoring and recording;

b. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and

c. For publicly accessible systems:

1. Displays system use information *containing the applicable information contained within a Standard Mandatory DoD Notice and Consent Banner*, before granting further access;
2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
3. Includes a description of the authorized uses of the system.

Regulatory/Statutory Reference(s): CNSSI 1015; and White House Memo - National Insider Threat Policy, and Minimum Standards for Executive Branch Insider Threat Programs, Section H.4.

AC-9 Previous Logon (Access) Notification

Justification to Select: Although AC-9 is not selected in the CNSSI 1253 baseline or an overlay, AC-9 supports detection of exploitation, compromise, or other unauthorized disclosure by an insider threat, and may also provide a degree of prevention to the extent that insiders are aware of this detection capability.

Supplemental Guidance: This control should be implemented for logons managed by operating systems and applications. If a system does not notify the user of the date and time of the last logon, then misuse of their credentials by an insider threat might not be detected.

Regulatory/Statutory Reference(s): EO 13587, Section 2.1(b) and Section 5.2.

AC-9(1) Previous Logon (Access) Notification | Unsuccessful Logons

Justification to Select: Although AC-9(1) is not selected in the CNSSI 1253 baseline or an overlay, AC-9(1) supports detection of exploitation, compromise, or other unauthorized disclosure by an insider threat, and may also provide a degree of prevention to the extent that insiders are aware of this detection capability.

Supplemental Guidance: This control enhancement should be implemented for logons managed by operating systems and applications. If a system does not notify the user of the number of unsuccessful logon/access attempts, then attempted misuse of their credentials by an insider threat might not be detected.

Regulatory/Statutory Reference(s): EO 13587, Section 2.1(b) and Section 5.2.

AC-10 Concurrent Session Control

Justification to Select: Although AC-10 is not selected in the CNSSI 1253 baseline or an overlay, AC-10 limits the number of concurrent sessions, which helps to prevent malicious insiders from hijacking such sessions, and helps identify possible compromises of user authenticators.

Supplemental Guidance: If a system does not limit the number of concurrent sessions, then an insider threat would have a greater opportunity to hijack a session without being detected.

Parameter Value(s): The information system limits the number of concurrent sessions for each *all accounts and account types (both privileged and non-privileged)* to *a maximum of 3 sessions*.

Regulatory/Statutory Reference(s): EO 13587, Section 2.1(b) and Section 5.2.

AC-11 Session Lock

Justification to Select: AC-11 is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system does not initiate and maintain a session lock after a period of inactivity, then an insider threat would be able to use the abandoned session to gain access to systems and information for which they have not been authorized.

Parameter Value(s): The information system:
a. Prevents further access to the system by initiating a session lock after *a time period not to exceed 15 minutes* of inactivity or upon receiving a request from a user; and
b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.

AC-11(1) Session Lock | Pattern-Hiding Displays

Justification to Select: AC-11(1) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system does not conceal information previously visible prior to the session lock, then an insider threat might be able to view information for which they have not been authorized.

AC-12 Session Termination

Justification to Select: AC-12 is selected in the CNSSI 1253 baseline categorized Moderate or High for Confidentiality or Integrity and in the Privacy Overlay for PHI. AC-12 is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The information system automatically terminates a user session after *a maximum of 30 minutes of inactivity and other trigger events requiring session disconnect (user sessions include both privileged and functional user sessions).*

AC-12(1) Session Termination | User-Initiated Logouts / Message Displays

Justification to Select: AC-12(1) is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The information system:
(a) Provides a logout capability for user-initiated communications sessions whenever authentication is used to gain access to *any and all information resources*; and
(b) Displays an explicit logout message to users indicating the reliable termination of authenticated communications sessions.

AC-14 Permitted Actions Without Identification or Authentication

Justification to Select: AC-14 is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization:
a. Identifies *no user actions* that can be performed on the information system without identification or authentication consistent with organizational mission's/business functions; and
b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.

AC-16 Security Attributes

Justification to Select: AC-16 is selected in the CNSSI 1253 baseline for all systems and in the Privacy Overlay for all Privacy Impact Levels and PHI. AC-16 is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization:

a. Provides the means to associate *security attributes* having *security attribute values* with information in storage, in process, and/or in transmission;

b. Ensures that the security attribute associations are made and retained with the information;

c. Establishes the permitted *security attributes* for *all information systems*; and

d. Determines the permitted *values or ranges* for each of the established security attributes.

AC-16(3) Security Attributes | Maintenance of Attribute Associations by Information System

Justification to Select: AC-16(3) is selected in the Privacy Overlay for all Privacy Impact Levels and PHI and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The information system maintains the association and integrity of *all security attributes* to *all subjects and objects*.

AC-16(6) Security Attributes | Maintenance of Attribute Association by Organization

Justification to Select: AC-16(6) is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization allows personnel to associate, and maintain the association of *all security attributes* with *all subjects and objects* in accordance with *established security policies*.

AC-17 Remote Access

Justification to Select: AC-17 is selected in the CNSSI 1253 baseline for all systems and in the Privacy Overlay for all Privacy Impact Levels and PHI. AC-17 is therefore applicable to systems or activities that directly support the Insider Threat Program.

AC-17(1) Remote Access | Automated Monitoring / Control

Justification to Select: AC-17(1) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system does not monitor and control remote access methods, then an insider threat could use a remote session to perform malicious activities without detection.

Automated methods can include employing tools or solutions that monitor the connection establishment, information flow, and resource accesses during remote access sessions to ensure ongoing compliance with remote access policies.

AC-17(2) Remote Access | Protection of Confidentiality / Integrity Using Encryption

Justification to Select: AC-17(2) is selected in the CNSSI 1253 baseline for all systems and in the Privacy Overlay for all Privacy Impact Levels and PHI. AC-17(2) is therefore applicable to systems or activities that directly support the Insider Threat Program.

AC-17(3) Remote Access | Managed Access Control Points

Justification to Select: AC-17(3) is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The information system routes all remote accesses through *a limited number of centrally* managed network access control points.

AC-17(4) Remote Access | Privileged Commands / Access

Justification to Select: AC-17(4) is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization:
(a) Authorizes the execution of privileged commands and access to security-relevant information via remote access only for *compelling operational (i.e., mission critical) needs*; and
(b) Documents the rationale for such access in the security plan for the information system.

AC-17(6) Remote Access | Protection of Information

Justification to Select: AC-17(6) is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

AC-17(9) Remote Access | Disconnect / Disable Access

Justification to Select: AC-17(9) is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: Disconnection methods can include pre-established processes, authorities, and permissions by the organization that are promptly implemented following initiation by a Security Administrator or other designated individuals.

Parameter Value(s): The organization provides the capability to expeditiously disconnect or disable remote access to the information system *immediately upon execution by the Security Administrator*.

AC-18(4) Wireless Access | Restrict Configurations by Users

Justification to Select: AC-18(4) is selected in the CNSSI 1253 baseline for all systems.

Supplemental Guidance: If a system and the organization do not identify and explicitly authorize users allowed to configure wireless networking capabilities, then an insider threat could establish an unauthorized wireless connection as a pathway for exploitation. Configuration of wireless networking is performed and managed at both the individual information system and enterprise levels.

AC-20 Use of External Information Systems

Justification to Select: AC-20 is selected in the CNSSI 1253 baseline for all systems and in the Privacy Overlay for all Privacy Impact Levels and PHI. AC-20 is therefore applicable to systems or activities that directly support the Insider Threat Program.

AC-20(2) Use of External Information Systems | Portable Storage Devices

Justification to Select: AC-20(2) is selected in the CNSSI 1253 baseline for all systems.

Supplemental Guidance: If a system or the organization does not restrict the use of organization-controlled portable media on external information systems, then an insider threat could use the media as a potential access and exfiltration path to sensitive information contained on the device. Such use also establishes a path for malicious code to be introduced onto the storage device from the external information system. Restricting the external use of portable storage devices is a key mitigation measure to these vulnerabilities. Management of portable storage devices is performed at both the individual device and enterprise levels.

Parameter Value(s): The organization *restricts* the use of organization-controlled portable storage devices by authorized individuals on external information systems.

AC-20(3) Use of External Information Systems | Non-Organizationally Owned Systems / Components / Devices

Justification to Select: AC-20(3) is selected in the CNSSI 1253 baseline for all systems.

Supplemental Guidance: If a system or the organization does not restrict the use of non-organizationally owned information systems, system components, or devices to process, store, or transmit organizational information, then an insider threat could use the systems, components and devices to access and exfiltrate sensitive information. Restricting the use of non-organizationally owned information systems, system components, or devices is a key mitigation

measure to this vulnerability. Management of non-organizationally owned information systems, system components, or devices is performed at both the individual information system and enterprise levels.

Parameter Value(s): The organization *restricts* the use of non-organizationally owned information systems, system components, or devices to process, store, or transmit organizational information.

AC-21 Information Sharing

Justification to Select: AC-21 is selected in the CNSSI 1253 baseline categorized Moderate or High for Confidentiality, and in the Privacy Overlay for all Privacy Impact Levels and PHI. AC-21 is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization:
a. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for *information sharing circumstances where user discretion is required (e.g., contract-sensitive information, proprietary information, personally identifiable information, classified information related to special access programs or compartments)*; and
b. Employs *automated mechanisms or manual processes* to assist users in making information sharing/collaboration decisions.

AC-22 Publicly Accessible Content

Justification to Select: AC-22 is selected in the CNSSI 1253 baseline for all systems for publicly accessible content. Although this control does not originally address non-publicly accessible content, the White House Memorandum, Near-term Measures to Reduce the Risk of High-Impact Unauthorized Disclosures, requires organizations to similarly conduct a review of all content contained on information sharing portals hosted on classified computer networks to identify particularly sensitive information that should not be shared with the full user population able to access it. Accordingly, the control's coverage has been expanded by the following control extension to include protective reviews for particularly sensitive information on classified networks.

Control Extension and Parameter Value(s): The organization shall, *quarterly or as new information is posted,* review the content on information sharing portals hosted on classified computer networks for particularly sensitive information that should not be shared with the full user population able to access it, and remove such information, if discovered.

Supplemental Guidance: If a system or the organization does not conduct a periodic review of all content contained on information sharing portals hosted on classified computer networks, then information may be inadvertently exposed to an insider threat without the proper access authorization. Reviews should be conducted at both the system and enterprise levels. Reports and other content containing particularly sensitive information shall be securely removed as soon as possible, or access otherwise terminate, until appropriate access control regimes are in place to

strictly limit readership to those with a need to know. The respective chief security officer shall be notified when such content is identified for spill determination and response.

Regulatory/Statutory Reference(s): White House Memo - Near-Term Measures to Reduce the Risk of High-Impact Unauthorized Disclosures, Section B-2.

AC-23 Data Mining Protection

Justification to Select: AC-23 is selected in the CNSSI 1253 baseline categorized Moderate or High for Confidentiality.

Supplemental Guidance: If a system does not employ data mining protection and detection techniques, then an insider threat could use data mining to collect sensitive and classified information for the purpose of exfiltration.

Parameter Value(s): The organization employs *data mining prevention and detection techniques* for *data storage objects (to include databases, database records, and database fields)* to adequately detect and protect against data mining.

Regulatory/Statutory Reference(s): EO 13587, Section 2.1(b) and Section 5.2.

AT-2 Security Awareness

Justification to Select: AT-2 is selected in the CNSSI 1253 baseline for all systems and is also selected in the Privacy Overlay at all Privacy Impact levels and PHI. AT-2 is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors):
a. As part of initial training for new users;
b. When required by information system changes; and
c. *At least annually, for as long as the user has access to the system,* thereafter.

AT-2(2) Security Awareness | Insider Threat

Justification to Select: AT-2(2) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program. The White House Memorandum, Minimum Standards for Executive Branch Insider Threat Programs, requires that organizations provide Insider Threat awareness training to all cleared employees.

Supplemental Guidance: If the organization does not include security awareness training on recognizing and reporting potential indicators of insider threat, then users will not be able to recognize potential insider threats and report them to the appropriate authority. DoDD 5205.16 directs organizations to incorporate insider threat education and awareness into annual Counterintelligence Awareness and Reporting (CIAR) training in accordance with DoD CIAR Policies.

White House Memo on Insider Threat directs:
1. Agency heads to ensure personnel assigned to the Insider Threat Program are fully trained in:

- Counterintelligence and security fundamentals to include applicable legal issues;
- Agency procedures for conducting insider threat response action(s);
- Applicable laws and regulations regarding the gathering, integration, retention, safeguarding, and use of records and data, including the consequences of misuse of such information;
- Applicable civil liberties and privacy laws, regulations, and policies; and Investigative referral requirements of Section 811 of the Intelligence. Authorization Act for FY 1995, as well as other policy or statutory requirements that require referrals to an internal entity, such as a security office or office of Inspector General, or external investigative entities such as the Federal Bureau of Investigation, the Department of Justice, or military investigative services.

2. Agency heads to ensure Insider Threat Programs provide insider threat awareness training, either in-person or computer-based, to all cleared employees within 30 days of initial employment, entry-on-duty (EOD), or following the granting of access to classified information, and annually thereafter. Training shall address current and potential threats in the work and personal environment, and shall include, at a minimum, the following topics:

- The importance of detecting potential insider threats by cleared employees and reporting suspected activity to insider threat personnel or other designated officials;
- Methodologies of adversaries to recruit trusted insiders and collect classified information;
- Indicators of insider threat behavior and procedure to report such behavior; and
- Counterintelligence and security reporting requirements, as applicable.

3. Agency heads to ensure Insider Threat Programs verify that all cleared employees have completed the required insider threat awareness training contained in these standards.

Regulatory/Statutory Reference(s): White House Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, Tab 2, Section I.1; DoDD 5205.16, Enclosure 2, Section 10.f; DoDD 5240.06; and DoDD-5240.02.

AT-3 Role-Based Security Training

Justification to Select: AT-3 is selected in the CNSSI 1253 baseline for all systems and is also selected in the Privacy Overlay baseline at all Privacy Impact levels and PHI. AT-3 is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization provides role-based security training to personnel with assigned security roles and responsibilities:

a. Before authorizing access to the information system or performing assigned duties;
b. When required by information system changes; and
c. *At least annually* thereafter.

AT-3(2) Role-Based Security Training | Physical Security Controls

Justification to Select: AT-3(2) is selected in the CNSSI 1253 baseline for all systems.

Supplemental Guidance: If the organization does not provide initial and periodic physical security training to security personnel, then an insider could bypass physical security controls

and protections without detection. Training in physical control systems is typically conducted at the enterprise level.

Parameter Value(s): The organization provides *all associated personnel and roles (e.g., Insider Threat Team employees and contractor support personnel)* with initial and *when sufficient changes are made to physical control systems or at least annual* training in the employment and operation of physical security controls.

AT-3(4) Role-Based Security Training | Suspicious Communications and Anomalous System Behavior

Justification to Select: AT-3(4) is selected in the CNSSI 1253 baseline for all systems.

Supplemental Guidance: If the organization does not provide training to users of suspicious communications and anomalous system behavior, then an insider threat could use malicious code to gain access to systems or information for which they have not been authorized. Training in malicious code protection is typically conducted at the enterprise level.

Parameter Value(s): The organization provides training to its personnel on *at least indicators of potentially malicious code in suspicious email* to recognize suspicious communications and anomalous behavior in organizational information systems.

AT-4 Security Training Records

Justification to Select: AT-4 is selected in the CNSSI 1253 baseline for all systems and in the Privacy Overlay for all Privacy Impact Levels and PHI. AT-4 is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization:
a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and
b. Retains individual training records for *a minimum of five (5) years*.

AU-1 Audit and Accountability Policy and Procedures

Justification to Select: AU-1 is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance:

If the organization does not establish, and periodically review and update, standardized enterprise policies and procedures for audit, then systems will not generate audit logs with the information required to detect insider threats and evaluate their activity.

Organizations should define and implement automated policy to include roles, responsibilities, and accountability for Security Professionals' (i.e., IAO, IAM, LE/CI) accessible audit accounts (Security Logs) and establish frequency of policy and procedure reviews/updates.

UAM alerts may provide the basis for Focused Observation of an insider threat using information system containing sensitive or classified information. Each organization must develop policy on Focused Observation that addresses how and when Focused Observation can be conducted.

Coordination of the policy and procedures is required due to the sensitivity of information collected for UAM and the potential need to employ information as evidence in legal proceedings. This will ensure that legal, civil liberties, and privacy protections are incorporated throughout the organization's Insider Threat Program.

Parameter Value(s): The organization:

a. Develops, documents, and disseminates to *all personnel*:
    1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and
b. Reviews and updates the current:
    1. Audit and accountability policy *at least annually*; and
    2. Audit and accountability procedures *at least annually*.

Regulatory/Statutory Reference(s): CNSSD 504, Sections B.2 and B.6; and CNSSI 1015, Annex A, Elements: M1.1, M1.2, T1.1, T1.2, T2.1, and T3.1.

AU-2 Audit Events

Justification to Select: AU-2 is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance:

If the organization does not specify the events for which systems are required to audit, then audit logs will not contain the information required to detect insider threats and evaluate their activity.

Organizations should define and implement audit events that enable audit triggers and alerts to effectively audit the organization. Organizations should also define thresholds and priorities to support audit triggers and alerts. Note: This is a continuous process influenced by the network/user environment and changing priorities and threats.

Systems shall have the ability to collect audit data through automated means and store the information securely. The information will be marked and handled at the appropriate classification and sensitivity levels.

Organizations should ensure enterprise audit is applied to all cross domain transfers and use of removable storage devices.

An observable occurrence within the information system or ICT supply chain infrastructure should be identified as an ICT supply chain auditable event, based on the organization's system

development lifecycle (SDLC) context and requirements. Auditable events may include software/hardware changes, failed attempts to access ICT supply chain infrastructure systems, or movement of source code. Information on such events should be captured by appropriate audit mechanisms and should be traceable and verifiable. Information captured may include type of event, date/time, length, and frequency of occurrence. Among other things, auditing may help detect misuse of the ICT supply chain infrastructure caused by Insider threat.

Organizations must share, where lawful and appropriate, audit data to support Information Assurance, business analytics, personnel security, and other community audit needs related to information resources.

Parameter Value(s): The organization:

a. Determines that the information system is capable of auditing the following events:
    1. Authentication events:
        (1) Logons (Success/Failure)
        (2) Logoffs (Success)
    2. File and Objects events:
        (1) Create (Success/Failure)
        (2) Access (Success/Failure)
        (3) Delete (Success/Failure)
        (4) Modify (Success/Failure)
        (5) Permission Modification (Success/Failure)
        (6) Ownership Modification (Success/Failure)
    3. Writes/downloads to external devices/media (e.g., A-Drive, CD/DVD devices/printers) (Success/Failure)
    4. Uploads from external devices (e.g., CD/DVD drives) (Success/Failure)
    5. User and Group Management events:
        (1) User add, delete, modify, suspend, lock (Success/Failure)
        (2) Group/Role add, delete, modify (Success/Failure)
    6. Use of Privileged/Special Rights events:
        (1) Security or audit policy changes (Success/Failure)
        (2) Configuration changes (Success/Failure)
    7. Admin or root-level access (Success/Failure)
    8. Privilege/Role escalation (Success/Failure)
    9. Audit and log data accesses (Success/Failure)
    10. System reboot, restart and shutdown (Success/Failure)
    11. Print to a device (Success/Failure)
    12. Print to a file (e.g., pdf format) (Success/Failure)
    13. Application (e.g., Firefox, Internet Explorer, MS Office Suite, etc.) initialization (Success/Failure)
    14. Export of information (Success/Failure) include (e.g., to CDRW, thumb drives, or remote systems)
    15. Import of information (Success/Failure) include (e.g., from CDRW, thumb drives, or remote systems);

b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;
c. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and
d. Determines that the following events are to be audited within the information system: *at every occurrence of all auditable events identified above;*

Regulatory/Statutory Reference(s): White House Memo - Near-Term Measures to Reduce the Risk of High-Impact Unauthorized Disclosures; CNSSI 1015; NDAA for Fiscal Year 2017, Subtitle F, Section 951, paragraph (a)(4); CNSSI 1015, Section 2 and Annex A, Elements: M1.3, T1.3, T2.3, and T3.3; and NIST SP 800-161.

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

Justification to Select: AU-2(3) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If the organization does not periodically review and update the events for which systems are required to audit, then audit logs may not contain the information required to detect insider threats and evaluate their activity.

Parameter Value(s): The organization reviews and updates the audited events *at least annually or as needed in response to situational awareness of threats and vulnerabilities.*

AU-3 Content of Audit Records

Justification to Select: AU-3 is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program. AU-3 is necessary to ensure audit records are generated to support the Insider Threat Program.

Supplemental Guidance: If the system does not generate audit records with the specified details, then audit logs will not contain the information required to detect insider threats and evaluate their activity.

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

Justification to Select: AU-3(1) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program. AU-3(1) is necessary to ensure audit records are generated with detailed information supporting the Insider Threat Program.

Supplemental Guidance: Organizations should define, implement and capture sufficient auditable content to be established as part of the record in support of the use cases. Organizations should ensure audit data is attributable to a unique user and/or information resource. Organizations should implement capability to dynamically change content of auditable events to support enterprise analysis use cases and event triggers.

If the system does not generate audit records with the specified details, then audit logs will not contain the information required to detect insider threats and evaluate their activity.

Parameter Value(s): The information system generates audit records containing the following additional information *in the audit records, at a minimum, full text recording of privileged commands or the individual identities of group account users, and:*

a. Date and time of the event using the common network time (e.g., Network Time Protocol),
b. Type of event (e.g., login, print, etc.),
c. Identifier indicating the source/system of the event activity,
d. Identifier indicating the identity of the subject or actor (e.g., UserId, ProcessId, etc.),
e. Details identifying any objects or resources accessed or involved (a.k.a.., Resource List - e.g., flies (including location), document id, peripherals, storage devices, etc.), and
f. Outcome (e.g., Success or Failure).

Regulatory/Statutory Reference(s): CNSSI 1015; and CNSSI 1015, Annex A, Elements: M1.5, M2.1, T1.5, T2.1, and T2.5.

AU-3(2) Content of Audit Records | Centralized Management of Planned Audit Record Content

Justification to Select: AU-3(2) is selected in the CNSSI 1253 baseline for systems categorized High for Confidentiality or Integrity, including systems or activities that directly support the Insider Threat Program. CNSSI 1015 requires that Departments and Agencies configure and implement audit management capabilities to effectively protect and defend information systems and they must implement, a capability to dynamically change content of auditable events to support enterprise analysis use cases and event triggers as outlined in CNSSI 1015, Annex A, Elements T2.1 and T2.5.

Supplemental Guidance: Organizations should implement the capability to dynamically change auditable content to support enterprise analysis of use cases and event triggers. If a system or the organization does not provide centralized management and configuration of the content to be captured in audit records, then decentralized, manual, configuration would result in delays in collecting the information required to detect insider threats and evaluate their activity.

Parameter Value(s): The information system provides centralized management and configuration of the content to be captured in audit records generated by *all information system, network, and CDS components*.

Regulatory/Statutory Reference(s): CNSSI 1015, Annex A, Elements T2.1 and T2.5.

AU-4 Audit Storage Capacity

Justification to Select: AU-4 is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program. AU-4 is necessary to ensure audit records are retained and available to support the Insider Threat Program.

Supplemental Guidance: If a system or the organization does not allocate sufficient audit record storage capacity, then audit records that are required to detect insider threats and evaluate their activity might not be retained. The organization should implement an enterprise-wide audit-data back-up storage solution.

Parameter Value(s): The organization allocates audit record storage capacity in accordance with *the organization's established audit procedures and configure auditing to reduce the likelihood of such capacity being exceeded. Storage allocation must be sufficient to maintain the required audit information, without adversely affecting the operational requirements of the information system. Audit data should not be overwritten under any circumstances.*

Regulatory/Statutory Reference(s): CNSSI 1015, Annex A, Element T3.13.

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

Justification to Select: AU-4(1) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program. AU-4(1) is necessary to ensure audit records are retained and available to support the Insider Threat Program.

Supplemental Guidance: If a system or the organization does not offload audit records onto a different system or media other than the system being audited, then an insider threat may alter or delete the audit record and thereby obfuscate their activity from detection and evaluation. Organizations should automate backup of data records to external system within an organizationally defined timeframe, not to exceed one day.

Parameter Value(s): The information system off-loads audit records *in near real-time for interconnected systems and at least weekly for stand-alone systems* onto a different system or media than the system being audited.

Regulatory/Statutory Reference(s): CNSSI 1015, Annex A, Element T2.13.

AU-5 Response to Audit Processing Failures

Justification to Select: AU-5 is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program. AU-5 is necessary to ensure audit records are continuously generated to support the Insider Threat Program.

Supplemental Guidance: Organizations should define and implement a procedure for alert function in the event of loss-of-audit capability at the device, logger, storage capability, or analyst's desktop and implement organizationally defined, automated remediation strategies to audit system failures. If a system does not detect and send alert(s) in the event of audit processing failure, then an insider threat could take advantage of the failure to perform malicious activities without detection.

Parameter Value(s): The information system:
a. Alerts *the System Administrator and/or Security Administrator, and Security Operations Center* in the event of an audit processing failure; and
b. Takes the following additional actions:

(1) If possible, record the details of any audit processing failure in the audit record; and (2) Configure all Enterprise Servers, to include Domain Controllers and Exchange Servers, to overwrite the oldest audit files, if their audit logs reach capacity prior to being archived and thereby prevent these enterprise systems from crashing upon failure to audit.

Regulatory/Statutory Reference(s): CNSSI 1015, Annex A, Elements: M1.7, T1.7, and T3.7.

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

Justification to Select: AU-5(1) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program. AU-5(1) is necessary to ensure audit records are retained and available to support the Insider Threat Program.

Supplemental Guidance: If a system does not provide a warning when the audit record storage is reaching capacity, then appropriate actions might not be taken in time to preclude loss of audit records, to include insider threat activity, when the maximum capacity is reached.

Parameter Value(s): The information system provides a warning to *system administrators and IA personnel* within *a twelve-hour time period* when allocated audit record storage volume reaches *75 percent* of repository maximum audit record storage capacity.

AU-5(2) Response to Audit Processing Failures | Real-Time Alerts

Justification to Select: AU-5(2) is selected in the CNSSI 1253 baseline for systems categorized High for Availability, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: Audit processing failures involving an inability to continue the collection or retention of audit records create an effective blind spot; appropriate personnel need to be made aware of such failures as soon as possible. If a system does not provide an alert when an audit failure occurs, then insider threat activity occurring during the failure might not be detected.

Parameter Value(s): The information system provides an alert in *real-time (within 10 seconds) alert* to *system administrators, IA personnel (e.g., security administrator) and duty officer responsible for enterprise continuous monitoring* when the following audit failure events occur *(minimally but not limited to): auditing software/hardware errors; failures in the audit capturing mechanisms; an audit storage capacity being reached or exceeded; or an audit processing failure resulting in a degraded ability to collect or retain audit records*.

Regulatory/Statutory Reference(s): EO 13587, Section 2.1(b) and Section 5.2 (a); White House Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, Tab 1, Section B.2(1), Tab 2, Section H; and CNSSI 1015, Annex A, Element T2.7.

AU-6 Audit Review, Analysis, and Reporting

Justification to Select: AU-6 is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program. AU-6 is necessary to detect potential insider threat activity.

Control Extension:

The organization accomplishes user activity monitoring through the implementation of triggers that monitor user activities on a network.

Control Extension:

The information system alerts *insider threat personnel monitoring user activity* when specific anomalous activities occur that may be indicators of insider threat behavior.

Supplemental Guidance: If a system or the organization does not review and analyze audit records and report their findings, then potential insider threat activity captured by the audit records would not be detected and evaluated.

Reviewing and analyzing audit records support the detection of insider threat activities. Organizations should define how analysts receive and evaluate information to execute response action, define an organizational reporting frequency, and report findings at that organizationally defined frequency.

Triggers generate data to facilitate the detection of potentially anomalous user activities indicative of insider threats. Triggers are a set of logic statements to be applied to a data stream or a specification of data to be collected when a specific activity or event occurs and thereby produces an alert when an anomalous incident or behavior occurs.

Triggers are most effective if they are designed to highlight activities that reflect the habits, techniques, and tradecraft of insider threats. Triggers will often be specific to the mission activities of a given IC elements. Triggers should be developed and applied in a non-discriminatory manner, based on knowledge and experience of the habits, techniques, and trade-craft of persons who misuse access to IC information resources.

Triggers should be capable of detecting insider threats proactively on an ongoing basis, ideally close to real-time. When a user activity meets the trigger threshold, an automated alert should prompt an assessment by authorized personnel, subject to rules and procedures defied by the responsible office.

Organizations shall ensure triggers are appropriately tailored to the purpose of the collection, consistent with applicable law, policy and Constitutional safeguards. Organizations shall establish guidance for assessing supposed anomalous activity (i.e. triggered events) prior to undertaking any adverse action or determination with regard to the system user.

Each organization must implement a comprehensive detection program within their capabilities by using a combination of triggers. Each organization should develop and maintain current triggers that reflect the unique environment of the individual organization. The organization should employ the following process to select triggers for implementation:

a. Complete a periodic inventory of all information, files, and systems owned by the organization, then determine which ones are most at risk to insider threats.
b. Identify and prioritize targets within NSS to which authorized users have access.
c. Identify the potential insider threat behaviors and prioritize based on risks; Table 1 lists 11 categories of user behaviors to consider.
d. Identify the data required to evaluate the potential insider threat behavior and select and define triggers that will generate the required data. The following events or indicators are recommended for consideration because they have proven to be effective indications of anomalous behavior:
    - Account Change
    - Authentication Failure/Anomaly
    - Baseline Anomaly
    - Excessive Activity
    - Evidence Tampering
    - Exfiltration
    - Malware
    - Network Traffic Anomaly
    - Privilege Violation
    - System Configuration Change
    - User Behavior Anomaly
e. The Insider Threat Program Office of each organization must review and approve, in consultation with legal counsel, and civil liberties, and privacy officials, the insider threat triggers to be implemented.
f. The trigger specification may include a threshold for a value, date/time, number of occurrences, or location. The threshold limits the generation of data to activities considered anomalous and thereby improves the value of the data.
g. The data generated by triggers must be provided to the Insider Threat Program for storage, analysis, and [referral for] possible investigative action.
h. Where appropriate, a referral should be made to the appropriate security and /or investigative authorities and reported in accordance with the requirements of EO 13462, as amended, President's Intelligence Advisory Board and Intelligence Oversight board.
i. Each organization must periodically evaluate the effectiveness of their triggers to facilitate the detection of anomalous user activities indicative of insider threats. This evaluation may cause organization to add, delete or modify triggers. The organization must add a trigger if additional data is required for effective analysis and it is not available from another source. Organization must modify triggers if the threshold needs to be modified or additional data attributes need to be collected.

Parameter Value(s): The organization:

a. Reviews and analyzes information system audit records *at least on a weekly basis or more frequently if required by an alarm or anomaly, or as directed by the Authorizing Official (AO)*for indications of *inappropriate or unusual activity (including any user having a number of concurrent sessions that are higher than normal for that user)*; and

b. Reports findings to, *at a minimum, the Security Administrator, ISSO and ISSM*.

Regulatory/Statutory Reference(s): EO 13587, Section 2.1(b) and Section 5.2; White House Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, Tab 1, Section B.2(1) and Tab 2, Section H; CNSSI 1015; CNSSD 504, Sections B.2, B.9, B.10, and B.12; and CNSSI 1015, Annex A, Elements: M1.9, MI.10., and TI.10.

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

Justification to Select: AU-6(1) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program. AU-6(1) is necessary to promptly detect and report potential insider threat activity.

Supplemental Guidance: Organizations should implement an automated audit process for:

- Audit review
- Audit analysis
- Indication of anomalies,
- Reporting of unusual activities
- Reporting for events with selectable remediation criteria
- Reporting capabilities to support situational awareness and other organizationally defined defensive activities
- Generating Security Content Automation Protocol (SCAP)-compliant data

If the organization does not employ automated mechanisms to integrate audit processes in support of incident analysis and response, then the efficient and effective analysis of, and response to, potential insider threat activity will be impeded.

Regulatory/Statutory Reference(s): CNSSI 1015, Annex A, Elements: M1.11. T2.2, T2.3, T2.10, and T3.10.

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

Justification to Select: AU-6(3) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program. AU-6(3) is necessary to promptly detect and report potential insider threat activity.

Supplemental Guidance: If the organization does not analyze and correlate audit records across different repositories to gain an organization-wide situational awareness, then low-level, widely-distributed, insider threat activity might not be detected.

Organizations shall define event reduction and correlation methodology to support threat determination and collect and share audit data and maintain audit capabilities to support CI, security and other needs. Audit data collected shall be used to identify, proactively or retrospectively, electronic activity by personnel that may be indicative of an insider threat. Organizations shall implement audit data-monitoring tools for enterprise-wide situational status, event profiles, risk matrix, and dashboards (remediation). Organizations shall implement audit

reduction and correlation at an organizationally defined location and provide correlated event alerts to a community-defined location.

Regulatory/Statutory Reference(s): NDAA for Fiscal Year 2017, Subtitle F, Section 951, paragraph (a)(4); and CNSSI 1015, Annex A, Elements: M1.8 T2.8, T3.8, and T3.9.

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

Justification to Select: AU-6(4) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program. AU-6(4) and is necessary to promptly detect and report potential insider threat activity.

Supplemental Guidance: Organizations should implement automated centralized management of audit record content, event reduction and correlation at a centralized location, and an audit review capability that generates SCAP-compliant data supporting automation. If the organization does not implement centralized audit record review and analysis, then low-level, widely-distributed, insider threat activity might not be detected.

Regulatory/Statutory Reference(s): White House Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, Tab 2, Section E.1; and CNSSI 1015, Annex A, Elements: T1.8, T2.11, and T3.5.

AU-6(5) Audit Review, Analysis, and Reporting | Integration / Scanning and Monitoring Capabilities

Justification to Select: AU-6(5) is selected in the CNSSI 1253 baseline for systems categorized High for Confidentiality or Integrity, including systems or activities that directly support the Insider Threat Program. AU-6(5) is also commonly applied for systems categorized as Low or Moderate for Confidentiality or Integrity to detect insider threat activities at these lower categorization levels.

Supplemental Guidance: Organizations should build and maintain an insider threat analytic and response capability to manually and/or electronically gather, integrate, review, assess, and respond to information derived from counterintelligence, security, information assurance, human resources, law enforcement, the monitoring of user activity, and other sources as necessary and appropriate. If the organization does not integrate analysis of audit records with other relevant (non-audit) information, then the full context of an insider threat's logged activities would not be understood and those activities might be overlooked.

Parameter Value(s): The organization integrates analysis of audit records with analysis of *counterintelligence, security, information assurance, human resources, law enforcement, the monitoring of user activity and other sources as necessary and appropriate* to further enhance the ability to identify inappropriate or unusual activity.

Regulatory/Statutory Reference(s): EO 13587, Section 2.1(b) and Section 5.2 (a); White House Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch

Insider Threat Programs, Tab 1, Section B.2(1), Tab 2, Section E.1; and NDAA for Fiscal Year 2017, Subtitle F, Section 951, paragraph (a)(4).

AU-6(6) Audit Review, Analysis, and Reporting | Correlation with Physical Monitoring

Justification to Select: AU-6(6) is selected in the CNSSI 1253 baseline for systems categorized High for Confidentiality or Integrity, including systems or activities that directly support the Insider Threat Program. AU-6(6) is commonly applied for systems categorized as Low or Moderate for Confidentiality or Integrity to detect insider threat activities at these lower categorization levels.

Supplemental Guidance: Audit data shall be analyzed in conjunction with other available data, to include facility access information, to support detection, mitigation or assessment of insider threats. If the organization does not integrate analysis of audit records with physical access information, then an insider threat could compromise another user's account without detection.

Regulatory/Statutory Reference(s): EO 13587, Section 2.1(b) and Section 5.2 (a);; White House Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, Tab 1, Section B.2(1), Tab 2, Section H; and NDAA for Fiscal Year 2017, Subtitle F, Section 951, paragraph (a)(4).

AU-6(8) Audit Review, Analysis, and Reporting | Full Text Analysis of Privileged Commands

Justification to Select: Although AU-6(8) is not selected in the CNSSI 1253 baseline or an overlay, AU-6(8) is commonly implemented to comply with the White House Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, which requires agencies to monitor and audit user activity on classified networks. Insider Threat Programs have determined that full text analyses of all privileged user commands need to be performed to effectively execute task C-5 of the White House Memorandum, Near-term Measures to Reduce the Risk of High-Impact Unauthorized Disclosures.

Supplemental Guidance: Organizations should establish an ongoing practice that Insider Threat Program personnel analyze audit data relating to the actions of privileged users.

Regulatory/Statutory Reference(s): EO 13587, Section 2.1(b) and Section 5.2 (a); White House Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, Tab 1, Section B.2(1), Tab 2, Section H; White House Memorandum, Near-term Measures to Reduce the Risk of High-Impact Unauthorized Disclosures, Task C-5; and NDAA for Fiscal Year 2017, Subtitle F, Section 951, paragraph (a)(4).

AU-6(9) Audit Review, Analysis, and Reporting | Correlation with Information from Nontechnical Sources

Justification to Select: Although AU-6(9) is not selected in the CNSSI 1253 baseline or an overlay, AU-6(9) is commonly implemented to comply with the White House Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat

Programs, which requires agencies to build and maintain an insider threat analytic and response capability to manually and/or electronically gather, integrate, review, assess and respond to information derived from CI, Security, IA, HR, LE, the monitoring of user activity, and other sources as necessary and appropriate.

Supplemental Guidance: Non-technical sources may include, but is not limited to:
a. Foreign contact information;
b. Foreign travel information;
c. Personnel security information; and
d. Financial disclosure information.

Regulatory/Statutory Reference(s): White House Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, Tab 1, Section B.2 (2, 4), Tab 2, Section E.1; and NDAA for Fiscal Year 2017, Subtitle F, Section 951, paragraph (a)(4).

AU-6(10) Audit Review, Analysis, and Reporting | Audit Level Adjustment

Justification to Select: AU-6(10) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program. AU-6(10) is necessary to detect and report potential insider threat activity in a dynamic environment.

Supplemental Guidance: If a system or the organization does not dynamically adjust the level of audit review, analysis, and reporting when there is a change in insider threat risk, then an insider threat's activity might not be detected.

AU-7 Audit Reduction and Report Generation

Justification to Select: AU-7 is selected in the CNSSI 1253 baseline for systems categorized High for Confidentiality or Integrity, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If the organization does not provide an audit reduction and report generation capability that readily and uncompromisingly supports security incident investigation, then an insider threat's activities might not be able to be properly assessed. Audit aggregation, reduction and report generation is typically performed at the enterprise level.

Regulatory/Statutory Reference(s): EO 13587, Section 2.1(b) and Section 5.2 (a); White House Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, Tab 1, Section B.2(1), Tab 2, Section H.

AU-7(1) Audit Reduction and Report Generation | Automatic Processing

Justification to Select: AU-7(1) is selected in the CNSSI 1253 baseline for systems categorized High for Confidentiality or Integrity, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If the organization does not provide the capability to fully process audit records for events of interest, then an inside threat's activity might not be detected. Automatic processing of audit records for events of interest is typically performed at the enterprise level.

Parameter Value(s): The information system provides the capability to process audit records for events of interest based on *at a minimum, date/time of events; user identifiers; IP addresses involved in the event; type of event; and event success/failure of all auditable events defined in AU-2 per occurrence*.

Regulatory/Statutory Reference(s): EO 13587, Section 2.1(b) and Section 5.2 (a); White House Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, Tab 1, Section B.2(1), Tab 2, Section H.

AU-7(2) Audit Reduction and Report Generation | Automatic Sort and Search

Justification to Select: AU-7(2) is selected in the Privacy Overlay for Privacy Impact Levels of Moderate or High, and for PHI and is therefore applicable to systems or activities that directly support the Insider Threat Program. Although AU-7(2) is not selected in the CNSSI 1253 baseline, it is required to perform automatic searching of audit records and should therefore be applicable to all systems.

Supplemental Guidance: If the organization does not provide the capability to sort and search audit records for events of interest based on their content, then the organization would be unable to fully analyze and detect an insider threat's activities. Organizations should define and implement audit data-tagging methodology to enable metadata look-ups of audit content by authorized analysts. The ability to sort and search audit records for events of interest is typically implemented at the enterprise level.

Parameter Value(s): The information system provides the capability to sort and search audit records for events of interest based on the content of *audit records fields including: date/time, user identifiers, IP addresses, type, and success/failure of all auditable events defined in AU-2 per occurrence*.

Regulatory/Statutory Reference(s): EO 13587, Section 2.1(b) and Section 5.2 (a); White House Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, Tab 1, Section B.2(1), Tab 2, Section H; and CNSSI 1015, Annex A, Elements: M1.6 and T2.6.

AU-8 Time Stamps

Justification to Select: AU-8 is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program. AU-8 is necessary to correlate audit events across separate devices, information systems, and networks.

Supplemental Guidance: If a system does not generate accurate universal time stamps for audit record entries, then an insider threat's activities might not be correlated across systems or networks.

Parameter Value(s): The information system:
a. Uses internal system clocks to generate time stamps for audit records; and
b. Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets *a one-second granularity of time measurement.*

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

Justification to Select: AU-8(1) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program. AU-8(1) is necessary to correlate audit events across separate devices, information systems, and networks.

Supplemental Guidance: Organizations should define an authoritative source clock for synchronizing organizational internal information system clocks and implement the internal information system clock synchronization with the authoritative source for the collected audit data. If a system does not generate accurate authoritative time stamps for audit record entries, then an insider threat's activities might not be correlated across systems or networks.

Parameter Value(s): The information system:
(a) Compares the internal information system clocks *at least every 12 hours with an organization defined authoritative time source that complies* with *the provisions of IC Standard 500-6*; and
(b) Synchronizes the internal system clocks to the authoritative time source when the time difference is greater than *the organizationally defined granularity in AU-8 (one second).*

Regulatory/Statutory Reference(s): CNSSI 1015, Annex A, Elements: M1.12, T1.12, and T2.12.

AU-9 Protection of Audit Information

Justification to Select: AU-9 is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program. AU-9 is necessary to ensure the integrity of the audit record.

Supplemental Guidance: Audit data shall be protected from unauthorized access, modification, or destruction and shall be safeguarded in accordance with applicable law, policy, and department or agency regulations, at rest, in transit, and during presentation, to include appropriate limitations on access and use. Organizations should define the protection mechanisms for audit data, including frequency, cryptographic process, and accesses consistent with automation goals and ensure audit data relating to the actions of privileged users are stored beyond the reach of those users and that all accesses to the data are also audited. Organizations should also consolidate audit data to facilitate review and implement protection mechanisms to limit access to audit data records (from source or backup) to authorized users. Organizations should establish guidance to ensure against misuse of audit data. If a system or the organization

does not protect audit information and audit tools from unauthorized access, modification, and deletion, then an insider threat might alter or delete those records or tools.

Regulatory/Statutory Reference(s): CNSSI 1015; White House Memo - Near-Term Measures to Reduce the Risk of High-Impact Unauthorized Disclosures, Section C-4; and CNSSI 1015, Annex A, Elements: M1.14 and T1.14.

AU-9(2) Protection of Audit Information | Audit Backup on Separate Physical Systems / Components

Justification to Select: AU-9(2) is selected in the CNSSI 1253 baseline categorized High for Availability and in the Privacy Overlay for all Privacy Impact Levels and PHI. AU-9(2) is therefore applicable to systems or activities that directly support the Insider Threat Program. CNSSI 1015 requires that Departments and Agencies define automated processes to achieve and ensure back-up of audit data, within an organizationally defined frequency, for all devices and implement backup of data records on an information system or media separate from the originating source as outlined in CNSSI 1015, Annex A, Elements M1.13and T1.13. Therefore, AU-9(2) is applicable to all systems.

Supplemental Guidance: Organizations should define automated processes to achieve and ensure back-up of audit data, within an organizationally defined frequency, for all devices. If a system does not back up audit records periodically onto a physically different system or system component than the system or component being audited, then the historical record of an insider threat's activity might not be recovered following a system failure.

Parameter Value(s): The information system backs up audit records *at least weekly* onto a physically different system or system component than the system or component being audited.

Regulatory/Statutory Reference(s): CNSSI 1015, Annex A, Elements: M1.13 and T1.13.

AU-9(3) Protection of Audit Information | Cryptographic Protection

Justification to Select: AU-9(3) is selected in the CNSSI 1253 baseline categorized High for Integrity and in the Privacy Overlay for Privacy Impact Levels of Moderate or High, and for PHI. AU-9(3) is therefore applicable to systems or activities that directly support the Insider Threat Program. CNSSD 504 requires that user activity data be protected from unauthorized access, modification, or destruction. The proper application of cryptographic mechanisms can protect the integrity and confidentiality of user activity data. Therefore, AU-9(3) is applicable to all systems.

Supplemental Guidance: If a system or the organization does not implement cryptographic mechanisms to protect the integrity of audit information and audit tools, then an insider threat might alter or replace those records or tools without detection.

User activity data must be protected from unauthorized access, modification, or destruction. User activity monitoring (UAM) activities and data are highly sensitive for the following reasons:

a. Privacy Information: UAM data may contain private information such as social security numbers and passwords.
b. Potential to Damage an Individual's Reputation: The fact that an individual is being monitored for insider threat behaviors is sensitive information. If divulged, it could impact a user's career or an ongoing investigation.
c. Alert Malfeasance: UAM tactics, techniques and procedures, if generally known, would permit insiders to change their tradecraft or computer activity to avoid detection.
Audit and user activity data must be protected commensurate with the highest level of sensitivity and classification of the aggregated information.

Regulatory/Statutory Reference(s): CNSSD 504, Section B.3.

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

Justification to Select: AU-9(4) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program. AU-9(4) is necessary to ensure the content and integrity of the audit record.

Control Extension: The organization ensures that personnel authorized to access audit information are trained regarding all applicable laws policies and the consequences of misuse of audit data.

Control Extension: The organization performs oversight of compliance by audit personnel and monitors audit personnel activities.

Supplemental Guidance: If a system or the organization does not limit and specifically authorize management of audit functionality, then any insider threat with privileged user status could change the audit configuration such that their activity would be undetected.

Organizations shall develop procedures for access audit data ensuring that access is restricted to personnel who require the information to perform their authorized functions, oversees compliance by audit personnel and monitors their activities. The organization shall provide training to all personnel authorized to access the data regarding all applicable laws and policies and the consequences of misuse of data for personal or other unauthorized purposes

Parameter Value(s): The organization authorizes access to management of audit functionality to only *a limited subset of privileged users. Access shall be further restricted by distinguishing between privileged users with audit-related privileges and privileged users without audit-related privileges to improve audit integrity*.

Regulatory/Statutory Reference(s): CNSSI 1015

AU-9(6) Protection of Audit Information | Read Only Access

Justification to Select: Although AU-9(6) is not selected in the CNSSI 1253 baseline or an overlay, AU-9(6) is commonly implemented to restricting audit information access to read-only helps to prevent malicious Insiders from altering or removing audit records, and thereby supports the detection of insider threat activities.

Supplemental Guidance: If a system or the organization does not implement read-only access to audit records by designated personnel, then an insider threat could access, and then alter or remove, the audit records.

Parameter Value(s): The organization authorizes read-only access to audit information to *designated Audit Reviewers, Cyber Security Operations Teams, and other Program of Record Personnel who have been individually appointed and designated by name in advance in writing*.

Regulatory/Statutory Reference(s): EO 13587, Section 2.1(b) and Section 5.2 (a); White House Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, Tab 1, Section B.2(1), Tab 2, Section H; and CNSSI 1015.

AU-10 Non-Repudiation

Justification to Select: AU-10 is selected in the CNSSI 1253 baseline categorized Moderate or High for Integrity and in the Privacy Overlay for Privacy Impact Levels of Moderate or High, and for PHI. AU-10 is therefore applicable to systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system does not fully and properly implement non-repudiation, then an insider threat might not be held accountable for malicious activity.

Parameter Value(s): The information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed *actions including, but not limited to creating information for CDS transfer, sending and receiving information via CDS transfer, approving information for CDS transfer, or the signatory of not having electronically signed a document*.

Regulatory/Statutory Reference(s): EO 13587, Section 2.1(b) and Section 5.2 (a); White House Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, Tab 1, Section B.2(1), Tab 2, Section H.

AU-10(1) Non-Repudiation | Association of Identities

Justification to Select: AU-10(1) is selected in the Privacy Overlay for Privacy Impact Levels of Moderate or High, and for PHI. AU-10(1) is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The information system:
(a) Binds the identity of the information producer with the information to *strength of binding levels appropriate to the classification or sensitivity of the information to provide a high level of assurance*; and
(b) Provides the means for authorized individuals to determine the identity of the producer of the information.

AU-10(3) Non-Repudiation | Chain of Custody

Justification to Select: Although AU-10(3) is not selected in the CNSSI 1253 baseline or an overlay, CNSSD 504 paragraph B.4 requires the heads of Departments and Agencies ensure the chain of custody of user activity data is preserved in coordination with the organizations legal counsel. Therefore, AU-10(3) is applicable for the Insider Threat Program

Control Extension: The organization shall ensure the chain of custody of user activity data is preserved in coordination with the organization's legal counsel.

Regulatory/Statutory Reference(s): CNSSD 504, Section B.4.

AU-11 Audit Record Retention

Justification to Select: AU-11 is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program. AU-11 is necessary to ensure audit records are maintained for long-term incident analysis and criminal investigations.

Supplemental Guidance: Organizations should develop and implement a plan for retention of audit data for an organizationally defined period (pursuant to the Federal Records Act and in accordance with the applicable records control schedule) to support investigations and support detection of behavioral patterns and relationships with other insider threats. Organizations should also implement an automated capability for expiration of retained audit data. If the organization does not retain audit records for the specified period, then an insider threat's long-term activity would not be available for correlation with recent activity and go undetected.

Parameter Value(s): The organization retains audit records for:
a. Not less than 5-years for Sensitive Compartmented Information;
b. Not less than 5-years for Sources and Methods Intelligence information; and
c. Not less than 1-year for all other information (Unclassified through Collateral Top Secret)
to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

Regulatory/Statutory Reference(s): CNSSD 504 paragraph B.11; CNSSI 1015; and CNSSI 1015, Annex A, Elements: M1.15, T1.15, and T2.15.

AU-11(1) Audit Record Retention | Long-Term Retrieval Capability

Justification to Select: AU-11(1) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program. AU-11(1) is necessary to ensure audit records are readily accessible for long-term incident analysis and criminal investigations.

Supplemental Guidance: If the organization does not employ a capability to access audit records for the duration of the required retention period, then long-term audit records generated by the

information system, which include insider threat activity, might not be available to be retrieved for analysis.

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

AU-12 Audit Generation

Justification to Select: AU-12 is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program. AU-12 is necessary to ensure audit records are generated with the necessary content for incident detection and analysis.

Control Extension and Parameter Value(s): The organization shall verify the ability to perform enterprise audit on information sharing portals hosted on classified computer networks *quarterly* and non-compliant portals shall be appropriately secured or removed.

Supplemental Guidance: If a system does not properly generate audit records in accordance with the enterprise audit standards as applied by the audit administrators, then the information needed to fully assess insider threat activity might not be captured in the audit record.

The list of audited events for specific components within an IT system is determined as part of the assessment process. The list of audited events should not be modified following authorization without approval of the Authorizing Official or his designated representative. Organizations that need to share audit information with other organizations must also generate sufficient audit data to satisfy, at a minimum, the mandatory elements of the ODNI Audit.XML specification.

Following evaluation for audit compliancy (as specified in the Control Extension), non-compliant portals shall be appropriately secured (e.g., configured in accordance with the applicable STIG or other configuration guidance) or removed.

Parameter Value(s): The information system:
a. Provides audit record generation capability for the auditable events defined in AU-2 a. at *all information systems and network components*;
b. Allows *only the Audit Administrator, as designated by the ISSM,* to select which auditable events are to be audited by specific components of the information system; and
c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.

Regulatory/Statutory Reference(s): EO 13587, Section 2.1(b) and Section 5.2 (a); White House Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, Tab 1, Section B.2(1), Tab 2, Section H.1; CNSSI 1015; and White House Memo - Near-Term Measures to Reduce the Risk of High-Impact Unauthorized Disclosures, Section B-1.

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

Justification to Select: AU-12(1) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.AU-12(1) is necessary to correlate audit events across separate devices, information systems, and networks.

Supplemental Guidance: If a system and the organization do not compile audit records into a system-wide, time-correlated, audit trail, then low-level, widely-distributed, insider threat activity might not be detected.

Parameter Value(s): The information system compiles audit records from *all information system components* into a system-wide (logical or physical) audit trail that is time-correlated to within *the time tracking tolerance defined in AU-8 (one second).*

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

Justification to Select: AU-12(3) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program. AU-12(3) is necessary to ensure audit records are generated with the necessary content for incident detection and analysis.

Supplemental Guidance: If a system or the organization does not provide designated personnel the capability to change audit parameters, then the organization would not be able to promptly capture activity related to evolving insider threat methodology.

Parameter Value(s): The information system provides the capability for *system administrators* to change the auditing to be performed on *all information system components that have the ability to perform audit logging functions* based on *a specific set of events to facilitate audit reduction, analysis, and reporting* within *near real-time*.

AU-14 Session Audit

Justification to Select: AU-14 is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program. AU-14 is necessary to collect session detail for insider threat incident detection and analysis. The White House Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, requires the capability to capture audit information to detect and mitigate insider threat and requires agencies to monitor and audit user activity on classified and unclassified networks. This control directly supports the capture of user activities during sessions. Having the capability to generate audit records containing this content is considered a best practice for safeguarding against insider threat.

Supplemental Guidance: If a system or the organization does not provide the ability to select a specific user session to monitor, then the organization would be unable to perform full contextual analysis of the activity of a specific insider threat.

The capability to perform full session and user activity monitoring (e.g., monitoring keystrokes, tracking websites visited, and recording information and/or file transfers) is typically achieved through a combination of auditing and monitoring solutions (e.g., enterprise audit, user activity

monitoring, network boundary/gateway monitoring, etc.). For host based capabilities, individual IT systems must install and/or configure this capability on all devices and verify its proper functionality with the centralized enterprise systems.

The collection of user activity data will:

a. Enable the organization to identify and evaluate anomalous activity involving NSS.
b. Enable the organization to identify and assess misuse (witting or unwitting), and/or exploitation of NSS by insiders.
c. Support authorized inquiries and investigations.

CNSSD 504 requires all departments and agencies to have the following minimum user activity monitoring (UAM) capabilities to collect user activity data for all NSS: key stroke monitoring and full application content (e.g., email, chat, data import, data export), obtain screen captures, and perform file shadowing for all lawful purposes. UAM is the technical capability to observe and record the actions and activities of all users, at any time, on any device accessing NSI in order to detect insider threats and to support authorized investigations. UAM data must be attributable to a specific user. The organization should incorporate this data into an analysis system capable of identifying anomalous behavior that may provide indications of insider threat activity and support organization investigative requests. These capabilities must be used only in accordance with applicable law, policy and regulations. Each organization must consult with legal counsel before employing such capabilities. Each organization must develop internal processes and procedures for using these capabilities and the information collected in consultation with their respective legal counsel, civil liberties officials and privacy officials.

Organizations should ensure Insider Threat Programs include, either internally or via agreement with external agencies, the technical capability, subject to appropriate approvals, to monitor user activity on all classified networks in order to detect activity indicative of insider threat behavior. When necessary, Service Level Agreements (SLA's) should be executed with all other agencies that operate or provide classified network connectivity or systems. SLAs should outline the capabilities the provider will employ to identify suspicious user behavior and how that information shall be reported to the subscriber's insider threat personnel.

The organization’s providers of computers, networks and services must provide support to the subscriber to facilitate the implementation of UAM. The details of the support must be defined in a Service Level Agreement (SLA). The SLA must define how UAM capabilities will be maintained, updated, and how data will be collected and transmitted to the subscriber.

Regulatory/Statutory Reference(s): White House Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, Tab 1, Section B.2 (1), Tab 2, Section H.1; NDAA for Fiscal Year 2017, Subtitle F, Section 951, paragraph (a)(4); CNSSD 504, Annex B, Section 5, 7 and 8; Intelligence Community Enterprise Audit Conceptual Framework, Section 2.2.2; and CNSSI 1015.

AU-14(1) Session Audit | System Start-Up

Justification to Select: AU-14(1) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program. AU-14(1) is necessary to collect session detail for insider threat incident detection and analysis.

Supplemental Guidance: If a system or the organization does not initiate session audit upon start up, then insider threat activity performed before session audit initiation would not be available for analysis.

AU-14(2) Session Audit | Capture/Record and Log Content

Justification to Select: AU-14(2) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program. AU-14(2) is necessary to collect session detail for insider threat incident detection and analysis.

Supplemental Guidance: If a system or the organization does not provide the ability to select a specific user session to monitor and log, then the organization would be unable to perform full contextual analysis of the activity of a specific insider threat over time.

Insider threat organizations should have the capability to collect key strokes and full application content (email, chat, imports, exports, etc.), obtain screen captures, and perform file shadowing for all lawful purposes, to include detecting unauthorized use or disclosure. Organizations should develop internal processes and procedures for using these specific capabilities and the information collected, in consultation with their respective legal counsel and civil liberties and privacy officials.

Regulatory/Statutory Reference(s): CNSSI 1015.

AU-14(3) Session Audit | Remote Viewing / Listening

Justification to Select: AU-14(3) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program. AU-14(3) is necessary to centrally monitor and collect session detail for insider threat incident detection and analysis.

Supplemental Guidance: If a system or the organization does not provide the ability to select a specific user session to remotely monitor, then the organization would be unable to perform full contextual analysis of the activity of a specific insider threat from a centralized monitoring capability.

AU-16 Cross-Organizational Auditing

Justification to Select: Although AU-16 is not selected in the CNSSI 1253 baseline or an overlay, EO 13587 requires an organization to coordinate audit information across other internal and external organizations to support the detection of insider threat activities. Therefore, AU-16 is applicable for all organizations to support the Insider Threat Program.

Supplemental Guidance: If the organization does not use audit exchange standards when sharing audit information with external organizations, then the external organizations may not be able to correlate the shared audit information.

Organizations should define and implement inter-organizational methodology to report correlated audit alerts of malicious nature to cyber situational awareness authorities for identifying a government response.

Sharing of audit data shall be consistent with access restrictions developed pursuant to AU-9. To the extent that audit data is attributable to a unique user, it may be shared with others, such sharing shall be limited to the least amount required to assess the threat or to address the concern for which the sharing is requested. Additionally, each organization shall determine if the collection, sharing, and use of such data requires a Privacy Act System of Records Notice (SORN)."

Organizations should use IC enterprise standard, IC Enterprise Audit Exchange Technical Specification (AUDIT.XML) to guide near-term sharing.

Parameter Value(s): The organization employs *real-time sharing using the IC Enterprise Audit Exchange Technical Specification (Audit.XML)* for coordinating *audit records specified in DNI* CNSSI 1015 among external organizations when audit information is transmitted across organizational boundaries.

Regulatory/Statutory Reference(s): EO 13587, Section 2.1(b) and Section 5.2 (a); White House Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, Tab 2, Section H.1; CNSSI 1015; and Intelligence Community Enterprise Audit Conceptual Framework, Section 2.2.3.

AU-16(1) Cross-Organizational Auditing | Identity Preservation

Justification to Select: Although AU-16(1) is not selected in the CNSSI 1253 baseline or an overlay, EO 13587 requires organizations preserve the identities of individuals in cross-organization audit trails to facilitate the detection of insider threats on all classified and unclassified networks. Therefore, AU-16(1) is applicable for all organizations to support the Insider Threat Program.

Supplemental Guidance: If the organization does not preserve the identity of individuals in cross-organization audit trails, then related insider threat activity will not be correlated to the individual.

Regulatory/Statutory Reference(s): EO 13587, Section 2.1 (b) and Section 5.2 (a); and White House Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, Tab 2, H.1.

AU-16(2) Cross-Organizational Auditing | Sharing of Audit Information

Justification to Select: Although AU-16(2) is not selected in the CNSSI 1253 baseline, EO 13587 requires organizations provide cross-organizational audit information to facilitate the detection

and mitigation of insider threats on all classified and unclassified networks. Therefore, AU-16(2) is applicable for all organizations to support the Insider Threat Program.

Supplemental Guidance: If the organization does not share audit information across other internal and external organizations, then the organization would be unable to perform full contextual analysis of the activity of a specific insider threat.

Organizations should establish or maintain a multi-disciplinary threat management capability and procedures to conduct and integrate the monitoring, timely review, analysis, reporting, and response to insider threats. Organizations should develop and implement sharing policies and procedures where by the organizations' Insider Threat Program accesses, shares, and integrates information and data derived from offices across the organization, including CI, security, information assurance, and human resources offices.

Organizations should share, where lawful and appropriate, any information identified during the course of an insider threat inquiry or investigation that may have an effect on information assurance, security, or other community audit needs. In any case involving information assurance, the information shall be shared, as appropriate, with the Authorizing Official or designee.

Organizations should establish reporting guidelines for CI, Security, IA, HR, and other relevant organizational components to securely provide Insider Threat Program personnel, regular, timely, and, if possible, electronic access to the information necessary to identify, analyze, and resolve insider threat matters. Such access and information includes, but is not limited to, the following:

a. Counterintelligence and Security. All relevant databases and files to include, but not limited to, personnel security files, polygraph examination reports, facility access records, security violation files, travel records, foreign contact reports, and financial disclosure filings
b. Information Assurance. All relevant unclassified and classified network information generated by IA elements to include, but not limited to, personnel usernames and aliases, levels of network access, audit data, unauthorized use of removable media, print logs, and other data needed for clarification or resolution of an insider threat concern.
c. Human Resources. All relevant HR databases and files to include, but not limited to, personnel files, payroll and voucher files, outside work and activities requests disciplinary files, and personal contact records, as may be necessary for resolving or clarifying insider threat matters.

When data reveals an act or pattern of acts indicative of a crime that data should be provided to appropriate security and/or investigative authorities in accordance with applicable rules and procedures, and reported in accordance with the requirements of EO 13462, as amended, President's Intelligence Advisory Board and Intelligence Oversight Board.

Organizations should maintain the ability to share audit process results with relevant law enforcement, civilian and military personnel management, mental health, cybersecurity, security, and counterintelligence information with commanders (or civilian equivalents) component-wide.

Organizations should share audit data regarding detected anomalies on information resources that potentially stem from an insider threat in a timely manner with all appropriate organizations responsible for insider threat detection (which may include the users' gaining or employing organization, or department or agency).

Organizations should, establish a memorandum of agreement or memorandum of understanding on the handling, storage, or dissemination of IC information, with entities external to the organization, including Federal departments and agencies; state, local, and tribal governments; foreign governments or international organizations; or private sector organizations.

Parameter Value(s): The organization provides cross-organizational audit information to *the organization's Insider Threat Program and other external organizations (e.g., the respective user's gaining and employing organization)* based on *all formally established policy (to include CNSSI 1015) and other cross-organizational sharing agreements*.

Regulatory/Statutory Reference(s): EO 13587, Section 2.1(b) and Section 5.2 (a); White House Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, Tab 2, H.1; and CNSSI 1015.

CA-2 Security Assessments

Justification to Select: CA-2 is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization:

a. Develops a security assessment plan that describes the scope of the assessment including:
    1. Security controls and control enhancements under assessment;
    2. Assessment procedures to be used to determine security control effectiveness; and
    3. Assessment environment, assessment team, and assessment roles and responsibilities;

b. Assesses the security controls in the information system and its environment of operation *as part of initial security authorization and at least annually thereafter, or as stipulated in the organization's continuous monitoring program, or in response to environmental or operational changes affecting the security of the system's information* to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements;

c. Produces a security assessment report that documents the results of the assessment; and

d. Provides the results of the security control assessment to *at a minimum, the Authorizing Official, ISSO and ISSM*.

CA-2(1) Security Assessments | Independent Assessors

Justification to Select: CA-2(1) is selected in the CNSSI 1253 baseline for all systems.

Supplemental Guidance: If the organization does not employ assessors with the necessary level of independence, then security controls that mitigate insider threats may not be properly implemented.

Parameter Value(s): The organization employs assessors or assessment teams with *a level of independence that has been determined by the AO to be free from any perceived or actual conflicts of interest with regard to the development, operation, or management of the organization's information systems* to conduct security control assessments.

CA-2(2) Security Assessments | Specialized Assessments

Justification to Select: CA-2(2) is selected in the CNSSI 1253 baseline for systems categorized High for Confidentiality, Integrity, or Availability.

Supplemental Guidance: If the organization does not include specialized insider threat assessments as part of security control assessments, then security controls may not be properly implemented for insider threat activity.

Organizations should use a variety of assessment techniques and methodologies such as continuous monitoring, insider threat assessment, and malicious user's assessment. These assessment mechanisms are context-specific and require the organization to understand its ICT supply chain infrastructure and to define the required set of measures for assessing and verifying that appropriate protections have been implemented.

Parameter Value(s): The organization includes as part of security control assessments, *to include: continuous monitoring; insider threat assessment; malicious user's assessment; and at a minimum, annual, announced malicious user testing, penetration testing, and/or red team exercises conducted for information systems with a Confidentiality, Integrity, or Availability impact level of High or as required by the Authorizing Official*.

Regulatory/Statutory Reference(s): NIST SP 800-161

CA-3 System Interconnections

Justification to Select: CA-3 is selected in the CNSSI 1253 baseline for all systems and in the Privacy Overlay for Privacy Impact Levels of Moderate or High, and for PHI. CA-3 is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization:
a. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements;
b. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and
c. Reviews and updates Interconnection Security Agreements *at least annually and in response to environmental or operational changes affecting the security of the system's information*.

CA-3(2) System Interconnections | Classified National Security System Connections

Justification to Select: Although CA-3(2) is not selected in NIST SP 800-53 , it is selected in the Classified Information Overlay for all systems, CA-3(2) is therefore applicable to systems with classified information that support the Insider Threat Program.

Parameter Value(s): The organization prohibits the direct connection of a classified, national security system to an external network without the use of *enterprise controlled security gateway appropriate to the classification/sensitivity of the external network*.

CA-3(3) System Interconnections | Unclassified Non-National Security System Connections

Justification to Select: CA-3(3) is selected in the Privacy Overlay for all Privacy Impact Levels, and for PHI. CA-3(3) is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization shall prohibit the direct connection of *systems containing PII or PHI* to an external network without the use of *a firewall or other network boundary protection device approved to prevent unauthorized access to the system*.

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

Justification to Select: CA-3(5) is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization employs *a deny-all, permit-by-exception* policy for allowing *any and all* systems to connect to external information systems.

CA-5 Plan of Action and Milestones

Justification to Select: CA-5 is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization:
a. Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and
b. Updates existing plan of action and milestones *at least quarterly (90 days)* based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

CA-6 Security Authorization

Justification to Select: CA-6 is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization:

a. Assigns a senior-level executive or manager as the authorizing official for the information system;
b. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and
c. Updates the security authorization *continuously if the organization and/or system is adequately covered by a continuous monitoring program; If not:*

- *At least every three (3) years,*
- *When significant security breaches occur,*
- *Whenever there is a significant change to the system, or*
- *To the environment in which the system operates*.

CA-7 Continuous Monitoring

Justification to Select: CA-7 is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: Organizations should integrate automated Enterprise Audit Management and automated insider threat activity monitoring with the organizational continuous monitoring efforts. If the organization does not integrate automated insider threat activity monitoring with the organizational continuous monitoring efforts, then potential insider threat activity would not be promptly detected.

Parameter Value(s): The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:
a. Establishment of *metrics that provide meaningful indications of the security posture* to be monitored;
b. Establishment of *continuous or specific periodic frequencies* for monitoring and *criticality and risk driven frequencies* for assessments supporting such monitoring;
c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;
d. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy;
e. Correlation and analysis of security-related information generated by assessments and monitoring;
f. Response actions to address results of the analysis of security-related information; and
g. Reporting the security status of organization and the information system to *the CISO, CIO and Senior Leadership, at least annually or when requested by organizational officials*.

Regulatory/Statutory Reference(s): CNSSI 1015, Section 14.

CA-7(3) Continuous Monitoring | Trend Analysis

Justification to Select: Although CA-7(3) is not selected in the CNSSI 1253 baseline or an overlay, CA-7(3) is selected for all systems, including systems that directly support the Insider Threat Program, because continuous monitoring trend analyses is a key measure in mitigating or detecting insider threat.

Supplemental Guidance: If the organization does not employ trend analysis to monitor the effectiveness of continuous monitoring activity, then the organization will not be able to dynamically adjust thresholds and triggers to detect insider threat activity based on empirical data.

Information gathered during continuous monitoring/trend analysis serves as input into ICT SCRM decisions including criticality analysis, vulnerability and threat analysis, and risk assessment. It also provides information that can be used in incident response and potentially can identify an ICT supply chain compromise, including Insider threat. Examples of continuous monitoring trend analysis includes:

(1) Examining recent insider threat information regarding the types of threat events that have occurred within the organization or across the federal government;
(2) Success rates of certain types of insider threat attacks, emerging vulnerabilities in information technologies; evolving social engineering techniques;
(3) Results from multiple security control assessments; and
(4) The effectiveness of configuration settings.

Regulatory/Statutory Reference(s): NIST SP 800-161

CA-8 Penetration Testing

Justification to Select: CA-8 is selected in the CNSSI 1253 baseline for systems categorized as High for Integrity and is selected in the Privacy Overlay for Privacy Impact Level of High. CA-8 is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization conducts penetration testing *prior to authorization of information system and periodically, no less frequently than when a significant change to the information system occurs* on *information systems requiring High Integrity or containing PII at the High Privacy Impact Level*.

CA-9 Internal System Connections

Justification to Select: CA-9 is selected in the CNSSI 1253 baseline for all systems and in the Privacy Overlay for Privacy Impact Levels of Moderate or High, and PHI. CA-9 is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization:

a. Authorizes internal connections of *all network attached peripherals or devices, such as printers, scanners, and copiers,* to the information system; and
b. Documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.

CA-9(1) Internal System Connections | Security Compliance Checks

Justification to Select: CA-9(1) is selected in the Privacy Overlays for Privacy Impact Levels of Moderate and High, and PHI and is therefore applicable to systems or activities that directly support the Insider Threat Program.

CM-2 Baseline Configuration

Justification to Select: CM-2 is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

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

Justification to Select: CM-2(1) is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization reviews and updates the baseline configuration of the information system:
(a) *At least annually*;
(b) When required due to *baseline configuration changes, significant or security relevant changes, or security incidents occur or as events dictate (e.g., changes due to USCYBERCOM tactical orders/directives or cyber-attacks)*; and
(c) As an integral part of information system component installations and upgrades.

CM-2(2) Baseline Configuration | Automation Support for Accuracy / Currency

Justification to Select: CM-2(2) is selected in the CNSSI 1253 baseline for systems categorized as High for Integrity and is therefore applicable to systems or activities that directly support the Insider Threat Program.

CM-2(3) Baseline Configuration | Retention of Previous Configurations

Justification to Select: CM-2(3) is selected in the CNSSI 1253 baseline for systems categorized as Moderate or High for Integrity and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization retains *at least two previous versions of baseline configurations of the information system* to support rollback.

CM-3 Configuration Change Control

Justification to Select: CM-3 is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization:
a. Determines the types of changes to the information system that are configuration-controlled;
b. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses;
c. Documents configuration change decisions associated with the information system;
d. Implements approved configuration-controlled changes to the information system;
e. Retains records of configuration-controlled changes to the information system for *one year or two change cycles of baseline configurations as defined in CM-2 (3), whichever is longer*;
f. Audits and reviews activities associated with configuration-controlled changes to the information system; and

g. Coordinates and provides oversight for configuration change control activities through *Configuration Change Board (CCB)* that convenes *at a frequency determined by the CCB or as configuration change conditions warrant*.

CM-3(1) Configuration Change Control | Automated Document / Notification / Prohibition of Changes

Justification to Select: CM-3(1) is selected in the CNSSI 1253 baseline categorized High for Integrity and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization employs automated mechanisms to:
(a) Document proposed changes to the information system;
(b) Notify *the Engineering Review Board and Configuration Control Board* of proposed changes to the information system and request change approval;
(c) Highlight proposed changes to the information system that have not been approved or disapproved by *(i.e., fully processed) in accordance with the timeline specified in the Configuration Management Plan (CMP), not to exceed a maximum of 90 days (or 7 days for CDS)*;
(d) Prohibit changes to the information system until designated approvals are received;
(e) Document all changes to the information system; and
(f) Notify, *at a minimum, the Configuration Control Board* when approved changes to the information system are completed.

CM-3(2) Configuration Change Control | Test / Validate / Document Changes

Justification to Select: CM-3(2) is selected in the CNSSI 1253 baseline categorized Moderate or High for Integrity and is therefore applicable to systems or activities that directly support the Insider Threat Program.

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

Justification to Select: CM-3(4) is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization requires an information security representative to be a member of the *Configuration Control Board (CCB).*

CM-3(5) Configuration Change Control | Automated Security Response

Justification to Select: CM-3(5) is selected in the CNSSI 1253 baseline for systems categorized High for Integrity and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The information system implements *measures delineated in the Configuration Management Plan (CMP)* automatically if baseline configurations are changed in an unauthorized manner.

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

Justification to Select: CM-3(6) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system or the organization does not include cryptographic mechanisms in the configuration management program, then an insider threat could circumvent or compromise access controls and other protections that rely on cryptographic processes. Cryptographic management is provided as an enterprise service subscribed to by individual systems.

Parameter Value(s): The organization ensures that cryptographic mechanisms used to provide *all security controls and safeguards that rely on cryptography or which provide safeguarding of controlled unclassified and classified information from unauthorized access or modification* are under configuration management.

CM-4 Security Impact Analysis

Justification to Select: CM-4 is selected in the CNSSI 1253 baseline for all systems and in the Privacy Overlay for all Privacy Impact Levels, and for PHI. CM-4 is therefore applicable to systems or activities that directly support the Insider Threat Program.

CM-4(1) Security Impact Analysis | Separate Test Environments

Justification to Select: CM-4(1) is selected in the CNSSI 1253 baseline for systems categorized Moderate or High for Integrity and in the Privacy Overlay for Privacy Impact Levels of Moderate or High. CM-4(1) is therefore applicable to systems or activities that directly support the Insider Threat Program.

CM-4(2) Security Impact Analysis | Verification of Security Functions

Justification to Select: CM-4(2) is selected in the Privacy Overlay for Privacy Impact Levels of Moderate or High, and for PHI. CM-4(2) is therefore applicable to systems or activities that directly support the Insider Threat Program.

CM-5 Access Restrictions for Change

Justification to Select: CM-5 is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system does not properly manage physical and logical access restrictions associated with changes to the information system, then an insider threat could gain access and make configuration changes to systems without authorization.

CM-5(1) Access Restrictions for Change | Automated Access Enforcement / Auditing

Justification to Select: CM-5(1) is selected in the CNSSI 1253 baseline for systems categorized Moderate or High for Integrity, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system does not use automation to enforce access restrictions and support auditing of the enforcement actions, then the enforcement actions could be bypassed by an insider threat without detection.

CM-5(2) Access Restrictions for Change | Review System Changes

Justification to Select: CM-5(2) is selected in the CNSSI 1253 baseline for systems categorized Moderate or High for Integrity, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system does not regularly review information system changes, then an insider threat could make unauthorized changes without detection.

Parameter Value(s): The organization reviews information system changes *every 90 days or more frequently as the organization defines for high integrity systems AND at least annually or more frequently as the organization defines for low integrity and moderate integrity systems* and *when there is an incident or when planned changes have been performed* to determine whether unauthorized changes have occurred.

CM-5(3) Access Restrictions for Change | Signed Components

Justification to Select: CM-5(3) is selected in the CNSSI 1253 baseline categorized High for Integrity and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The information system prevents the installation of *all digitally signed software and firmware products* without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

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

Justification to Select: CM-5(5) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: EO 13526 requires organizations to establish procedures and controls to prevent access by unauthorized persons to classified information. If a system does not limit privileges to change information system components and system-related information within a production or operational environment, then an insider threat could make unauthorized changes to the system.

Parameter Value(s): The organization:
(a) Limits privileges to change information system components and system-related information within a production or operational environment; and
(b) Reviews and reevaluates privileges *at least every 90 days (quarterly)*.

Regulatory/Statutory Reference(s): EO 13526, Section 4.1, Section (g).

CM-5(6) Access Restrictions for Change | Limit Library Privileges

Justification to Select: CM-5(6) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system does not limit privileges to change software resident within software libraries, then an insider threat could make changes to the libraries that enable the system to be compromised.

CM-6 Configuration Settings

Justification to Select: CM-6 is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If the reference documents cited in the parameter values are not available, the following are acceptable in descending order as available:
(1): Configurations vetted through approved security assessment programs (e.g., NIAP, CSfC, CCEVS)
(2) Commercially accepted practices (e.g., SANS)
(3) Independent testing results (e.g., ICSA) or
(4) Vendor literature.

Parameter Value(s): The organization:
a. Establishes and documents configuration settings for information technology products employed within the information system using *DoD approved guides (e.g., DoD SRGs and STIGs; or NSA SCGs; USCYBERCOM CTOs; DTMs)* that reflect the most restrictive mode consistent with operational requirements;
b. Implements the configuration settings;
c. Identifies, documents, and approves any deviations from established configuration settings for *all configurable information system components* based on *explicit operational requirements as approved by the AO*; and
d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

CM-6(1) Configuration Settings | Automated Central Management / Application / Verification

Justification to Select: CM-6(1) is selected in the CNSSI 1253 baseline for systems categorized Moderate or High for Integrity, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system does not employ automated mechanisms to centrally manage, apply, and verify configuration settings, then an insider threat could introduce or exploit a misconfiguration that would allow the system to be compromised. Automated central

management, application, and verification of configuration settings enables prompt detection of misconfiguration by insider threat and restoral of settings back to an approved baseline.

Parameter Value(s): The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings for *at a minimum, all IA enabled or related components*.

CM-6(2) Configuration Settings | Respond to Unauthorized Changes

Justification to Select: CM-6(2) is selected in the CNSSI 1253 baseline categorized High for Integrity and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization employs *Defensive Cyber Operations* to respond to unauthorized changes to *security sub-system configuration settings*.

CM-7 Least Functionality

Justification to Select: CM-7 is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization:
a. Configures the information system to provide only essential capabilities; and
b. Prohibits or restricts the use of the following functions, ports, protocols, and/or services: *Functions, ports, protocols, and services as established for DoD by DISA for Unclassified and Secret networks (i.e., DoDI 8551.01) or for the Intelligence Community the Office of the Director of National Intelligence (ODNI) for Top Secret Networks.*

CM-7(1) Least Functionality | Periodic Review

Justification to Select: CM-7(1) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system or the organization does not regularly review the information system as system changes or incidents occur, then an insider threat could misuse unnecessary and/or nonsecure functions, ports, protocols, and services to compromise the system.

Periodic review of a system's functions, ports, protocols, and services enables prompt detection of misconfiguration by insider threat and restoral of settings back to an approved baseline.

Parameter Value(s): The organization:
(a) Reviews the information system *every 30 days or more frequently as system changes or incidents occur* to identify unnecessary and/or nonsecure functions, ports, protocols, and services; and
(b) Disables *all functions, ports, protocols, and services within the information system and at the enterprise level that are deemed to be unnecessary and/or nonsecure (as specified for DoD by DISA for Unclassified and Secret networks (i.e., DoDI 8551.01) or for the Intelligence Community the Office of the Director of National Intelligence (ODNI) for Top Secret Networks).*

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

Justification to Select: CM-7(2) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system does not prevent program execution in accordance with established rules, then an insider threat could introduce malicious code to compromise the system.

Parameter Value(s): The information system prevents program execution in accordance with *the rules authorizing the terms and conditions of software program usage, which establish a deny-all, permit-by-exception process*.

CM-7(3) Least Functionality | Registration Compliance

Justification to Select: CM-7(3) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system does not ensure registration compliance for functions, ports, protocols, and services, then an insider threat could introduce or manipulate a system's functions, ports, protocols, and services to compromise the system. Centralized registration and management of functions, ports, protocols, and services for an enterprise will establish a standardized baseline to aid in detecting unauthorized misconfigurations by insider threats.

Parameter Value(s): The organization ensures compliance with *the registration and management requirements of all functions, ports, protocols, and services, in compliance with DoDI 8551.01*.

CM-7(4) Least Functionality | Unauthorized Software / Blacklisting

Justification to Select: Although CM-7(4) is not selected in the CNSSI 1253 baseline or an overlay, CM-7(4) should be implemented in conjunction with CM-7(5) to inhibit the installation and execution of known malicious or otherwise unauthorized executables by insider threat.

Supplemental Guidance: If a system or the organization does not identify and block unauthorized software, then an insider threat could introduce software onto the system that has not been authorized. An approach to prevent the use of unauthorized software and malware is to block the use of known malicious or otherwise unauthorized software considered unsafe to run. An existing capability such as Application Blacklisting is highly recommended. The use of Blacklisting helps to prevent unauthorized encryption, obfuscation, exploitation, or exfiltration. This will mitigate vulnerabilities from a technically sophisticated insider threat from rapidly exfiltrating large amounts of sensitive information through injected code and covering their activities.

Parameter Value(s): The organization:
(a) Identifies *software programs not authorized to execute on the information system*;
(b) Employs an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the information system; and
(c) Reviews and updates the list of unauthorized software programs *at least annually*.

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

Justification to Select: CM-7(5) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system or the organization does not identify and specifically allow only authorized software, then an insider threat could introduce software onto the system that has not been authorized. An approach to prevent the use of unauthorized software and malware is to limit the use of software to approved products considered safe to run. An existing capability such as Application Whitelisting is highly recommended. The use of Whitelisting helps to prevent unauthorized encryption, obfuscation, exploitation, or exfiltration. This will mitigate vulnerabilities from a technically sophisticated insider threat from rapidly exfiltrating large amounts of sensitive information through injected code and covering their activities.

Parameter Value(s): The organization:
(a) Identifies *all software programs authorized to execute on the information system*;
(b) Employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system; and
(c) Reviews and updates the list of authorized software programs *monthly and as needed to reflect approved changes*.

Regulatory/Statutory Reference(s): CNSSD 504 Section A.2.a.

CM-8 Information System Component Inventory

Justification to Select: CM-8 is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization:
a. Develops and documents an inventory of information system components that:
    1. Accurately reflects the current information system;
    2. Includes all components within the authorization boundary of the information system;
    3. Is at the level of granularity deemed necessary for tracking and reporting; and
    4. Includes *but is not limited to: hardware specifications (e.g., manufacturer, type, model, serial number, physical location, etc.), software and software license information, information system/component owner, and for a networked component/device, the machine name*; and
b. Reviews and updates the information system component inventory *at least annually*.

CM-8(1) Information System Component Inventory | Updates During Installations / Removals

Justification to Select: CM-8(1) is selected in the CNSSI 1253 baseline for systems categorized as Moderate or High for Integrity and is selected in the Privacy Overlays for PHI. CM-8(1) is therefore applicable to systems that support the Insider Threat Program.

CM-8(2) Information System Component Inventory | Automated Maintenance

Justification to Select: CM-8(2) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system or the organization does not employ automated mechanisms to maintain the component inventory, then an insider threat could introduce components that have not been authorized to circumvent security protections. The organization should implement automated maintenance mechanisms to ensure that changes to component inventory for the information system and ICT supply chain infrastructure are monitored for installation, update, and removal. When automated maintenance is performed with a predefined frequency and with the automated collation of relevant inventory information about each defined component, the organization should ensure that updates are available to relevant stakeholders for evaluation. Predefined frequencies for data collection should be less predictable in order to reduce the risk of an insider threat bypassing security mechanisms.

Regulatory/Statutory Reference(s): NIST SP 800-161

CM-8(3) Information System Component Inventory | Automated Unauthorized Component Detection

Justification to Select: CM-8(3) is selected in the CNSSI 1253 baseline for all systems.

Supplemental Guidance: If the organization does not use automated mechanisms to detect the presence of unauthorized hardware, software, and firmware components, then an insider threat could introduce hardware, software, and firmware components that have not been authorized and thereby circumvent security protections. Such automated mechanisms are implemented at an enterprise level.

Parameter Value(s): The organization:
(a) Employs automated mechanisms *continuously* to detect the presence of unauthorized hardware, software, and firmware components within the information system; and
(b) Takes the following actions when unauthorized components are detected: *at a minimum, notify the Security Administrator, ISSO and ISSM, and others as the local organization deems appropriate*.

CM-8(4) Information System Component Inventory | Accountability Information

Justification to Select: CM-8(4) is selected in the CNSSI 1253 baseline for systems categorized as High for Confidentiality and Integrity and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization includes in the information system component inventory information, a means for identifying by *at least, position or role,* individuals responsible/accountable for administering those components.

CM-9 Configuration Management Plan

Justification to Select: CM-9 is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

CM-10 Software Usage Restrictions

Justification to Select: CM-10 is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

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

Justification to Select: CM-10(1) is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization establishes the following restrictions on the use of open source software: *Restrictions as established in DoD Memorandum "Clarifying Guidance Regarding Open Source Software (OSS)" of 16 Oct 2009 (http://dodcio.defense.gov/Home/Issuances/DoDCIOMemorandums.aspx).*

CM-11 User-Installed Software

Justification to Select: CM-11 is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system or the organization does not establish, enforce, and monitor policies governing the installation of software by users, then an insider threat could install software that has not been authorized. The establishment of policy governing user-installed software and the monitoring of compliance with the policy enables the enterprise to detect and mitigate the installation of unauthorized software by insiders.

Parameter Value(s): The organization:
a. Establishes *a policy* governing the installation of software by users;
b. Enforces software installation policies through *procedural methods (e.g., periodic examination of user accounts), automated methods (e.g., configuration settings implemented on organizational information systems), or both*; and
c. Monitors policy compliance *continuously*.

CM-11(1) User-Installed Software | Alerts for Unauthorized Installations

Justification to Select: Although CM-11(1) is selected in the CNSSI 1253 baseline only for systems categorized as High for Confidentiality or Integrity, selection of CM-11(1) for all systems enhances the ability to detect and promptly mitigate insider threat activity.

Supplemental Guidance: If a system or the organization does not alert designated personnel when the installation of unauthorized software is detected, then an insider threat could install and

thereafter remove unauthorized software without discovery. Monitoring and notification is best performed using an enterprise solution.

Parameter Value(s): The information system alerts *the Security Administrator and Security Operations Center (SOC)* when the unauthorized installation of software is detected.

CM-11(2) User-Installed Software | Prohibit Installation Without Privileged Status

Justification to Select: CM-11(2) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system does not prohibit installation of software without privileged status, then an insider threat without privileged status could install unauthorized software.

CP-2 Contingency Plan

Justification to Select: CP-2 is selected in the CNSSI 1253 baseline for all systems and in the Privacy Overlay for all Privacy Impact Levels, and for PHI. CP-2 is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization:

a. Develops a contingency plan for the information system that:
   1. Identifies essential missions and business functions and associated contingency requirements;
   2. Provides recovery objectives, restoration priorities, and metrics;
   3. Addresses contingency roles, responsibilities, assigned individuals with contact information;
   4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;
   5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and
   6. Is reviewed and approved by *the ISSM and ISSO at a minimum*;

b. Distributes copies of the contingency plan to *the stakeholders, key personnel or roles and organizational elements identified in the organization's Continuity of Operations Plan (COOP) and Component Business Continuity/Disaster Recovery (BC/DR) Plans*;

c. Coordinates contingency planning activities with incident handling activities;

d. Reviews the contingency plan for the information system *at least annually*;

e. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;

f. Communicates contingency plan changes to *the stakeholders, key personnel and organizational elements identified in the contingency plan*; and

g. Protects the contingency plan from unauthorized disclosure and modification.

CP-2(1) Contingency Plan | Coordinate with Related Plans

Justification to Select: CP-2(1) is selected in the CNSSI 1253 baseline for systems categorized Moderate or High for Availability and is therefore applicable to systems or activities that directly support the Insider Threat Program.

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

Justification to Select: CP-2(3) is selected in the CNSSI 1253 baseline for systems categorized Moderate or High for Availability and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization plans for the resumption of essential missions and business functions within *the time frames established within the organization's COOP and BC/DR Plan* of contingency plan activation.

CP-2(8) Contingency Plan | Identify Critical Assets

Justification to Select: CP-2(8) is selected in the CNSSI 1253 baseline for systems categorized Moderate or High for Availability, and in the Privacy Overlay for PHI. CP-2(8) is therefore applicable to systems or activities that directly support the Insider Threat Program.

CP-3 Contingency Training

Justification to Select: CP-3 is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization provides contingency training to information system users consistent with assigned roles and responsibilities:

a. Within *10 working days* of assuming a contingency role or responsibility;
b. When required by information system changes; and
c. *At least annually* thereafter, *or more frequently in high risk areas or as specifically defined in the organization's COOP and BC/DR Plan*.

CP-4 Contingency Plan Testing

Justification to Select: CP-4 is selected in the CNSSI 1253 baseline for all systems and in the Privacy Overlay for PHI. CP-4 is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization:

a. Tests the contingency plan for the information system *at least annually or more often as specified in the organization's COOP and BC/DR Plans* using *the tests defined in the contingency plan* to determine the effectiveness of the plan and the organizational readiness to execute the plan;
b. Reviews the contingency plan test results; and
c. Initiates corrective actions, if needed.

CP-4(1) Contingency Plan Testing | Coordinate with Related Plans

Justification to Select: CP-4(1) is selected in the CNSSI 1253 baseline for systems categorized Moderate or High for Availability and is therefore applicable to systems or activities that directly support the Insider Threat Program.

CP-6 Alternate Storage Site

Justification to Select: CP-6 is selected in the CNSSI 1253 baseline for systems categorized Moderate or High for Availability and is therefore applicable to systems or activities that directly support the Insider Threat Program.

CP-6(1) Alternate Storage Site | Separation from Primary Site

Justification to Select: CP-6(1) is selected in the CNSSI 1253 baseline for systems categorized Moderate or High for Availability and is therefore applicable to systems or activities that directly support the Insider Threat Program.

CP-6(3) Alternate Storage Site | Accessibility

Justification to Select: CP-6(3) is selected in the CNSSI 1253 baseline for systems categorized Moderate or High for Availability and is therefore applicable to systems or activities that directly support the Insider Threat Program.

CP-7 Alternate Processing Site

Justification to Select: CP-7 is selected in the CNSSI 1253 baseline for systems categorized Moderate or High for Confidentiality, Integrity, or Availability, and in the Privacy Overlay for Privacy Impact Levels of Moderate or High, and for PHI. CP-7 is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization:
a. Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of *information system operations as defined in the organization's COOP and BC/DR Plan* for essential missions/business functions within *1 hour (Availability High) or 12 hours (Availability Moderate) as defined in the contingency plan* when the primary processing capabilities are unavailable;
b. Ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption; and
c. Ensures that the alternate processing site provides information security safeguards equivalent to those of the primary site.

CP-7(1) Alternate Processing Site | Separation from Primary Site

Justification to Select: CP-7(1) is selected in the CNSSI 1253 baseline for systems categorized Moderate or High for Availability and is therefore applicable to systems or activities that directly support the Insider Threat Program.

CP-7(3) Alternate Processing Site | Priority of Service

Justification to Select: CP-7(3) is selected in the CNSSI 1253 baseline for systems categorized Moderate or High for Availability and is therefore applicable to systems or activities that directly support the Insider Threat Program.

CP-9 Information System Backup

Justification to Select: CP-9 is selected in the CNSSI 1253 baseline for all systems and in the Privacy Overlay for Privacy Impact Levels of Moderate or High, and for PHI. CP-9 is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization:
a. Conducts backups of user-level information contained in the information system *at least weekly or as defined in the organization's COOP and BC/DR Plan*;
b. Conducts backups of system-level information contained in the information system *at least weekly and as required by system baseline configuration changes in accordance with the contingency plan*;
c. Conducts backups of information system documentation including security-related documentation *when created, received, updated, and, as required by system baseline configuration changes in accordance with the contingency plan;* and
d. Protects the confidentiality, integrity, and availability of backup information at storage locations.

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

Justification to Select: CP-9(1) is selected in the CNSSI 1253 baseline for systems categorized Moderate or High for Integrity or Availability and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization tests backup information *at least monthly or as defined in the organization's COOP and BC/DR Plan* to verify media reliability and information integrity.

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

Justification to Select: CP-9(5) is selected in the CNSSI 1253 baseline for systems categorized Moderate or High for Availability and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization tests backup information *continuously (Availability High), 24 hours (Availability Moderate), or 7 days (Availability Low) or otherwise as defined in the organization's COOP and BC/DR Plan* to verify media reliability and information integrity.

CP-10 Information System Recovery and Reconstitution

Justification to Select: CP-10 is selected in the CNSSI 1253 baseline for all systems and in the Privacy Overlay for Privacy Impact Levels of Moderate or High, and for PHI. CP-10 is therefore applicable to systems or activities that directly support the Insider Threat Program.

CP-10(2) Information System Recovery and Reconstitution | Transaction Recovery

Justification to Select: CP-10(2) is selected in the CNSSI 1253 baseline for systems categorized Moderate or High for Integrity or Availability and is therefore applicable to systems or activities that directly support the Insider Threat Program.

CP-10(4) Information System Recovery and Reconstitution | Restore within Time Period

Justification to Select: CP-10(4) is selected in the CNSSI 1253 baseline for systems categorized High for Integrity or Availability and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization provides the capability to restore information system components within *1 hour (Availability High), 24 hours (Availability Moderate), or 1-5 days (Availability Low) or otherwise as defined in the organization's COOP and BC/DR Plan* from configuration-controlled and integrity-protected information representing a known, operational state for the components.

IA-2 Identification and Authentication (Organizational Users)

Justification to Select: IA-2 is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Control Extension and Parameter Value(s): The organization shall verify the authentication measures on information sharing portals hosted on classified computer networks *quarterly* and non-compliant portals shall be appropriately secured or removed.

Supplemental Guidance: If a system does not uniquely identify and authenticate users and processes, then the organization would not be able to associate insider threat activity to a specific individual.

The configuration of portals, to include authentication measures supporting the portal, should be verified against the applicable STIG or other configuration guidance and if found to be non-compliant with the standard, they should be appropriately secured or removed.

Regulatory/Statutory Reference(s): EO 13587, Section 2.1(b) and Section 5.2.; and White House Memo - Near-Term Measures to Reduce the Risk of High-Impact Unauthorized Disclosures, Section B-1.

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

Justification to Select: IA-2(1) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: CNSSD 504 Annex A requires that agencies implement standardized access control methodologies for NSS, specifically multifactor authentication. If a system does not implement multifactor authentication for network access to privileged accounts, then an

insider threat could circumvent the authentication mechanisms to gain unauthorized access to the system.

Regulatory/Statutory Reference(s): CNSSD 504, Annex A, Section 2.b.i.

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

Justification to Select: IA-2(2) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: CNSSD 504 Annex A requires that agencies implement standardized access control methodologies for NSS, specifically multifactor authentication. If a system does not implement multifactor authentication for network access to non-privileged accounts, then an insider threat could circumvent the authentication mechanisms to gain unauthorized access to the system.

Regulatory/Statutory Reference(s): CNSSD 504, Annex A, Section 2.b.i.

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

Justification to Select: IA-2(3) is selected in the CNSSI 1253 baseline for systems categorized Moderate or High for Integrity or Availability, including systems or activities that directly support the Insider Threat Program. USCYBERCOM TO 15-0102 requires the use of multifactor authentication (i.e., DoD PKI) at all categorization levels.

Supplemental Guidance: CNSSD 504 Annex A requires that agencies implement standardized access control methodologies for NSS, specifically multifactor authentication. If a system does not implement multifactor authentication for local access to privileged accounts, then an insider threat could circumvent the authentication mechanisms to gain unauthorized access to the system.

Regulatory/Statutory Reference(s): CNSSD 504, Annex A, Section 2.b.i.; and USCYBERCOM TO 15-0102.

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

Justification to Select: IA-2(4) is selected in the CNSSI 1253 baseline for systems categorized Moderate or High for Integrity or Availability, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: CNSSD 504 Annex A requires that agencies implement standardized access control methodologies for NSS, specifically multifactor authentication. If a system does not implement multifactor authentication for local access to non-privileged accounts, then an insider threat could circumvent the authentication mechanisms to gain unauthorized access to the system.

Regulatory/Statutory Reference(s): CNSSD 504, Annex A, Section 2.b.i.

IA-2(5) Identification and Authentication (Organizational Users) | Group Authentication

Justification to Select: IA-2(5) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system does not require individuals to be authenticated with an individual authenticator when a group authenticator is employed, then insider threat activity performed using the group authenticator could not be associated to a specific individual. Requiring individuals to use individual authenticators as a second level of authentication when using group authenticators enables the association of user actions to specific individuals.

IA-2(6) Identification and Authentication (Organizational Users) | Network Access to Privileged Accounts - Separate Device

Justification to Select: IA-2(6) is selected in the Privacy Overlay for Privacy Impact Levels of Moderate or High. IA-2(6) is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The information system implements multifactor authentication for network access to privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets *DoD or IC PKI or a technology approved by their Authorizing Official, FIPS 140-2, NIAP Certification, or NSA approval*.

IA-2(7) Identification and Authentication (Organizational Users) | Network Access to Non-Privileged Accounts - Separate Device

Justification to Select: IA-2(7) is selected in the Privacy Overlay for Privacy Impact Levels of Moderate or High. IA-2(7) is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The information system implements multifactor authentication for network access to non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets *DoD or IC PKI or a technology approved by their Authorizing Official, FIPS 140-2, NIAP Certification, or NSA approval*.

IA-2(8) Identification and Authentication (Organizational Users) | Network Access to Privileged Accounts – Replay Resistant

Justification to Select: IA-2(8) is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

IA-2(9) Identification and Authentication (Organizational Users) | Network Access to Non-Privileged Accounts - Replay Resistant

Justification to Select: IA-2(9) is selected in the CNSSI 1253 baseline for systems categorized Moderate or High for Confidentiality or Integrity and is therefore applicable to systems or activities that directly support the Insider Threat Program.

IA-2(11) Identification and Authentication (Organizational Users) | Remote Access - Separate Device

Justification to Select: IA-2(11) is selected in the CNSSI 1253 baseline for all systems and in the Privacy Overlay for Privacy Impact Levels of Moderate or High. IA-2(11) is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The information system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets *DoD or IC PKI or a technology approved by their Authorizing Official, FIPS 140-2, NIAP Certification, or NSA approval*.

IA-2(12) Identification and Authentication (Organizational Users) | Acceptance of PIV Credentials

Justification to Select: IA-2(12) is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

IA-3 Device Identification and Authentication

Justification to Select: IA-3 is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system does not uniquely identify and authenticate devices before the device establishes connections, then an insider threat could use an unauthorized or unintended device to gain unauthorized access. Uniquely identifying and authenticating devices is necessary to specifically identify the devices that an insider threat is using.

Parameter Value(s): The information system uniquely identifies and authenticates *all mobile devices and network connected endpoint devices (including but not limited to: workstations, printers, servers (outside a datacenter), VoIP Phones, VTC CODECs)* before establishing a *local, remote, or network* connection.

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

Justification to Select: IA-3(1) is selected in the CNSSI 1253 baseline for systems categorized Moderate or High for Confidentiality or Integrity, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system does not bidirectionally identify and authenticate devices before the device establishes connections, then an insider threat could use an unauthorized or unintended device to gain unauthorized access. EO 13526 requires organizations to establish uniform procedures to ensure information systems that store, process, or transmit classified information prevent access by unauthorized persons. Using bidirectional authentication for devices that is cryptographically based enables controlling access by devices that are known and

approved to connect. Bidirectional identification and authentication of devices is necessary to specifically identify the devices that an insider threat is using.

Parameter Value(s): The information system authenticates *all mobile devices and network connected endpoint devices (including but not limited to: workstations, printers, servers (outside a datacenter), VoIP Phones, VTC CODECs)* before establishing *local, remote, or network* connection using bidirectional authentication that is cryptographically based.

Regulatory/Statutory Reference(s): EO 13526, Section 4.1 (f); and EO 13587, Section 5.2 (a).

IA-4 Identifier Management

Justification to Select: IA-4 is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system does not properly manage and assign information system identifiers, then the organization may not be able to associate insider threat activity to a specific individual. Note: Items d and e of this Control are not appropriate to define for device identifiers (e.g., media access control (MAC), Internet protocol (IP) addresses, or device-unique token identifiers).

Parameter Value(s): The organization manages information system identifiers by:

a. Receiving authorization from *ISSO or ISSM* to assign an individual, group, role, or device identifier;
b. Selecting an identifier that identifies an individual, group, role, or device;
c. Assigning the identifier to the intended individual, group, role, or device;
d. Preventing reuse of *user* identifiers for *at least a year for individuals, groups, roles*; and
e. Disabling the identifier after *not to exceed:*
    (1) NIPRNet and SIPRNet: 35 days;
    (2) TS Network: 90 days;
    (3) Cross-Domain Systems: 30 days; or
    (4) A shorter period if so specified in the applicable STIG(s).

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

Justification to Select: IA-4(4) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: Formally establishing a user's status (e.g., government employee, military, contractor, foreign national, etc.) is an attribute used when controlling the distribution of restricted information. If a system does not uniquely identify the status of each individual, then restricted information (e.g., no-foreign, contract sensitive) might be improperly disclosed to unauthorized individuals.

Parameter Value(s): The organization manages individual identifiers by uniquely identifying each individual as *specified in by the Intelligence Community Public Key Infrastructure Interface Specification, or otherwise as a contractor or government employee and by nationality:*

- *User identifiers will follow the same format as DoD user e-mail addresses (john.smith.ctr@army.mil or john.smith.uk@army.mil);*
- *DoD user e-mail display names (e.g., John Smith, Contractor <john.smith.ctr@army.mil> or John Smith, United Kingdom <john.smith.uk@army.mil>); and*
- *Automated signature blocks (e.g., John Smith, Contractor, J-6K, Joint Staff or John Doe, Australia, LNO, Combatant Command).*
- *Contractors who are also foreign nationals are identified as both, e.g., john.smith.ctr.uk@army.mil.*

IA-5 Authenticator Management

Justification to Select: IA-5 is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system or the organization does not properly manage information system authenticators, then an insider threat could use compromised authenticators to gain unauthorized access to systems and information. Management of authenticators is performed at both the enterprise and system levels.

Parameter Value(s): The organization manages information system authenticators by:
a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;
b. Establishing initial authenticator content for authenticators defined by the organization;
c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
e. Changing default content of authenticators prior to information system installation;
f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;
g. Changing/refreshing authenticators *at least once every 60 days for passwords; every 3 years or 1 year from term of contract for CAC/PIV; every 3 years for biometrics*;
h. Protecting authenticator content from unauthorized disclosure and modification;
i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and
j. Changing authenticators for group/role accounts when membership to those accounts changes.

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

Justification to Select: IA-5(1) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system or the organization does not properly manage password-based authenticators, then an insider threat could use compromised password-based authenticators to gain unauthorized access to systems and information. Management of password-based authenticators is performed at both the enterprise and system levels. If an

operating system or application is technically or functionally unable to meet the minimum standards for password complexity, the shortfall must be fully described and explained, along with any associated mitigations applied, in the system documentation (e.g., body of evidence), the residual risk identified in the risk assessment report, and the specific deviation approved by the Authorizing Official.

Parameter Value(s): The information system, for password-based authentication:
(a) Enforces minimum password complexity of:

(1) 14 characters in length (or longer if so specified in the applicable STIG or overlay) including one of each of the following character sets:

- Upper-case (A through Z)

- Lower-case (a through z)

- Numeric (0 through 9)

*- Special character (e.g. ~ ! @ # $ % ^ & * ( ) _ + = - ‘ [ ] / ? > <)*

(2) Passwords shall not contain more than three consecutive characters from the same character set,

(3) Passwords shall not contain commonly used words, phases, or personally identifiable information,

(4) Passwords shall not contain repeated patterns of key sequences or words, and

(5) Passwords shall not be based on any keyboard pattern such as up, down, or horizontal sequences of keys (e.g. ‘1qaz’ ; ‘XSW@’; ‘qwerty’)

(b) Enforces at least the following number of changed characters when new passwords are created: *50% of the minimum password length*;
(c) Stores and transmits only cryptographically-protected passwords;
(d) Enforces password minimum and maximum lifetime restrictions of *24 hours minimum lifetime (except for initial change of a password or when compromise of a password is known or suspected) and sixty (60) days maximum lifetime*;
(e) Prohibits password reuse for *a minimum of 24* generations; and
(f) Allows the use of a temporary password for system logons with an immediate change to a permanent password.

IA-5(2) Authenticator Management | PKI-Based Authentication

Justification to Select: IA-5(2) is selected in the CNSSI 1253 baseline for systems categorized Moderate or High Confidentiality or Integrity, including systems or activities that directly support the Insider Threat Program. PKI-based authenticators are used at all categorization levels, therefore IA-5(2) is applicable to all systems employing PKI-based authentication.

Supplemental Guidance: If a system or the organization does not properly implement PKI-based authenticators, then an insider threat could use compromised PKI-based authenticators to gain

unauthorized access to systems and information. Implementation and management of PKI-based authentication is performed at both the enterprise and system levels.

IA-5(3) Authenticator Management | In-Person or Trusted Third-Party Registration

Justification to Select: IA-5(3) is selected in the CNSSI 1253 baseline categorized Moderate or High for Integrity and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization requires that the registration process to receive *PKI-based specific authenticators* be conducted *in accordance with the DoD or IC Certificate Policies.*

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

Justification to Select: IA-5(4) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system or the organization does not use automated tools to determine if password authenticators are sufficiently strong, then an insider threat could exploit weak passwords to gain unauthorized access to systems and information. Such verification of compliance with these standards should be performed at the time that users create or change their passwords. Alternatively, if verification cannot be accomplished at the time of creation, then automated password cracking tools should be used on a recurring basis.

Parameter Value(s): The organization employs automated tools to determine if password authenticators are sufficiently strong to satisfy *the requirements specified in IA-5(1).*

IA-5(7) Authenticator Management | No Embedded Unencrypted Static Authenticators

Justification to Select: IA-5(7) is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

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

Justification to Select: IA-5(8) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system does not properly implement safeguards for users having accounts on multiple systems, then the insider threat could reuse compromised passwords to gain unauthorized access to other information systems.

Parameter Value(s): The organization implements *policies, user training and other precautions, including advising users that they shall not use the same password for any of the following:*
a. Systems or domains of differing classification levels;
b. More than one system or domain of a classification level (e.g., internal agency network and Intelink);
c. More than one privilege level (e.g., user, administrator); to manage the risk of compromise due to individuals having accounts on multiple information systems.

IA-5(11) Authenticator Management | Hardware Token-Based Authentication

Justification to Select: IA-5(11) is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The information system, for hardware token-based authentication, employs mechanisms that satisfy *applicable token quality requirements (e.g., for DoD CDSs, DoDI 8520.03).*

IA-5(13) Authenticator Management | Expiration of Cached Authenticators

Justification to Select: IA-5(13) is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The information system prohibits the use of cached authenticators after *one hour*.

IA-5(14) Authenticator Management | Managing Content of PKI Trust Stores

Justification to Select: IA-5(14) is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

IA-6 Authenticator Feedback

Justification to Select: IA-6 is selected in the CNSSI 1253 baseline for all systems and in the Privacy Overlay for PHI. IA-6 is therefore applicable to systems or activities that directly support the Insider Threat Program.

IA-7 Cryptographic Module Authentication

Justification to Select: IA-7 is selected in the CNSSI 1253 baseline for all systems and in the Privacy Overlay for all Privacy Impact Levels, and for PHI. IA-7 is therefore applicable to systems or activities that directly support the Insider Threat Program.

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

Justification to Select: IA-8 is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system does not uniquely identify and authenticate non-organizational users and processes acting on behalf of non-organizational users, then the organization would not be able to associate insider threat activity to a specific individual.

System integrators, external services providers, and suppliers have the potential to engage the organization's ICT supply chain infrastructure for service delivery (development/integration services, product support, etc.). Organizations should manage the establishment, auditing, use, and revocation of identification and authentication of non-organizational users within the ICT supply chain infrastructure. Organizations should ensure promptness in performing identification and authentication activities, especially in the case of revocation management, to help mitigate against ICT supply chain risks such as Insider threat.

Regulatory/Statutory Reference(s): NIST SP 800-161

IA-10 Adaptive Identification and Authentication

Justification to Select: IA-10 is selected in the CNSSI 1253 baseline for systems categorized High for Confidentiality or Integrity, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system or the organization does not employ adaptive identification and authentication mechanisms for selected individuals (e.g., privileged users) on high impact systems, then insider threats may compromise individual authentication mechanisms and attempt to impersonate legitimate users. This situation can potentially occur with any authentication mechanisms employed by organizations. To address this threat, organizations may employ specific techniques/mechanisms and establish protocols to assess suspicious behavior (e.g., individuals accessing information that they do not typically access as part of their normal duties, roles, or responsibilities, accessing greater quantities of information than the individuals would routinely access, or attempting to access information from suspicious network addresses). In these situations, when certain pre-established conditions or triggers occur, organizations should require selected individuals to provide additional authentication information. Another potential use for adaptive identification and authentication is to increase the strength of mechanism based on the number and/or types of records being accessed.

Parameter Value(s): The organization requires that individuals accessing the information system employ s*upplemental authentication techniques or mechanisms* under specific *suspicious conditions or triggers*.

IA-11 Re-authentication

Justification to Select: IA-11 is selected in the CNSSI 1253 baseline categorized High for Confidentiality or Integrity, and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization requires users and devices to re-authenticate when *changing roles or accessing Special Access Program (SAP) information from another system*.

IR-1 Incident Response Policy and Procedures

Justification to Select: IR-1 is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If the organization does not develop and maintain incident response policies and procedures, to include measures to specifically address insider threat, then the organization will not be able to properly respond to, and mitigate, insider threat activity.

Parameter Value(s): The organization:
a. Develops, documents, and disseminates to *all personnel (including end users, maintenance personnel, administrators, etc.)*:

1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and

b. Reviews and updates the current:
   1. Incident response policy *at least annually*; and
   2. Incident response procedures *at least annually*.

IR-2 Incident Response Training

Justification to Select: IR-2 is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system or the organization does not conduct incident response training, to include instruction on the proper measures to detect and respond to insider threat incidents, then the organization will not properly respond to, and mitigate, insider threat activity.

Parameter Value(s): The organization provides incident response training to information system users consistent with assigned roles and responsibilities:
a. Within *30 working days* of assuming an incident response role or responsibility;
b. When required by information system changes; and
c. *at least annually* thereafter.

IR-2(1) Incident Response Training | Simulated Events

Justification to Select: IR-2(1) is selected in the CNSSI 1253 baseline for systems categorized High for Confidentiality for Integrity or Availability and is therefore applicable to systems or activities that directly support the Insider Threat Program.

IR-2(2) Incident Response Training | Automated Training Environments

Justification to Select: IR-2(2) is selected in the CNSSI 1253 baseline for systems categorized High for Integrity or Availability and is therefore applicable to systems or activities that directly support the Insider Threat Program.

IR-3 Incident Response Testing

Justification to Select: IR-3 is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If the organization does not conduct incident response testing, to include incident response effectiveness for insider threat incidents, then the organization may not be able to properly respond to, and mitigate, evolving insider threat activity.

Parameter Value(s): The organization tests the incident response capability for the information system *at least annually* using *tests defined in the incident response plan or tests derived from*

hot-washes of actual events that occurred during the past year to determine the incident response effectiveness and documents the results.

IR-3(2) Incident Response Testing | Coordination with Related Plans

Justification to Select: IR-3(2) is selected in the CNSSI 1253 baseline for systems categorized Moderate or High for Confidentiality, Integrity, or Availability, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If the organization does not coordinate insider threat incident response testing with organizational elements responsible for related plans, then the organization might not properly respond to, and recover from, insider threat incidents.

IR-4 Incident Handling

Justification to Select: IR-4 is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system or the organization does not include insider threat incidents into the organization's incident handling capabilities, activities, and lessons learned processes, then the organization might not properly respond to, and recover from, insider threat incidents.

IR-4(1) Incident Handling | Automated Incident Handling

Justification to Select: IR-4(1) is selected in the CNSSI 1253 baseline for systems categorized Moderate or High for Confidentiality, Integrity, or Availability, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system or the organization does not include automated incident handling for insider threat incidents, then the organization might not promptly detect and respond to insider threat incidents.

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

Justification to Select: IR-4(3) is selected in the CNSSI 1253 baseline for systems categorized Moderate or High for Confidentiality, Integrity, or Availability, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system or the organization does not identify classes of incidents, to include insider threat incidents, and their associated response actions, then incident response activity may not be sufficient to ensure continuation of organization missions and business functions.

Classes of incidents should include the following attributable events indicating violations of system/target (events of concern requiring further analysis or review of additional information.):
a. Malicious code detection
b. Unauthorized local device access
c. Unauthorized executables
d. Unauthorized privileged access

e. After-hours privileged access
f. System reset/reboot
g. Disabling the audit mechanism
h. Downloading to local devices
i. Printing to local devices
j. Uploading from local devices

Parameter Value(s): The organization identifies *attributable events [Per* CNSSI 1015, *Enterprise Audit Management Instruction for National Security Systems (NSS), all ISs shall be capable of auditing attributable events that indicate violation of system/target which require further analysis or review of additional information or events]:*
1. Malicious code detection
2. Unauthorized local device access
3. Unauthorized executables
4. Unauthorized privileged access
5. After-hours privileged access
6. System reset/reboot
7. Disabling of audit mechanism
8. Downloading to local devices
9. Printing to local devices
10. Uploading from local devices
as well as classes of incidents (to include those defined in CJCSM 6510.01B, Appendix A, Enclosure B) and *take the actions defined in CNSSI 1015 for the collection and sharing of attributable audit data and CJCSM 6510.01B in response to the classes of incident* to ensure continuation of organizational missions and business functions.

Regulatory/Statutory Reference(s): CNSSI 1015 Section 3; CNSSI 1015; and CJCSM 6510.01B, Appendix A, Enclosure B.

IR-4(4) Incident Handling | Information Correlation

Justification to Select: IR-4(4) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: Insider threat incident information should be correlated with other incident information to achieve an organization-wide perspective on incident awareness and response.

IR-4(6) Incident Handling | Insider Threats - Specific Capabilities

Justification to Select: IR-4(6) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If the organization does not implement incident handling capability for insider threats, then the organization will not appropriately and promptly respond to insider threat incidents.

Organizations should establish procedures for insider threat response action(s), such as inquiries, to clarify or resolve insider threat matters while ensuring that such response action(s) are centrally managed by the Insider Threat Program within the agency or one of its subordinate entities. Organizations should also build and maintain an insider threat analytic and response capability to manually and/or electronically gather, integrate, review, assess and respond to information derived from CI, Security, IA, HR, LE, the monitoring of user activity, and other sources as necessary and appropriate. This enhancement helps limit exposure of the ICT SCRM infrastructure to insider threats.

Regulatory/Statutory Reference(s): White House Memo - National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, Sections E.1 and E.2; and NIST SP 800-161.

IR-4(7) Incident Handling | Insider Threats - Intra-Organization Coordination

Justification to Select: IR-4(7) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If the organization does not coordinate insider threat incident handling capability for insider threats across the organization's components and external law enforcement agencies, then the organization will not appropriately and promptly respond to insider threat incidents.

Organizations should build and maintain an insider threat analytic and response capability to manually and/or electronically gather, integrate, review, assess and respond to information derived from CI, Security, IA, HR, LE, the monitoring of user activity, and other sources as necessary and appropriate. If security or CI offices are alerted to any security or other reportable event, they shall notify the employing element and any other affected elements for further review and action. Organizations should establish procedures for access requests by the Insider Threat Program involving particularly sensitive or protected information, such as information held by special access, law enforcement, inspector general, or other investigative sources or programs, which may require that access be obtained upon request of the Senior Official(s). This enhancement helps limit exposure of the ICT SCRM infrastructure to insider threats.

Parameter Value(s): The organization coordinates incident handling capability for insider threats across *the organization and with other IC and DoD elements.*

Regulatory/Statutory Reference(s): White House Memo - National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, Section E.1 and G.2; Office of the Secretary of Defense Insider Threat Mitigation, 12 July 2013; and NIST SP 800-161.

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

Justification to Select: IR-4(8) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If the organization does not coordinate insider threat incident handling capability for insider threats with external organizations, then the organization will not appropriately and promptly respond to insider threat incidents.

Cross organizational coordination and correlation should include insider threat related incident information.

Parameter Value(s): The organization coordinates with *IC Incident Response Center and USCYBERCOM* to correlate and share *incident information identified in the Intelligence Community and USCYBERCOM Incident Reporting Procedures* to achieve a cross-organization perspective on incident awareness and more effective incident responses.

IR-5 Incident Monitoring

Justification to Select: IR-5 is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If the organization does not track and document insider threat incidents, then the organization will not be able to correlate and fully analyze insider threat activities over the long term.

IR-5(1) Incident Monitoring | Automated Tracking / Data Collection / Analysis

Justification to Select: IR-5(1) is selected in the CNSSI 1253 baseline for systems categorized High for Confidentiality, Integrity, or Availability, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system or the organization does not employ automated mechanisms to assist with the tracking of insider threat related incidents, then the organization will not be able to promptly correlate and fully analyze insider threat activities.

IR-6 Incident Reporting

Justification to Select: IR-6 is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If the organization does not require personnel to promptly report suspected insider threat related activities to the organizationally identified authorities, then the organization would not promptly respond to, and mitigate, those insider threat activities.

Parameter Value(s): The organization:
a. Requires personnel to report suspected security incidents to the organizational incident response capability within *the timeframes specified by CJCSM 6510.01B (Table C-A-1), unless the data owner provides more restrictive guidance*; and
b. Reports security incident information to *IC Incident Response Center and USCYBERCOM*.

IR-6(1) Incident Reporting | Automated Reporting

Justification to Select: IR-6(1) is selected in the CNSSI 1253 baseline for systems categorized Moderate or High for Confidentiality, Integrity, or Availability, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If the organization does not use automated mechanisms to assist in the reporting of insider threat related security incidents, then coordinated response to, and recovery from, insider threat incidents will be delayed.

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

Justification to Select: IR-6(2) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If the organization does not report information system vulnerabilities associated with reported insider threat activities, then the same vulnerability could be exploited by another insider threat.

Parameter Value(s): The organization reports information system vulnerabilities associated with reported security incidents to *the IC Incident Response Center and USCYBERCOM*.

IR-7 Incident Response Assistance

Justification to Select: IR-7 is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If the organization does not provide an insider threat incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents, then potential insider threat related activity may not be promptly reported or handled.

IR-7(1) Incident Response Assistance | Automation Support for Availability of Information / Support

Justification to Select: IR-7(1) is selected in the CNSSI 1253 baseline categorized Moderate or High for Confidentiality, Integrity, or Availability, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If the organization does not employ automated mechanisms to increase the availability of insider threat incident response-related information and support, then potential insider threat related activity may not be promptly reported or handled.

IR-7(2) Incident Response Assistance | Coordination with External Providers

Justification to Select: IR-7(2) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If the organization does not establish a direct, cooperative relationship between its insider threat incident response capability and external providers of information system protection capability and identify organizational insider threat incident response team

members to the external providers, then the organization information systems and networks might not be properly protected and monitored for insider threat activity and insider threat incidents might not be promptly analyzed, detected, and responded to.

IR-8 Incident Response Plan

Justification to Select: IR-8 is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If the organization does not include insider threat incident response in its incident response plan, then response to insider threat incidents will be inconsistent and incomplete.

Parameter Value(s): The organization:

a. Develops an incident response plan that:
    1. Provides the organization with a roadmap for implementing its incident response capability;
    2. Describes the structure and organization of the incident response capability;
    3. Provides a high-level approach for how the incident response capability fits into the overall organization;
    4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
    5. Defines reportable incidents;
    6. Provides metrics for measuring the incident response capability within the organization;
    7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and
    8. Is reviewed and approved by *the CISO, if not otherwise defined in formal organizational policy*;

b. Distributes copies of the incident response plan to *all personnel with a role or responsibility for implementing the incident response plan*;

c. Reviews the incident response plan *at least annually (incorporating lessons learned from past incidents)*;

d. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;

e. Communicates incident response plan changes to *all personnel with a role or responsibility for implementing the incident response plan no later than 30 days after the change is made*; and

f. Protects the incident response plan from unauthorized disclosure and modification.

IR-9 Information Spillage Response

Justification to Select: IR-9 is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization responds to information spills by:

a. Identifying the specific information involved in the information system contamination;

b. Alerting *at a minimum, the Original Classification Authority (OCA), the information owner/originator, the ISSM, the activity security manager, and the SOC* of the information spill using a method of communication not associated with the spill;
c. Isolating the contaminated information system or system component;
d. Eradicating the information from the contaminated information system or component;
e. Identifying other information systems or system components that may have been subsequently contaminated; and
f. Performing other *actions as required or specified by policy or standard procedures*.

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

Justification to Select: IR-9(3) is selected in the CNSSI 1253 baseline for systems categorized Moderate or High for Availability and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization implements, *if necessary, any requisite continuity of operations (COOP) procedures* to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions.

IR-9(4) Information Spillage Response | Exposure to Unauthorized Personnel

Justification to Select: IR-9(4) is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization employs *security safeguards (e.g., making personnel exposed to spilled information aware of the federal laws, directives, policies, and/or regulations regarding the information and the restrictions imposed based on exposure to such information)* for personnel exposed to information not within assigned access authorizations.

IR-10 Integrated Information Security Analysis Team

Justification to Select: IR-10 is selected in the CNSSI 1253 baseline for systems categorized as Moderate or High for Confidentiality, Integrity, or Availability, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If the organization's integrated information security analysis team does not include analysts, tool developers, and operations personnel specialized in addressing insider threat, then insider threat incidents might not be properly assessed.

MA-1 System Maintenance Policy and Procedures

Justification to Select: MA-1 is selected in the CNSSI 1253 baseline for all systems and in the Privacy Overlay for Privacy Impact Levels of Moderate or High, and for PHI. MA-1 is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization:

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

1. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; and

b. Reviews and updates the current:

1. System maintenance policy *at least annually*; and
2. System maintenance procedures *at least annually*.

MA-2 Controlled Maintenance

Justification to Select: MA-2 is selected in the CNSSI 1253 baseline for all systems and in the Privacy Overlay for PHI. MA-2 is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization:

a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements;

b. Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;

c. Requires that *the ISSM, or designee,* explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;

d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs;

e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and

f. Includes:

(1) the date and time of maintenance,
(2) name of the individual performing the maintenance,
(3) name of escort (if necessary),
(4) a description of the type of maintenance performed, and
(4) a list of equipment removed or replaced (including identification numbers, if applicable)
in organizational maintenance records.

MA-2(2) Controlled Maintenance | Automated Maintenance Activities

Justification to Select: MA-2(2) is selected in the CNSSI 1253 baseline for systems categorized High for Confidentiality, Integrity, or Availability and is therefore applicable to systems or activities that directly support the Insider Threat Program.

MA-3 Maintenance Tools

Justification to Select: MA-3 is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: Unapproved maintenance tools can potentially be used by insider threat to access, store, and exfiltrate sensitive information. Maintenance tools can include, for example, portable IT hardware/software used for diagnostic testing and portable hardware/software packet sniffers and storage devices. If a system or the organization does not approve, control, and monitor information system maintenance tools, then an insider threat could use those unauthorized tools to compromise the system or network.

MA-3(1) Maintenance Tools | Inspect Tools

Justification to Select: MA-3(1) is selected in the CNSSI 1253 baseline for systems categorized Moderate or High for Integrity and is therefore applicable to systems or activities that directly support the Insider Threat Program.

MA-3(2) Maintenance Tools | Inspect Media

Justification to Select: MA-3(2) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system or the organization does not check media containing diagnostic and test programs for malicious code before the media are used in the information system, then media containing diagnostic and test programs can potentially be used by insider threat to introduce malicious code (e.g., sniffers, root kits, key stroke monitoring utilities) into systems.

MA-3(3) Maintenance Tools | Prevent Unauthorized Removal

Justification to Select: MA-3(3) is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization prevents the unauthorized removal of maintenance equipment containing organizational information by:
(a) Verifying that there is no organizational information contained on the equipment;
(b) Sanitizing or destroying the equipment;
(c) Retaining the equipment within the facility; or
(d) Obtaining an exemption from *the designated facility control officer* explicitly authorizing removal of the equipment from the facility.

MA-4(1) Nonlocal Maintenance | Auditing and Review

Justification to Select: MA-4(1) is selected in the CNSSI 1253 baseline for systems categorized Moderate or High for Integrity.

Supplemental Guidance: If a system does not audit and review all nonlocal maintenance sessions by organizational administrators, then an insider threat could use such sessions to compromise the system without detection.

Parameter Value(s): The organization:
(a) Audits nonlocal maintenance and diagnostic sessions *as defined in the organization's formal audit policy (see AU-1)*; and
(b) Reviews the records of the maintenance and diagnostic sessions.

MA-4(3) Nonlocal Maintenance | Comparable Security / Sanitization

Justification to Select: MA-4(3) is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

MA-5 Maintenance Personnel

Justification to Select: MA-5 is selected in the CNSSI 1253 baseline for all systems and in the Privacy Overlay for all Privacy Impact Levels and PHI. MA-5 is therefore applicable to systems or activities that directly support the Insider Threat Program.

MA-6 Timely Maintenance

Justification to Select: MA-6 is selected in the CNSSI 1253 baseline for systems categorized Moderate or High for Availability and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization obtains maintenance support and/or spare parts for *critical information system components (including CDS)* within *24 Hours* of failure *(Low and Moderate Availability) or immediately upon failure (High Availability)*.

MP-1 Media Protection Policy and Procedures

Justification to Select: MP-1 is selected in the CNSSI 1253 baseline for all systems.

Supplemental Guidance: If the organization does not establish and update media protection policies and procedures, then an insider threat could use media to exfiltrate information without detection.

Portable, electronic storage media devices, i.e. removable media, pose a significant threat to NSS even though such devices may have no independent processing capabilities. Use of removable media must be prohibited except where authorized by the AO of the department/agency. Where exceptions are authorized removable media use must be controlled in accordance with national policy on removable media. Examples of removable media include floppy disks, zip drives, compact disks (CD), digital video disks (DVD), external hard drives, thumb drives, and similar universal serial bus (USB) storage devices used to record or store information using magnetic, optical, or solid-state write capabilities.

Parameter Value(s): The organization:
a. Develops, documents, and disseminates to *all personnel (including end users, maintenance personnel, administrators, etc.)*:

1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls; and

b. Reviews and updates the current:
1. Media protection policy *at least annually*; and
2. Media protection procedures *at least annually*.

Regulatory/Statutory Reference(s): CNSSD 504, Section A.2.c.

MP-2 Media Access

Justification to Select: MP-2 is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Control Extension(s) and Parameter Value(s):

The Organization conducts *initial and annual* training for authorized users of removable media, to include the requirements of removable media usage.

The organization requires *initial and annual* acknowledgement within a written agreement by authorized users of removable media. The agreement specifies the authorized users' understanding of the proper usage of removable media on NSS and their obligation to notify the responsible parties in case of misuse or potential loss in accordance with established security incident reporting procedures.

Supplemental Guidance: If the organization does not restrict access to media, then an insider threat could access restricted information without authorization or exfiltrate information without detection.

Media devices are resources that can be used to exfiltrate classified information and access to the devices should be limited to authorized personnel. EO 13526 states that classified information may not be removed from official premises without proper authorization.

Training and awareness assist in the mitigation of the unwitting insider from doing unknown potential harm to NSS by creating awareness of policies and incident response reporting mechanisms. Signed user agreements enforce accountability and can help deter the insider threat by creating acknowledgement and consent to monitoring.

Parameter Value(s): The organization restricts access to *all types of digital and/or non-digital media containing information not cleared for public release* to *Information Assurance Officers, Data Transfer Agents, and specific individuals approved by the Chief Information Security Officer (CISO) based upon vital mission need*.

Regulatory/Statutory Reference(s): EO 13526, Section 4.1 (d); EO 13587, Section 5.2 (a) and Section 6.1; and CNSSD 504 Section A.2.c.

MP-3 Media Marking

Justification to Select: MP-3 is selected in the CNSSI 1253 baseline for systems categorized Moderate or High for Confidentiality, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system or the organization does not properly mark information system media, then an insider threat could be provided access to sensitive information without authorization.

Prior to introduction into an area with NSS or into a NSS, all removable media with the potential to contain sensitive or classified information must be clearly labeled. Once introduced into a NSS, removable media must be clearly labeled in accordance with appropriate classification guides. Any unlabeled removable media must be protected at the highest level of classification processed within the facility in which it resides. Clearly labeled media can help prevent data spillage and physical markings can identify improper use by the insider threat.

Parameter Value(s): The organization:
a. Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and
b. Exempts *new factory-sealed media* from marking as long as the media remain within *factory-sealed packages*.

Regulatory/Statutory Reference(s): CNSSD 504, Section A.2.c.v.1.

MP-4 Media Storage

Justification to Select: MP-4 is selected in the CNSSI 1253 baseline for systems categorized Moderate or High for Confidentiality or Integrity, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system or the organization does not physically control and securely store media or protect the media until it is destroyed, then an insider threat could gain access to sensitive information without authorization.

Portable, electronic storage media devices, i.e. removable media, pose a significant threat to NSS even though such devices may have no independent processing capabilities. Use of removable media must be prohibited except where authorized by the AO of the D/A. Where exceptions are authorized removable media use must be controlled in accordance with national policy on removable media. Examples of removable media include floppy disks, zip drives, compact disks (CD), digital video disks (DVD), external hard drives, thumb drives, and similar universal serial bus (USB) storage devices used to record or store information using magnetic, optical, or solid-state write capabilities.

Parameter Value(s): The organization:
a. Physically controls and securely stores *digital and non-digital media containing sensitive, controlled, and/or classified information* within *an area and/or container approved for storing*

data in accordance with the sensitivity and/or classification level (including DNI CAP compartments and sub-compartments) of the information contained on/within the media; and
b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

Regulatory/Statutory Reference(s): CNSSD 504, Section A.2.c.

MP-5 Media Transport

Justification to Select: MP-5 is selected in the CNSSI 1253 baseline for systems categorized Moderate or High for Confidentiality or Integrity, and in the Privacy Overlay for all Privacy Impact Levels and for PHI. MP-5 is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization:
a. Protects and controls *all digital and non-digital media containing sensitive, controlled, and/or classified information* during transport outside of controlled areas using *defined security safeguards (to include CNSSP No. 26):*
- For non-digital media containing classified information: Double-wrapping in opaque enclosures and transport only by personnel with a security clearance for the classification of the media being transported;
- For all other media and information: A manner that prevents loss or unauthorized access and restricted to authorized courier personnel;
- For digital media that contains PII or PHI: NSA approved or FIPS validated encryption;
b. Maintains accountability for information system media during transport outside of controlled areas;
c. Documents activities associated with the transport of information system media; and
d. Restricts the activities associated with the transport of information system media to authorized personnel.

MP-5(4) Media Transport | Cryptographic Protection

Justification to Select: MP-5(4) is selected in the CNSSI 1253 baseline for systems categorized Moderate or High for Confidentiality or Integrity, and in the Privacy Overlay for all Privacy Impact Levels and for PHI. MP-5(4) is therefore applicable to systems or activities that directly support the Insider Threat Program.

MP-6 Media Sanitization

Justification to Select: MP-6 is selected in the CNSSI 1253 baseline for all systems and in the Privacy Overlay for Privacy Impact Levels of Moderate or High, and for PHI. MP-6 is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization:
a. Sanitizes *all digital and non-digital information system media containing sensitive and classified information* prior to disposal, release out of organizational control, or release for reuse

using *in accordance with NIST SP 800-88r1 and NSA/CSS-POL 9-12 and all other applicable federal and organizational standards and policies*; and
b. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

MP-6(1) Media Sanitization | Review / Approve / Track / Document / Verify

Justification to Select: MP-6(1) is selected in the CNSSI 1253 baseline for systems categorized High for Confidentiality and in the Privacy Overlay for all Privacy Impact Levels and for PHI. MP-6(1) is therefore applicable to systems or activities that directly support the Insider Threat Program.

MP-6(2) Media Sanitization | Equipment Testing

Justification to Select: MP-6(2) is selected in the CNSSI 1253 baseline for systems categorized High for Confidentiality and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization tests sanitization equipment and procedures *every 6 months for the first two (2) years of operation, and annually thereafter* to verify that the intended sanitization is being achieved.

MP-6(3) Media Sanitization | Nondestructive Techniques

Justification to Select: MP-6(3) is selected in the CNSSI 1253 baseline for systems categorized High for Confidentiality and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization applies nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the information system under the following circumstances: *when such devices are first purchased from the manufacturer or vendor prior to initial use, when being considered for reuse, or when the organization loses a positive chain of custody for the device. Solid state media and media obtained from unknown sources shall not be reused. [Note: the use of nondestructive sanitization techniques is for the elimination of malicious code, not removal of approved information or software.]*.

MP-6(8) Media Sanitization | Remote Purging / Wiping of Information

Justification to Select: MP-6(8) is selected in the Privacy Overlay for Privacy Impact Levels of Moderate or High and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization provides the capability to purge/wipe information from *portable and mobile computing devices and media authorized to process or store classified, sensitive or controlled information* either remotely or under the following conditions: *when an unauthorized user attempts to access the device; or when the integrity and/or confidentiality of the device and/or its information has been, or is at risk of, compromise*.

MP-7 Media Use

Justification to Select: MP-7 is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Control Extension(s) and Parameter Value(s):

The organization shall establish an Organizational Devices Management Program to implement centralized purchasing, distribution, and registration of all new removable media and removable media devices (e.g., CD/DVD, USB portable drives, USB flash drives, USB thumb drives).

The organization shall officially designate individuals responsible for controlling removable media and removable media devices and those individuals shall account for (i.e., register, track, distribute, decommission) all removable media.

The organization shall only use write protectable media.

The organization blocks devices that are not approved for official usage, such as MP3 players, phones, and tablets.

The organization shall log, audit and monitor the use of removable media and employ an automated alert capability within a software tool to detect the unauthorized use of removable media.

The organization reports *immediately* suspected misuse or compromise of removable media or the information contained therein to *the appropriate security office*.

Supplemental Guidance: If a system or the organization does not properly restrict or prohibit the use of media on organizationally-specified systems, then an insider threat could use media to exfiltrate information.

For the purpose of this control and control extensions:
(1) The term Removable Media includes, but is not limited to:
    (a) compact disks (CD),
    (b) digital video disks (DVD),
    (c) floppy disks/diskettes,
    (d) zip disks,
    (e) magnetic tapes,
    (f) thumb drives,
    (g) pen drives,
    (h) Secure Digital (SD) cards,
    (i) Multi-media Cards (MMC),
    (h) flash drives and flash memory data storage devices, and
    (i) similar Universal Serial Bus (USB) connected storage media;
(2) The term Removable Media/Storage Devices includes, but is not limited to:
    (a) externally connected, and otherwise externally removable, hard drives,
    (b) CD/DVD drives,

(c) Small Computer Systems Interface (SCSI) connectable storage drives,
(d) Firewire connectable storage drives, and
(e) USB connectable storage drives and storage devices;
(3) The term Mobile Devices with Information Storage Capability includes, but is not limited to:
(a) MP3 players,
(b) smart phones,
(c) tablets,
(d) e-readers, and
(e) digital picture frames
Audit log records must be attributable to a specific user. Auditing and monitoring such activities can significantly reduce the detection time of potential insider threat indicators involving removable media.

Media must have a physical switch that can be flipped to a locked and unlocked position to make writing/saving to it impossible when in the locked position. In the case of media that does not have such a physical switch (CD, DVD-ROM, etc.), organizations must implement a capability that provides such media as one-time writeable only.

The organization should use Unified Cross Domain Management Office (UCDMO) certified cross-domain solutions to move data across classification boundaries and security domains. This allows for far fewer removable media actions. For example, cross-domain solutions run 'target word lists' on a document to be transferred and will either approve or deny the requested transfer action based on those results.

Parameter Value(s): The organization *restricts* the use of a*ll removable media, all removable media/storage devices, and all mobile devices with information storage capability* on *all information systems or system components* using:
(1) information system configurations that enforce restrictions as to which users or groups of users may access removable media;
(2) information system configurations that prohibit the auto-execution of programs residing on removable media; and
(3) information system build and maintenance procedures that ensure no removable media is connected to information systems that are not configured accordingly.

Regulatory/Statutory Reference(s): CNSSD 504, Section A.2.c. and national policy on removable media.

MP-7(1) Media Use | Prohibit Use Without Owner

Justification to Select: MP-7(1) is selected in the CNSSI 1253 baseline for all systems and in the Privacy Overlay for Privacy Impact Levels of Moderate or High. MP-7(1) is therefore applicable to systems or activities that directly support the Insider Threat Program.

MP-8 Media Downgrading

Justification to Select: MP-8 is selected in the Privacy Overlay for Privacy Impact Levels of Moderate or High, and for PHI. MP-8 is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization:
a. Establishes *downgrading processes consistent with NIST SP 800-88 and NSA/CSS-POL 9-12* that includes employing downgrading mechanisms with *the strength and integrity applicable to the classification and sensitivity of the information being downgraded*;
b. Ensures that the information system media downgrading process is commensurate with the security category and/or classification level of the information to be removed and the access authorizations of the potential recipients of the downgraded information;
c. Identifies *all electronic (magnetic, optical, and solid state) storage media requiring downgrading, to include, as appropriate: hard disks, floppy disks, zip drives, compact disks (CD), thumb drives, pen drives, and similar USB storage devices*; and
d. Downgrades the identified information system media using the established process.

MP-8(3) Media Downgrading | Controlled Unclassified Information

Justification to Select: MP-8(3) is selected in the Privacy Overlay for Privacy Impact Levels of Moderate or High, and for PHI. MP-8(3) is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization downgrades information system media containing *any Controlled Unclassified Information (CUI) (specifically including, but not limited to, PII and PHI)* prior to public release in accordance with applicable federal and organizational standards and policies.

PE-2 Physical Access Authorizations

Justification to Select: PE-2 is selected in the CNSSI 1253 baseline for all systems and in the Privacy Overlay for all Privacy Impact Levels, and for PHI. PE-2 is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization:
a. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides;
b. Issues authorization credentials for facility access;
c. Reviews the access list detailing authorized facility access by individuals *at least annually*; and
d. Removes individuals from the facility access list when access is no longer required.

PE-2(1) Physical Access Authorizations | Access by Position / Role

Justification to Select: PE-2(1) is selected in the Privacy Overlay for PHI and is therefore applicable to systems or activities that directly support the Insider Threat Program.

PE-3 Physical Access Control

Justification to Select: PE-3 is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system or the organization does not properly implement physical access controls, then an insider threat could gain physical access to systems or information without authorization.

Parameter Value(s): The organization:

a. Enforces physical access authorizations at *all entrances and exits to all facilities where the information system resides (including external boundaries designated as primary, maintenance and emergency as well as other internal boundaries separating areas within the facility officially designated as publicly accessible) commensurate with the level of information being processed in that facility* by;
    1. Verifying individual access authorizations before granting access to the facility; and
    2. Controlling ingress/egress to the facility using *physical access control mechanisms, such as badge and pin-pad controlled turnstiles, guards, sensors, and cameras*;

b. Maintains physical access audit logs for *all entrances and exits to all facilities where the information system resides (including external boundaries designated as primary and maintenance, as well as other internal boundaries separating areas within the facility officially designated as publicly accessible, but excluding (alarmed and continuously monitored) exits solely used for emergencies)*;

c. Provides *police officers, guards, cameras, sensors, and alarms* to control access to areas within the facility officially designated as publicly accessible;

d. Escorts visitors and monitors visitor activity *at all times when uncleared personnel are approved temporary access to classified or otherwise controlled areas, particularly SCIFs*;

e. Secures keys, combinations, and other physical access devices;

f. Inventories *at a minimum, keys or other physical token used to gain access, periodically as required by the facility manager, or at least annually. [Note: physical access devices do not need to be inventoried within SCIFs.];* and

g. Changes combinations and keys *as required by security relevant events* and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.

Regulatory/Statutory Reference(s): NDAA for Fiscal Year 2017, Subtitle F, Section 951, paragraph (a)(4).

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

Justification to Select: PE-3(1) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system or the organization does not properly implement physical access controls to information systems, then an insider threat could gain physical access to system components.

Parameter Value(s): The organization enforces physical access authorizations to the information system in addition to the physical access controls for the facility at *all entry/exit points to spaces*

(e.g., server rooms, data center) containing one or more IT components, commensurate with the level of information being processed by the information system components located within the spaces.

PE-5 Access Control for Output Devices

Justification to Select: PE-5 is selected in the CNSSI 1253 baseline for systems categorized Moderate or High for Confidentiality, and in the Privacy Overlay for all Privacy Impact Levels, and for PHI. PE-5 is therefore applicable to systems or activities that directly support the Insider Threat Program.

PE-6 Monitoring Physical Access

Justification to Select: PE-6 is selected in the CNSSI 1253 baseline for all systems and in the Privacy Overlay for PHI. PE-6 is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization:
a. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents;
b. Reviews physical access logs *at least every 30 days* and upon occurrence of *detected physical security incidents or apparent security violations or suspicious physical access activities*; and
c. Coordinates results of reviews and investigations with the organizational incident response capability.

PE-8 Visitor Access Records

Justification to Select: PE-8 is selected in the CNSSI 1253 baseline for all systems and in the Privacy Overlay for PHI. PE-8 is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization:
a. Maintains visitor access records to the facility where the information system resides for *two (2) years after the last date of entry*; and
b. Reviews visitor access records *at least every 30 days*.

PE-8(1) Visitor Access Records | Automated Records Maintenance / Review

Justification to Select: PE-8(1) is selected in the CNSSI 1253 baseline for systems categorized High for Confidentiality, Integrity, or Availability, and is therefore applicable to systems or activities that directly support the Insider Threat Program.

PE-18 Location of Information System Components

Justification to Select: PE-18 is selected in the Privacy Overlay for Privacy Impact Level of High, and for PHI. PE-18 is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization positions information system components within the facility to minimize potential damage from *all, site-specific, physical and environmental hazards* and to minimize the opportunity for unauthorized access.

PL-1 Security Planning Policy and Procedures

Justification to Select: PL-1 is selected in the CNSSI 1253 baseline for all systems and in the Privacy Overlay for PHI. PL-1 is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization:

a. Develops, documents, and disseminates to *all personnel (including end users, maintenance personnel, administrators, etc.)*:
    1. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    2. Procedures to facilitate the implementation of the security planning policy and associated security planning controls; and
b. Reviews and updates the current:
    1. Security planning policy *at least annually*; and
    2. Security planning procedures *at least annually*.

PL-2 System Security Plan

Justification to Select: PL-2 is selected in the CNSSI 1253 baseline for all systems and in the Privacy Overlay for all Privacy Impact Levels, and for PHI. PL-2 is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization:

a. Develops a security plan for the information system that:
   1. Is consistent with the organization's enterprise architecture;
   2. Explicitly defines the authorization boundary for the system;
   3. Describes the operational context of the information system in terms of missions and business processes;
   4. Provides the security categorization of the information system including supporting rationale;
   5. Describes the operational environment for the information system and relationships with or connections to other information systems;
   6. Provides an overview of the security requirements for the system;
   7. Identifies any relevant overlays, if applicable;
   8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and
   9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;

b. Distributes copies of the security plan and communicates subsequent changes to the plan to *at a minimum, the ISSO, ISSM, and SCA*;

c. Reviews the security plan for the information system *at least annually or when required due to system modifications*;

d. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and

e. Protects the security plan from unauthorized disclosure and modification.

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

Justification to Select: PL-2(3) is selected in the CNSSI 1253 baseline for systems categorized Moderate or High for Confidentiality, Integrity, or Availability, and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization plans and coordinates security-related activities affecting the information system with *all affected parties (including the NOC, ESC and associated system owners, etc.) for outages and, additionally, with the AO for security-related configuration changes* before conducting such activities in order to reduce the impact on other organizational entities.

PL-4 Rules of Behavior

Justification to Select: PL-4 is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system or the organization does not establish and obtain signed acknowledgement for information system rules of behavior, then an insider threat could perform unauthorized activities without repercussion.

Agreements signed by all cleared employees acknowledging that their activity on any agency classified or unclassified network, to include portable electronic devices, is subject to monitoring and could be used against them in a criminal, security, or administrative proceeding. Agreement language shall be approved by the Senior Official(s) in consultation with legal counsel.

Parameter Value(s): The organization:
a. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage;
b. Receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system;
c. Reviews and updates the rules of behavior *at least annually*; and
d. Requires individuals who have signed a previous version of the rules of behavior to read and re-sign when the rules of behavior are revised/updated.

Regulatory/Statutory Reference(s): White House Memo - National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, Section H.3.

PL-8 Information Security Architecture

Justification to Select: PL-8 is selected in the CNSSI 1253 baseline for all systems and in the Privacy Overlay for all Privacy Impact Levels. PL-8 is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization:
a. Develops an information security architecture for the information system that:
    1. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information;
    2. Describes how the information security architecture is integrated into and supports the enterprise architecture; and
    3. Describes any information security assumptions about, and dependencies on, external services;
b. Reviews and updates the information security architecture *at least annually or when changes to the information system or its environment warrant* to reflect updates in the enterprise architecture; and
c. Ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions.

PS-1 Personnel Security Policy and Procedures

Justification to Select: PS-1 is selected in the CNSSI 1253 baseline for all systems and in the Privacy Overlay for all Privacy Impact Levels, and for PHI. PS-1 is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization:

a. Develops, documents, and disseminates to *all personnel*:
    1. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    2. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls; and
b. Reviews and updates the current:
    1. Personnel security policy *at least annually*; and
    2. Personnel security procedures *at least annually*.

PS-2 Position Risk Designation

Justification to Select: PS-2 is selected in the CNSSI 1253 baseline for all systems and in the Privacy Overlay for all Privacy Impact Levels, and for PHI. PS-2 is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization:

a. Assigns a risk designation to all organizational positions;
b. Establishes screening criteria for individuals filling those positions; and
c. Reviews and updates position risk designations *at least annually or when the position description is updated or when the position is vacated*.

PS-3 Personnel Screening

Justification to Select: PS-3 is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Control Extension(s):

The organization supports Executive branch vetting policies, processes, and procedures through institutionalized enterprise-wide continuous performance improvement, which shall align with and support process improvements.

Supplemental Guidance: If a system or the organization does not screen individual prior to authorizing access to the information system and rescreen individuals according to the organization’s continuous evaluation policy, then the organization would not be aware of potential insider threat indicators.

Heads of agencies shall:
(i) designate, or cause to be designated, as a 'sensitive position,' any position occupied by a covered individual in which the occupant could bring about by virtue of the nature of the position, a material adverse effect on the national security;

(ii) establish and maintain within their respective agencies, an effective program to ensure that employment and retention of any covered individual within the agency is clearly consistent with the interests of national security and, as applicable, meets standards for eligibility for access to classified information or to hold a sensitive position, suitability, fitness, or credentialing, established by the respective Executive Agent.

An individual who has been determined to be eligible for or who currently has access to classified information shall be subject to continuous evaluation as further defined by and under standards (including, but not limited to, the frequency of such evaluation) as determined by the Director of National Intelligence.

All covered individuals shall be subject to continuous vetting under standards (including, but not limited to, the frequency of such vetting) as determined by the Security Executive Agent or the Suitability and Credentialing Executive Agent exercising its Suitability Executive Agent functions, as applicable.

Vetting shall include a search of records of the Federal Bureau of Investigation, including a fingerprint-based search, and any other appropriate biometric or database searches not precluded by law.

All investigations being conducted by agencies that develop information indicating that an individual may have been subjected to coercion, influence, or pressure to act contrary to the interests of the national security, or information that the individual may pose a counterintelligence or terrorist threat, or as otherwise provided by law, shall be referred to the Federal Bureau of Investigation for potential investigation, and may also be referred to other agencies where appropriate.

Recipient departments and agencies may retain and use the received reports, information, and other investigative material within that recipient for authorized purposes (including, but not limited to, adjudications, hearings and appeals, continuous evaluation, inspector general functions, counterintelligence, research, and insider threat programs), in compliance with the Privacy Act of 1974, as amended (section 552a of title 5, United States Code).

Recipient departments and agencies shall not make any external releases of received information, other than to an investigative subject for the purpose of providing procedural rights or administrative due process; and shall direct any other requests for external releases of copies of the reports, information, and other investigative materials to the investigative agency. In the event redisclosure by the recipient agency is required by compulsory legal process, the recipient agency shall consult with the investigating agency.

Parameter Value(s): The organization:

a. Screens individuals prior to authorizing access to the information system; and

b. Rescreens individuals according to *personnel security guidelines, to include, but is not limited to, life changes such as marriage, divorce, co-habitation, arrests or other involvement with law enforcement, medical, or financial conditions. Periodic rescreening shall be accomplished at least every five years*.

Regulatory/Statutory Reference(s): NDAA for Fiscal Year 2017, Subtitle F, Section 951, paragraph (a)(4); EO 12968, Section 3.5.(b)(i), as Revised; EO 13467 Sections 1.1.(e), 2.1.(d) & (e), 2.3, and 2.7.(b) & (c), as Revised; and January 17, 2017 Executive Order Amending the Civil Service Rules, Executive Order 13488, and Executive Order 13467.

PS-3(3) Personnel Screening | Information with Special Protection Measures

Justification to Select: PS-3(3) is selected in the Privacy Overlay for all Privacy Impact Levels, and for PHI. PS-3(3) is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization ensures that individuals accessing an information system processing, storing, or transmitting information requiring special protection:

(a) Have valid access authorizations that are demonstrated by assigned official government duties; and
(b) Satisfy *prescribed additional personnel screening criteria (e.g., for CUI) and organization defined personnel screening criteria commensurate with increasing level of risk and responsibility for access to, or use of, different levels of PII or PHI.*

PS-4 Personnel Termination

Justification to Select: PS-4 is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system or the organization does not promptly disable information system access and terminate/revoke any authenticators/credentials associated with the terminated individual, then an insider threat could misuse those system accesses and authenticators/credentials to gain unauthorized access to systems and sensitive information.

Organizations should confirm that accesses and privileges have been revoked for any individual whose position and duties no longer require such access and privileges, and that user accounts have been disabled for all individuals who are no longer employed by or assigned to the organization.

Parameter Value(s): The organization, upon termination of individual employment:
a. Disables information system access within: *if voluntary, as soon as possible, not to exceed 5 working days; if involuntary, immediately, within same day as termination*;
b. Terminates/revokes any authenticators/credentials associated with the individual;
c. Conducts exit interviews that include a discussion of *at least, prohibitions against: (i) the removal of classified information from the organization's control; (ii) direction that information be declassified in order to remove it from the organization's control; and (iii) the proper handling of organizational information*;
d. Retrieves all security-related organizational information system-related property;
e. Retains access to organizational information and information systems formerly controlled by terminated individual; and

f. Notifies *at a minimum, the system security administrator, ISSO, and personnel responsible for revoking credentials and access, immediately, not to exceed 24 hours*.

Regulatory/Statutory Reference(s): NDAA for Fiscal Year 2017, Subtitle F, Section 951, paragraph (a)(4); and Office of the Secretary of Defense Insider Threat Mitigation, 12 July 2013.

PS-4(2) Personnel Termination | Automated Notification

Justification to Select: PS-4(2) is selected in the CNSSI 1253 baseline for systems categorized High for Confidentiality, Integrity, or Availability and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization employs automated mechanisms to notify *at a minimum, the system security administrator, ISSO and personnel responsible for revoking credentials and access* upon termination of an individual.

PS-5 Personnel Transfer

Justification to Select: PS-5 is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system or the organization does not review and confirm an individual's operational need for access authorizations as part of the personnel transfer process, then an insider threat could misuse those previous access authorizations, which are no longer appropriate to their new assignment, to gain unauthorized access to systems and sensitive information.

Parameter Value(s): The organization:
a. Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization;
b. Initiates *reassignment actions to ensure all system access no longer required (need to know) are removed or disabled immediately (e.g.,* within *1 working day for CDS or within 10 working days for NSS) following the formal transfer action*;
c. Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and
d. Notifies *the systems security administrator, ISSO and personnel responsible for assigning and transferring credentials* within *24 hours*.

Regulatory/Statutory Reference(s): NDAA for Fiscal Year 2017, Subtitle F, Section 951, paragraph (a)(4).

PS-6 Access Agreements

Justification to Select: PS-6 is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system or the organization does not develop and maintain access agreements and regularly obtain each individual user's signed re-acknowledgement of the conditions of the agreement, then an organization might not be able to hold an insider threat accountable for their malicious or unauthorized activities.

Parameter Value(s): The organization:
a. Develops and documents access agreements for organizational information systems;
b. Reviews and updates the access agreements *at least annually*; and
c. Ensures that individuals requiring access to organizational information and information systems:
    1. Sign appropriate access agreements prior to being granted access; and
    2. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or *when there is a change to the user's level of access, but at least annually*.

Regulatory/Statutory Reference(s): NDAA for Fiscal Year 2017, Subtitle F, Section 951, paragraph (a)(4).

PS-6(3) Access Agreements | Post-Employment Requirements

Justification to Select: PS-6(3) is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

PS-7 Third-Party Personnel Security

Justification to Select: PS-7 is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system or the organization does not properly document and manage third-party personnel security requirements, policies and procedures (per PS-7), then a third-party individual could use their access to conduct insider threat activities or a third-party individual's access could be misused by an insider threat to gain unauthorized access to systems or sensitive information.

Parameter Value(s): The organization:
a. Establishes personnel security requirements including security roles and responsibilities for third-party providers;
b. Requires third-party providers to comply with personnel security policies and procedures established by the organization;
c. Documents personnel security requirements;
d. Requires third-party providers to notify *the organizational Security Manager, the system security administrator, the ISSO, and personnel responsible for transferring credentials of any personnel transfers or terminations of third-party personnel who possess organizational credentials* of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within *immediately, not to exceed 24 hours*; and
e. Monitors provider compliance.

Regulatory/Statutory Reference(s): NDAA for Fiscal Year 2017, Subtitle F, Section 951, paragraph (a)(4).

PS-8 Personnel Sanctions

Justification to Select: PS-8 is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system or the organization does not employ a formal sanctions process for individuals failing to comply with established information security policies and procedures, and promptly and fully notify management and other oversight authorities when a formal employee sanctions process is initiated, then potential insider threats might not be properly monitored for subsequent potential insider threat activities.

Parameter Value(s): The organization:
a. Employs a formal sanctions process for individuals failing to comply with established information security policies and procedures; and
b. Notifies *at a minimum, the system security administrator and ISSO immediately* when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

Regulatory/Statutory Reference(s): NDAA for Fiscal Year 2017, Subtitle F, Section 951, paragraph (a)(4).

RA-2 Security Categorization

Justification to Select: RA-2 is selected in the CNSSI 1253 baseline for all systems and in the Privacy Overlay for all Privacy Impact Levels, and for PHI. RA-2 is therefore applicable to systems or activities that directly support the Insider Threat Program.

RA-3 Risk Assessment

Justification to Select: RA-3 is selected in the CNSSI 1253 baseline for all systems and in the Privacy Overlay for all Privacy Impact Levels, and for PHI. RA-3 is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization:
a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;
b. Documents risk assessment results in *a Risk Assessment Report to include an evaluation of risks associated with the potential impact of loss of the PII; all risk assessment documentation must reflect these findings*;
c. Reviews risk assessment results *upon re-accreditation, but at least annually*;
d. Disseminates risk assessment results to *the system security administrator, ISSO, ISSM, Accreditation Official, and Program Manager*; and

e. Updates the risk assessment *upon reaccreditation, but at least annually* or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

RA-5 Vulnerability Scanning

Justification to Select: RA-5 is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system or the organization does not regularly employ vulnerability scanning tools and promptly remediate identified vulnerabilities, then an insider threat could exploit the vulnerabilities to gain unauthorized access to systems or sensitive information.

Parameter Value(s): The organization:
a. Scans for vulnerabilities in the information system and hosted applications *at least every 30 days* and when new vulnerabilities potentially affecting the system/applications are identified and reported;
b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
1. Enumerating platforms, software flaws, and improper configurations;
2. Formatting checklists and test procedures; and
3. Measuring vulnerability impact;
c. Analyzes vulnerability scan reports and results from security control assessments;
d. Remediates legitimate vulnerabilities *as specifically authorized for the system, in accordance with any authoritative source (e.g., IC-IRC, IAVM, ICVM, CTOs, DTMs, and STIGs),* in accordance with an organizational assessment of risk; and
e. Shares information obtained from the vulnerability scanning process and security control assessments with, *at a minimum, the systems security administrator, ISSO and ISSM* to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

Regulatory/Statutory Reference(s): NDAA for Fiscal Year 2017, Subtitle F, Section 951, paragraph (a)(4).

RA-5(1) Vulnerability Scanning | Update Tool Capability

Justification to Select: RA-5(1) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system or the organization does regularly update vulnerability scanning tools with new vulnerability signatures, then an insider threat could exploit undetected vulnerabilities to gain unauthorized access to systems or sensitive information.

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

Justification to Select: RA-5(2) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system or the organization does regularly update vulnerability scanning tools with new vulnerability signatures, then an insider threat could exploit undetected vulnerabilities to gain unauthorized access to systems or sensitive information.

Parameter Value(s): The organization updates the information system vulnerabilities scanned *at least monthly; within 24 hours prior to running scans; as required by the ICVM (Intelligence Community Vulnerability Management) program; and when new vulnerabilities are identified and reported*.

RA-5(4) Vulnerability Scanning | Discoverable Information

Justification to Select: RA-5(4) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system or the organization does not regularly determine what information about the information system is discoverable by insider threats and take appropriate corrective actions, then an insider could use the discoverable information to compromise the system.

Parameter Value(s): The organization determines what information about the information system is discoverable by adversaries and subsequently takes *the necessary corrective actions to remediate all unacceptable risks*.

RA-5(5) Vulnerability Scanning | Privileged Access

Justification to Select: RA-5(5) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system or the organization does not require and implement privileged access authorization to sensitive or critical information system components to conduct in-depth vulnerability scanning activities, then some vulnerabilities may not be detected and an insider threat exploit those undetected vulnerabilities to compromise the system.

Parameter Value(s): The information system implements privileged access authorization to *vulnerability scanning components as selected and authorized by the CISO/SISO or formally appointed designee*.

RA-5(10) Vulnerability Scanning | Correlate Scanning Information

Justification to Select: RA-5(10) is selected in the CNSSI 1253 baseline for systems categorized High for Confidentiality, Integrity, or Availability and is therefore applicable to systems or activities that directly support the Insider Threat Program.

SA-2 Allocation of Resources

Justification to Select: SA-2 is selected in the CNSSI 1253 baseline for all systems and in the Privacy Overlay for all Privacy Impact Levels. SA-2 is therefore applicable to systems or activities that directly support the Insider Threat Program.

SA-3 System Development Life Cycle

Justification to Select: SA-3 is selected in the CNSSI 1253 baseline for all systems and in the Privacy Overlay for all Privacy Impact Levels. SA-3 is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization:
a. Manages the information system using *system development life cycle process and procedures* that incorporates information security considerations;
b. Defines and documents information security roles and responsibilities throughout the system development life cycle;
c. Identifies individuals having information security roles and responsibilities; and
d. Integrates the organizational information security risk management process into system development life cycle activities.

SA-4 Acquisition Process

Justification to Select: SA-4 is selected in the CNSSI 1253 baseline for all systems and in the Privacy Overlay for all Privacy Impact Levels, and for PHI. SA-4 is therefore applicable to systems or activities that directly support the Insider Threat Program.

SA-4(1) Acquisition Process | Functional Properties of Security Controls

Justification to Select: SA-4(1) is selected in the CNSSI 1253 baseline for systems categorized Moderate or High for Confidentiality, Integrity, or Availability and is therefore applicable to systems or activities that directly support the Insider Threat Program.

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

Justification to Select: SA-4(2) is selected in the CNSSI 1253 baseline for systems categorized Moderate or High for Confidentiality, Integrity, or Availability and is therefore applicable to systems or activities that directly support the Insider Threat Program.

SA-4(3) Acquisition Process | Development Methods / Techniques / Practices

Justification to Select: SA-4(3) is selected in the CNSSI 1253 baseline for systems categorized High for Integrity and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization requires the developer of the information system, system component, or information system service to demonstrate the use of a system development life cycle that includes *state-of-the practice system/security engineering methods, software development methods, testing/evaluation/validation techniques, quality control processes and other methods and processes*.

SA-4(5) Acquisition Process | System / Component / Service Configurations

Justification to Select: SA-4(5) is selected in the CNSSI 1253 baseline for systems categorized High for Integrity and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization requires the developer of the information system, system component, or information system service to:
(a) Deliver the system, component, or service with *deliver the system, component, or service with SSP-defined security configurations, to include, organization baseline and STIG security configurations, and all limitations on functions, ports, protocols, and services fully* implemented; and
(b) Use the configurations as the default for any subsequent system, component, or service reinstallation or upgrade.

SA-4(7) Acquisition Process | NIAP-Approved Protection Profiles

Justification to Select: SA-4(7) is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

SA-4(9) Acquisition Process | Functions / Ports / Protocols / Services in Use

Justification to Select: SA-4(9) is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

SA-4(10) Acquisition Process | Use of Approved PIV Products

Justification to Select: SA-4(10) is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

SA-5 Information System Documentation

Justification to Select: SA-5 is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization:
a. Obtains administrator documentation for the information system, system component, or information system service that describes:
1. Secure configuration, installation, and operation of the system, component, or service;
2. Effective use and maintenance of security functions/mechanisms; and
3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;
b. Obtains user documentation for the information system, system component, or information system service that describes:
1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;
2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and

3. User responsibilities in maintaining the security of the system, component, or service;

c. Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and takes *requisite action to recreate or develop the missing documentation (if such documentation is essential to the effective implementation or operation of security controls)* in response;

d. Protects documentation as required, in accordance with the risk management strategy; and

e. Distributes documentation to *at a minimum, the ISSO, ISSM, and SCA*.

SA-8 Security Engineering Principles

Justification to Select: SA-8 is selected in the CNSSI 1253 baseline for all systems and in the Privacy Overlay for all Privacy Impact Levels. SA-8 is therefore applicable to systems or activities that directly support the Insider Threat Program.

SA-9 External Information System Services

Justification to Select: SA-9 is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization:

a. Requires that providers of external information system services comply with organizational information security requirements and employ *the security controls defined by CNSSI 1253 (including those specified in the applicable overlay attachments)* in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;

b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and

c. Employs *pre-established and mutually agreed upon processes, methods, and techniques* to monitor security control compliance by external service providers on an ongoing basis.

SA-10 Developer Configuration Management

Justification to Select: SA-10 is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization requires the developer of the information system, system component, or information system service to:

a. Perform configuration management during system, component, or service *design, development, implementation, and operation*;

b. Document, manage, and control the integrity of changes to *all configuration items under configuration management*;

c. Implement only organization-approved changes to the system, component, or service;

d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and

e. Track security flaws and flaw resolution within the system, component, or service and report findings to *at a minimum, the ISSE, ISSO, ISSM and Program Manager*.

SA-10(1) Developer Configuration Management | Software / Firmware Integrity Verification

Justification to Select: SA-10(1) is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

SA-11 Developer Security Testing and Evaluation

Justification to Select: SA-11 is selected in the CNSSI 1253 baseline for systems categorized Moderate or High for Confidentiality, Integrity, or Availability, and in the Privacy Overlay for Privacy Impact Levels of Moderate or High. SA-11 is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization requires the developer of the information system, system component, or information system service to:

a. Create and implement a security assessment plan;
b. Perform *unit, integration, system, and regression* testing/evaluation at *the depth of security testing/evaluation required for the product and to cover all of the artifacts included*;
c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation;
d. Implement a verifiable flaw remediation process; and
e. Correct flaws identified during security testing/evaluation.

SA-11(5) Developer Security Testing and Evaluation | Penetration Testing

Justification to Select: SA-11(5) is selected in the Privacy Overlay for Privacy Impact Level of High and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization requires the developer of the information system, system component, or information system service to perform penetration testing *as specified in CA-8.*

SA-12 Supply Chain Protection

Justification to Select: SA-12 is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization protects against supply chain threats to the information system, system component, or information system service by employing *security safeguards in accordance with CNSSD No. 505 and measures of protection in accordance with DoDI 5200.44* as part of a comprehensive, defense-in-breadth information security strategy.

SA-12(1) Supply Chain Protection | Acquisition Strategies / Tools / Methods

Justification to Select: SA-12(1) is selected in the CNSSI 1253 baseline for systems categorized High for Confidentiality, Integrity, or Availability and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization employs *tailored acquisition strategies, contract tools, and procurement methods* for the purchase of the information system, system component, or information system service from suppliers.

SA-12(9) Supply Chain Protection | Operations Security

Justification to Select: SA-12(9) is selected in the CNSSI 1253 baseline for systems categorized High for Confidentiality, Integrity, or Availability and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization employs *Operations Security (OPSEC) safeguards* in accordance with classification guides to protect supply chain-related information for the information system, system component, or information system service.

SA-14 Criticality Analysis

Justification to Select: SA-14 is selected in the CNSSI 1253 baseline for systems categorized High for Confidentiality, Integrity, or Availability and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization identifies critical information system components and functions by performing a criticality analysis for *all information systems, information system components and information system services* at *all design reviews (i.e., Preliminary, Incremental/Supplementary, and Critical).*

SA-15 Development Process, Standards, and Tools

Justification to Select: SA-15 is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization:

a. Requires the developer of the information system, system component, or information system service to follow a documented development process that:

1. Explicitly addresses security requirements;
2. Identifies the standards and tools used in the development process;
3. Documents the specific tool options and tool configurations used in the development process; and
4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and

b. Reviews the development process, standards, tools, and tool options/configurations *before first use and annually thereafter* to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy *established security requirements*.

SA-15(3) Development Process, Standards, and Tools | Criticality Analysis

Justification to Select: SA-15(3) is selected in the CNSSI 1253 baseline for systems categorized High for Confidentiality, Integrity, or Availability and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization requires the developer of the information system, system component, or information system service to perform a criticality analysis at *the system level as determined by the system security boundary* and at *a program milestone decision point no later than the Critical Design Review (CDR) milestone*.

SA-15(4) Development Process, Standards, and Tools | Threat Modeling / Vulnerability Analysis

Justification to Select: SA-15(4) is selected in the CNSSI 1253 baseline for systems categorized High for Confidentiality, Integrity, or Availability and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization requires that developers perform threat modeling and a vulnerability analysis for the information system *in terms of the impact of the function or component failure on the ability of the component to complete organizational missions supported by the information system* that:
(a) Uses *information concerning impact, environment of operations, known or assumed threats, and acceptable risk levels*;
(b) Employs *available enterprise tools and methods*; and
(c) Produces evidence that meets *defined risk acceptance criteria*.

SA-15(7) Development Process, Standards, and Tools | Automated Vulnerability Analysis

Justification to Select: SA-15(7) is selected in the CNSSI 1253 baseline for systems categorized High for Integrity and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization requires the developer of the information system, system component, or information system service to:
(a) Perform an automated vulnerability analysis using *approved tools*;
(b) Determine the exploitation potential for discovered vulnerabilities;
(c) Determine potential risk mitigations for delivered vulnerabilities; and
(d) Deliver the outputs of the tools and results of the analysis to *the ISSE, ISSO, ISSM and Program Manager*.

SA-15(9) Development Process, Standards, and Tools | Incident Response Plan

Justification to Select: SA-15(9) is selected in the CNSSI 1253 baseline for all systems and in the Privacy Overlay for Privacy Impact Levels of Moderate or High. SA-15(9) is therefore applicable to systems or activities that directly support the Insider Threat Program.

SA-16 Developer-Provided Training

Justification to Select: SA-16 is selected in the CNSSI 1253 baseline for systems categorized High for Confidentiality, Integrity, or Availability and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization requires the developer of the information system, system component, or information system service to provide *training (options include classroom-style training, web-based/computer-based training, and hands-on training)* on the correct use and operation of the implemented security functions, controls, and/or mechanisms.

SA-17 Developer Security Architecture and Design

Justification to Select: SA-17 is selected in the CNSSI 1253 baseline for systems categorized High for Confidentiality, Integrity, or Availability, and in the Privacy Overlay for all Privacy Impact Levels. SA-17 is therefore applicable to systems or activities that directly support the Insider Threat Program.

SA-19 Component Authenticity

Justification to Select: SA-19 is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization:
a. Develops and implements anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the information system; and
b. Reports counterfeit information system components to *at a minimum, USCYBERCOM, ISSE, ISSO, ISSM, and Program Manager*.

SA-21 Developer Screening

Justification to Select: SA-21 is selected in the Privacy Overlay for all Privacy Impact Levels, and for PHI. SA-21 is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization requires that the developer of *systems containing PII or PHI*:
a. Have appropriate access authorizations as determined by assigned *contracting officer and contracting officer representative, in consultation with the organization's privacy office*; and
b. Satisfy *organization defined personnel screening criteria commensurate with increasing level of risk and responsibility for access to, or use of, different levels of PII*.

SA-22 Unsupported System Components

Justification to Select: SA-22 is selected in the CNSSI 1253 baseline for systems categorized High for Confidentiality, Integrity, or Availability and is therefore applicable to systems or activities that directly support the Insider Threat Program.

SC-1 System and Communications Protection Policy and Procedures

Justification to Select: SC-1 is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization:

a. Develops, documents, and disseminates to *all personnel (including, at a minimum, the ISSO, ISSM, maintenance personnel, administrators, etc.)*:

1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and

b. Reviews and updates the current:

1. System and communications protection policy *at least annually*; and
2. System and communications protection procedures *at least annually*.

SC-2 Application Partitioning

Justification to Select: SC-2 is selected in the CNSSI 1253 baseline for systems categorized Moderate or High for Confidentiality or Integrity, and in the Privacy Overlay for Privacy Impact Levels of Moderate or High, and for PHI. SC-2 is therefore applicable to systems or activities that directly support the Insider Threat Program.

SC-3 Security Function Isolation

Justification to Select: SC-3 is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

SC-4 Information in Shared Resources

Justification to Select: SC-4 is selected in the CNSSI 1253 baseline for systems categorized Moderate or High for Confidentiality, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system does not prevent unauthorized and unintended information transfer via its shared system resources, then an insider threat could be exposed, or gain access, to sensitive information without authorization.

Data Loss and Spillage Prevention (DLSP) capabilities must address misuse of data in the following:

i. User initiated activities:

1. Files - move, copy/paste, burn/print, upload
2. Email - attach, copy/paste, compose, send
3. Application Data – view/delete, modify, copy/paste

ii. To data destinations:

1. Devices
2. Network
3. Applications

4. Printers
5. Internet Protocol (IP) address
6. Recipients

iii. Responses to user initiated activities:

1. Incident alert
2. Prompt user
3. Warn user
4. Encrypt data
5. Block action
6. Mask data

Regulatory/Statutory Reference(s): CNSSD 504, Section A.2.d.

SC-5(1) Denial of Service Protection | Restrict Internal Users

Justification to Select: SC-5(1) is selected in the CNSSI 1253 baseline for all systems.

Supplemental Guidance: If the organization does not restrict the ability of individuals to launch denial of service attacks, then hostile insiders could use the system as a platform to launch cyber-attacks against other enterprise systems or third parties.

Protection against an insider threat having the ability to launch denial of service attacks is typically implemented on boundary devices prohibiting egress to potential target systems.

Parameter Value(s): The information system restricts the ability of individuals to launch *network, operating system, or application layer denial of service attacks* against other information systems.

SC-5(2) Denial of Service Protection | Excess Capacity / Bandwidth / Redundancy

Justification to Select: SC-5(2) is selected in the CNSSI 1253 baseline for systems categorized Moderate or High for Availability.

Supplemental Guidance: If the organization does not manage excess system capacity, bandwidth, or other redundancy to limit the effects of information flooding denial of service attacks, then the network or systems may not have sufficient capacity to counter flooding attacks launched by insider threat activities.

Management of excess capacity, bandwidth, or other redundancy to limit the effects of information flooding denial of service attacks is typically implemented at the enterprise (e.g., network) level.

SC-5(3) Denial of Service Protection | Detection / Monitoring

Justification to Select: SC-5(3) is selected in the CNSSI 1253 baseline for systems categorized Moderate or High for Availability and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization:

(a) Employs *monitoring tools, technologies and techniques approved by the Authorization Official and Designate Authorization Official, as appropriate,* to detect indicators of denial of service attacks against the information system; and
(b) Monitors *information system resources (including, but not limited to physical disk storage, memory, CPU cycles, and, as applicable, CDS resources)* to determine if sufficient resources exist to prevent effective denial of service attacks.

SC-7(5) Boundary Protection | Deny by Default / Allow by Exception

Justification to Select: SC-7(5) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system does not, by default, deny network communications traffic at managed interfaces, except for specifically allowed communications, then a malicious insider could establish an unauthorized network connection to download malware or exfiltrate information.

Policy-based restrictions on wired or wireless network connections and secure network connection configurations will prevent a malicious insider from exploiting the known vulnerability of hard-linking to areas outside of their authorized access.

Regulatory/Statutory Reference(s): CNSSD 504 Section A.2.d.

SC-7(9) Boundary Protection | Restrict Threatening Outgoing Communications Traffic

Justification to Select: SC-7(9) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system or the organization does not detect and deny outgoing communications traffic posing a threat to external information systems and audit the identity of internal users associated with denied communications, then hostile insiders could use an internal system as a platform to launch cyber-attacks against external third parties.

SC-7(10) Boundary Protection | Prevent Unauthorized Exfiltration

Justification to Select: SC-7(10) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system or the organization does not inspect and control outbound traffic using managed interfaces at enclave and network boundaries, then an insider threat could use the unguarded interface point to exfiltrate sensitive information.

Safeguards to prevent unauthorized exfiltration of information across managed interfaces are typically implemented by the enterprise at network boundaries (e.g., cross-domain solutions). These safeguards serve to inhibit unauthorized data exfiltration by an insider threat.

Regulatory/Statutory Reference(s): EO 13587, Section 2.1(b) and Section 5.2 (a); White House Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, Tab 2, Section H.1.

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

Justification to Select: SC-7(11) is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The information system only allows incoming communications from *authorized sources, specifically approved and documented in the SSP* to be routed to *authorized destinations, specifically approved and documented in SSP*.

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

Justification to Select: SC-7(12) is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization implements *Host Intrusion Prevention Solutions (HIPS)* at *all system components capable of supporting host-based boundary protection mechanisms such as but not limited to servers, workstations, and those subject to operation outside of the organizational boundary (i.e., laptops and other mobile devices)*.

SC-7(13) Boundary Protection | Isolation of Security Tools / Mechanisms / Support Components

Justification to Select: SC-7(13) is selected in the CNSSI 1253 baseline for all systems.

Supplemental Guidance: If the organization does not isolate security tools on subnetworks, separate from the main network, then an insider threat on the main network could use the direct connection to compromise or exploit the security tools.

Isolation of security tools is typically implemented at the network level for the enterprise.

Parameter Value(s): The organization isolates *key information security tools, mechanisms, and support components such as, but not limited to:*
- Public Key Infrastructure (PKI);
- Patching servers and infrastructure;
- Host Based Security Solutions;
- Computer Network Defense (CND) Tools;
- Special Purpose Gateways;
- Vulnerability scanning tools and tracking systems;
- Honeypots;
- Internet access points (IAPs);
- Network element and data center administrative/management traffic;
- Demilitarized Zones (DMZs);
- Server farms/computing centers; centralized audit log servers; etc.)
from other internal information system components by implementing physically separate subnetworks with managed interfaces to other components of the system.

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

Justification to Select: SC-7(14) is selected in the CNSSI 1253 baseline for all systems and in the Privacy Overlay for PHI. SC-7(14) is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization protects against unauthorized physical connections at *any managed interface that crosses security domains or connects to an external network; such as but not limited to: cross domain solutions (SABI, TSABI), an enclave or network boundary with a WAN, a partner network, or the Internet (Internet Access Points); any DoD Approved Alternate Gateway; and those organization-defined managed interfaces necessary to prevent unauthorized physical access, tampering, and theft of PHI*.

SC-7(15) Boundary Protection | Route Privileged Network Accesses

Justification to Select: Although SC-7(15) is not selected in the CNSSI 1253 baseline or an overlay, SC-7(15) is commonly implemented to generate privileged user audit information for insider threat detection and analysis.

Supplemental Guidance: If a system or the organization does not route all networked, privileged accesses through a dedicated, managed interface for purposes of access control and auditing, then an insider threat could use the system's main interface to execute privileged functions without detection.

Regulatory/Statutory Reference(s): NDAA for Fiscal Year 2017, Subtitle F, Section 951, paragraph (a)(4).

SC-7(18) Boundary Protection | Fail Secure

Justification to Select: SC-7(18) is selected in the CNSSI 1253 baseline for systems categorized High for Confidentiality, Integrity, or Availability and is therefore applicable to systems or activities that directly support the Insider Threat Program.

SC-7(21) Boundary Protection | Isolation of Information System Components

Justification to Select: SC-7(21) is selected in the CNSSI 1253 baseline for systems categorized High for Confidentiality or Integrity and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization employs boundary protection mechanisms to separate *information system components* supporting *missions and/or business functions evaluated to have High Confidentiality or Integrity criticality*.

SC-8 Transmission Confidentiality and Integrity

Justification to Select: SC-8 is selected in the CNSSI 1253 baseline for all systems and in the Privacy Overlay for all Privacy Impact Levels, and for PHI. SC-8 is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The information system protects the *confidentiality and integrity* of transmitted information.

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

Justification to Select: SC-8(1) is selected in the CNSSI 1253 baseline for all systems and in the Privacy Overlay for all Privacy Impact Levels, and for PHI. SC-8(1) is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The information system implements cryptographic mechanisms to *prevent unauthorized disclosure of, and detect changes to, information (including PII and PHI)* during transmission unless otherwise protected by *alternative physical safeguards to prevent unauthorized access to or alteration of the information as defined within the SSP, such as keeping transmission within physical areas rated IAW the sensitivity of the information or within a Protected Distribution System (PDS) when traversing areas not approved for the sensitivity of the information.*

SC-8(2) Transmission Confidentiality and Integrity | Pre / Post Transmission Handling

Justification to Select: SC-8(2) is selected in the CNSSI 1253 baseline for systems categorized Moderate or High for Confidentiality or Integrity, and in the Privacy Overlay for Privacy Impact Levels of Moderate or High. SC-8(2) is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The information system maintains the *confidentiality and integrity* of information during preparation for transmission and during reception.

SC-10 Network Disconnect

Justification to Select: SC-10 is selected in the CNSSI 1253 baseline for systems categorized Moderate or High for Confidentiality or Integrity, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system does not terminate the network connection at the end of the session or after a defined time period of inactivity, then an insider threat could hijack the connection to take over the inactive session.

Parameter Value(s): The information system terminates the network connection associated with a communications session at the end of the session or after:

(1) For DoD Systems: 10 minutes of inactivity *for in-band management sessions and 15 minutes* of inactivity *for user sessions; or*

(2) *For all other (non-DoD) NSS: No more than one hour* of inactivity.

Regulatory/Statutory Reference(s): EO 13587, Sec. 2.1(b) and Sec. 5.2 (a); and White House Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, Tab 2, Sec. H.1.

SC-12 Cryptographic Key Establishment and Management

Justification to Select: SC-12 is selected in the CNSSI 1253 baseline for all systems and in the Privacy Overlay for all Privacy Impact Levels, and for PHI. SC-12 is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with:
- DoDI 8520.02 and DoDI 8520.03,
- NIST FIPS's, NIST SP 800-56, and NIST SP 800-57 processes/requirements for key generation, distribution, storage, access, and destruction (for unclassified systems); and/or
- CNSSI 1253F Attachment 5 (Classified Information Overlay) complaint processes/requirements for key generation, distribution, storage, access, and destruction (for classified systems).

SC-13 Use of Cryptography

Justification to Select: SC-13 is selected in the CNSSI 1253 baseline for all systems and in the Privacy Overlay for all Privacy Impact Levels, and for PHI. SC-13 is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The information system implements *all uses and types of cryptography required for each use, for example:*
- NSA-approved cryptography for the protection of classified information from access by personnel who lack the necessary security clearance
- Either FIPS validated or NSA approved cryptography for encryption of PII at rest and during transmission
- FIPS-validated cryptography for protection classified information during transmission and at rest from access by personnel who lack the necessary formal access approvals for CAP information
- FIPS-validated cryptography for the provision of digital signatures and hashing in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

SC-15 Collaborative Computing Devices

Justification to Select: SC-15 is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The information system:
a. Prohibits remote activation of collaborative computing devices with the following exceptions: *dedicated VTC suites located in approved VTC locations that are centrally managed, and as otherwise specifically authorized by the AO, and defined and clearly documents in the SSP*; and
b. Provides an explicit indication of use to users physically present at the devices.

SC-17 Public Key Infrastructure Certificates

Justification to Select: SC-17 is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization issues public key certificates under a *DNI or DoD certificate policy (compliant with CNSSP No. 25 and DoDI 8520.02), as appropriate* or obtains public key certificates from an approved service provider.

SC-18 Mobile Code

Justification to Select: SC-18 is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

SC-18(1) Mobile Code | Identify Unacceptable Code / Take Corrective Actions

Justification to Select: SC-18(1) is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The information system identifies *all unacceptable mobile code* and takes *corrective actions in accordance with the Web Browser Protection Profile, the Application Security and Development STIG, and as defined the SSP*.

SC-18(2) Mobile Code | Acquisition / Development / Use

Justification to Select: SC-18(2) is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization ensures that the acquisition, development, and use of mobile code to be deployed in the information system meets *DoDI 8500.01, to include the following requirements:*
(a) Emerging mobile code technologies that have not undergone a risk assessment and been assigned to a Risk Category by DISA are not used.
(b) Category 1 mobile code is signed with a code signing certificate; use of unsigned Category 1 mobile code is prohibited; use of Category 1 mobile code technologies that cannot block or disable unsigned mobile code (e.g., Windows Scripting Host) is prohibited.
(c) Category 2 mobile code which executes in a constrained environment without access to system resources (e.g., Windows registry, file system, system parameters, and network connections to other than the originating host) may be used.
(d) Category 2 mobile code that does not execute in a constrained environment may be used when obtained from a trusted source over an assured channel (e.g., SIPRNet, SSL connection, S/MIME, code is signed with an approved code signing certificate).
(e) Category 3 (mobile code having limited functionality, with no capability for unmediated access to the services and resources of a computing platform) mobile code may be used.

SC-18(3) Mobile Code | Prevent Downloading / Execution

Justification to Select: SC-18(3) is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The information system prevents the download and execution of *all unacceptable mobile code such as:*

(a) Emerging mobile code technologies that have not undergone a risk assessment and been assigned to a Risk Category by the DISA;
(b) Unsigned Category 1 mobile code and Category 1 mobile code technologies that cannot block or disable unsigned mobile code (e.g., Windows Scripting Host); or
(c) Category 2 mobile code not obtained from a trusted source over an assured channel (e.g., SIPRNet, SSL connection, S/MIME, code is signed with an approved code signing certificate).

SC-18(4) Mobile Code | Prevent Automatic Execution

Justification to Select: SC-18(4) is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The information system prevents the automatic execution of mobile code in *accordance with DoDI 8500.01, to include in software applications and such as, but not limited to, email, scriptable document/file editing applications that support documents with embedded code (e.g., MS Office applications/documents)* and enforces *prompting the user for permission* prior to executing the code.

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

Justification to Select: SC-20 is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

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

Justification to Select: SC-21 is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

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

Justification to Select: SC-22 is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

SC-23 Session Authenticity

Justification to Select: SC-23 is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

SC-23(1) Session Authenticity | Invalidate Session Identifiers at Logout

Justification to Select: SC-23(1) is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

SC-23(3) Session Authenticity | Unique Session Identifiers with Randomization

Justification to Select: SC-23(3) is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The information system generates a unique session identifier for each session with *NSA or NIST approved randomness methods or mechanisms as defined in the SSP* and recognizes only session identifiers that are system-generated.

SC-23(5) Session Authenticity | Allowed Certificate Authorities

Justification to Select: SC-23(5) is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The information system only allows the use of *certificate authorities established or authorized by DNI or DoD* for verification of the establishment of protected sessions.

SC-24 Fail in Known State

Justification to Select: SC-24 is selected in the CNSSI 1253 baseline for systems categorized High for Confidentiality or Integrity and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The information system fails to a *known secure state* for *all types of failures, including failures during system initialization, shutdown, and aborts,* preserving *information necessary to determine cause of failure and to return to operations with least disruption to mission/business processes* in failure.

SC-28 Protection of Information at Rest

Justification to Select: SC-28 is selected in the CNSSI 1253 baseline for all systems and in the Privacy Overlay for all Privacy Impact Levels and for PHI. SC-28 is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The information system protects the *confidentiality and integrity* of *all information at rest not cleared for public release to include, at a minimum, classified and personally identifiable information (PII).*

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

Justification to Select: SC-28(1) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system does not implement cryptographic mechanisms to prevent unauthorized disclosure and modification of information on specified information system components, then an insider threat could gain unauthorized access to sensitive information.

Encryption of removable media (data at rest) provides an additional layer of security to avoid unauthorized access to sensitive data if the USB should become misplaced or stolen.

Parameter Value(s): The information system implements cryptographic mechanisms to prevent unauthorized disclosure and modification of *all information at rest not cleared for public release*

to include, at a minimum, classified and personally identifiable information (PII) on *system components outside of organization facilities*.

Regulatory/Statutory Reference(s): CNSSD 504, Section A.2.c.vi.1.

SC-38 Operations Security

Justification to Select: SC-38 is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system or the organization does not employ operations security safeguards against insider threats while protecting key organizational information throughout the system development life cycle, then an insider threat could gain access to the sensitive information and misuse it to compromise the system.

Parameter Value(s): The organization employs *operations security (OPSEC) safeguards* to protect key organizational information throughout the system development life cycle.

SC-39 Process Isolation

Justification to Select: SC-39 is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

SC-42 Sensor Capability and Data

Justification to Select: Although SC-42 is not selected in NIST SP 800-53 , it is selected in the Classified Information overlay. Prohibiting the remote activation of devices with sensor capabilities in all areas where classified information is stored, processed, transmitted or discussed is considered a requirement for safeguarding classified information.

Supplemental Guidance: If a system does not prohibit the remote activation of environmental sensing capabilities and provide an explicit indication of sensor use to specified users, then an insider threat could covertly activate the sensing capabilities and thereby gain unauthorized access to sensitive information.

This control often applies to types of information systems or system components characterized as mobile devices, for example, smart phones, tablets, and some wearable personal or fitness devices. These systems often include sensors that can collect and record data regarding the environment where the system is in use. Sensors that are embedded within mobile or personal devices include, for example, cameras and microphones. While the sensors on mobiles devices provide an important function, if activated covertly, such devices can potentially provide a means for an insider threat to record or capture sensitive or classified information for exfiltration. There should be no exceptions allowing remote activation of sensors where classified information is stored, processed, transmitted, or discussed.

Parameter Value(s): The information system:

a. Prohibits the remote activation of environmental sensing capabilities with the following exceptions: *no exceptions in areas where classified information is stored, processed, transmitted, or discussed*; and
b. Provides an explicit indication of sensor use to *all users*.

SC-42(3) Sensor Capability and Data | Prohibit Use of Devices

Justification to Select: Although SC-42(3) is not selected in NIST SP 800-53 , it is selected in the Classified Information overlay. Prohibiting the use of devices with sensor capabilities in all areas where classified information is stored, processed, transmitted or discussed is considered a best practice for safeguarding classified information.

Supplemental Guidance: If the organization does not prohibit the use of specified devices possessing environmental sensing capabilities in pre-identified facilities, areas, or systems, then an insider threat could activate the sensing capabilities and thereby gain unauthorized access to sensitive information.

The organization may define exceptions to allow the use of specified devices with sensor capabilities (such as digital cameras and two way radios) provided that the sensor capabilities are designed, configured, and operated securely.

Organizations may designate some areas acceptable for temporary storage, processing, transmission, or discussion of classified information; however, during the periods when classified information is not being stored, processed, transmitted or discussed, the organization may allow the use of devices with sensor capabilities in those areas.

Parameter Value(s): The organization prohibits the use of devices possessing *sensors capable of recording audio or imagery (still or video) or transmitting information (i.e., cell phones, two way radios)* in *all areas where classified information is stored, processed, transmitted or discussed, except for 1) specific devices in specific areas where the risk of use has been appropriately mitigated and for which the organization has defined and allowed an exception; or for 2) other cases that are clearly defined in approved policy*.

SI-1 System and Information Integrity Policy and Procedures

Justification to Select: SI-1is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization:
a. Develops, documents, and disseminates to *all personnel (including end users, maintenance personnel, administrators, etc.)*:
1. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and
b. Reviews and updates the current:

1. System and information integrity policy *at least annually*; and
2. System and information integrity procedures *at least annually*.

SI-2 Flaw Remediation

Justification to Select: SI-2 is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization:
a. Identifies, reports, and corrects information system flaws;
b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
c. Installs security-relevant software and firmware updates within *the time period directed by any authoritative source (e.g., IAVM, ICVM, CTOs, DTMs, STIGs), nominally within 21 days (for DoD IT systems on NIPRNet or SIPRNet) or within 90 days (for IC IT Systems on a TS Network)* of the release of the updates *or the associated authoritative issuance*; and
d. Incorporates flaw remediation into the organizational configuration management process.

SI-2(2) Flaw Remediation | Automated Flaw Remediation Status

Justification to Select: SI-2(2) is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization employs automated mechanisms:
- *Continuously with HBSS;*
- *At least every 30 days for any additional internal network scans not covered by HBSS; and*
- *Annually for external scans (e.g., by a Cybersecurity Service Provider (CSSP)),*
to determine the state of information system components with regard to flaw remediation.

SI-2(6) Flaw Remediation | Removal of Previous Versions of Software / Firmware

Justification to Select: SI-2(6) is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

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

SI-3 Malicious Code Protection

Justification to Select: SI-3 is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Control Extension: The information system automatically scans all removable media for malicious code when it is connected to the information system.

Supplemental Guidance: If a system does not properly implement, update, configure, and tune malicious code protections, then an insider threat could use malicious code to compromise the system and gain unauthorized access to sensitive information.

Malicious code protection will also protect against users from inadvertently loading malware onto the information system.

Parameter Value(s): The organization:
a. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;
b. Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures;
c. Configures malicious code protection mechanisms to:
1. Perform periodic scans of the information system *at least every 7 days (weekly)*and real-time scans of files from external sources at *endpoints and network entry/exit points* as the files are downloaded, opened, or executed in accordance with organizational security policy; and
2. *Block and quarantine malicious code and then send an alert to, at a minimum, the system administrator (immediately or in near real time)* in response to malicious code detection; and
d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

Regulatory/Statutory Reference(s): CNSSD 504, Section A.2.c.iv.

SI-3(2) Malicious Code Protection | Automatic Updates

Justification to Select: SI-3(2) is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

SI-4 Information System Monitoring

Justification to Select: SI-4 is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system or the organization does not properly implement information system monitoring (per SI-4), then insider threat activity might not be detected.

Information System Monitoring on both the device and network level is typically implemented using monitoring solutions that are standardized across the enterprise. Information system monitoring is critical to detecting insider threat activities.

Parameter Value(s): The organization:
a. Monitors the information system to detect:
1. Attacks and indicators of potential attacks in accordance with *sensor placement and monitoring requirements within CJCSI 6510.01F and host based intrusion detection/prevention requirements within ICS 502-02*; and
2. Unauthorized local, network, and remote connections;

b. Identifies unauthorized use of the information system through *a variety of tools, techniques, and methods (e.g., intrusion detection/prevention systems, malicious code protection software, scanning tools, and network monitoring software)*;
c. Deploys monitoring devices:
1. Strategically within the information system to collect organization-determined essential information; and
2. At ad hoc locations within the system to track specific types of transactions of interest to the organization;
d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;
e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information;
f. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and
g. Provides *information system monitoring information to cyber incident response, counter-intelligence, and security personnel, as needed for official investigative purposes.*

SI-4(1) Information System Monitoring | System-Wide Intrusion Detection System

Justification to Select: SI-4(1) is selected in the CNSSI 1253 baseline for all systems.

Supplemental Guidance: If the organization does not connect and configure individual intrusion detection tools into an information system-wide intrusion detection system, then related, but distributed, insider threat activities might not be correlated and properly assessed.

System-wide intrusion monitoring is typically implemented at the enterprise level. System-wide intrusion monitoring enables correlation across multiple sensors to detect insider threat activity.

SI-4(2) Information System Monitoring | Automated Tools for Real-Time Analysis

Justification to Select: SI-4(2) is selected in the CNSSI 1253 baseline for systems categorized Moderate or High for Confidentiality, Integrity, or Availability and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system or the organization does not employ automated tools to support near real-time analysis of events, then insider threat activity might not be promptly analyzed and responded to.

Real-time analysis of information system monitoring data is typically performed using automated tools implemented at the enterprise level. The use of automated tools for real-time analysis enhances the detection of insider threat activities.

Regulatory/Statutory Reference(s): EO 13587, Section 2.1(b) and Section 5.2 (a); White House Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch

Insider Threat Programs, Tab 1, Section B.2(1), Tab 2, Section H; and ICS 502-01, Section E.1.d.(5).

SI-4(4) Information System Monitoring | Inbound and Outbound Communications Traffic

Justification to Select: SI-4(4) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system or the organization does not regularly monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions, then insider threat communications and related activities might not be detected.

Monitoring of inbound and outbound communications is typically implemented at the enterprise level. Monitoring of inbound and outbound communications is critical to detect insider threat activity.

Parameter Value(s): The information system monitors inbound and outbound communications traffic *continuously* for unusual or unauthorized activities or conditions.

SI-4(5) Information System Monitoring | System-Generated Alerts

Justification to Select: SI-4(5) is selected in the CNSSI 1253 baseline for all systems.

Supplemental Guidance: If the organization does not alert designated personnel when the indications of compromise or potential compromise by insider threats are detected, then those personnel would not be able to take prompt action to assess and mitigate the insider threat activity.

Parameter Value(s): The information system alerts *at a minimum, the system security administrator, ISSM, and ISSO* when the following indications of compromise or potential compromise occur: *any compromise indicators, to include: actual real time intrusion, when there are threats identified by authoritative sources (e.g., CTOs), and other events consistent with incident categories I, II, IV, and VII defined within CJCSM 6510.1B.*

SI-4(10) Information System Monitoring | Visibility of Encrypted Communications

Justification to Select: SI-4(10) is selected in the CNSSI 1253 baseline for systems categorized Moderate or High for Confidentiality, Integrity, or Availability.

Supplemental Guidance: If the organization does not make provisions so that encrypted communications traffic is visible to monitoring tools, then insider threat communications or activities, obfuscated by encryption, would not be detected by the monitoring tools.

The ability to monitor and inspect all encrypted communications at the network boundary (e.g., gateway) is critical to detecting insider threat download and upload activities.

Parameter Value(s): The organization makes provisions so that *all encrypted network traffic (except traffic that has been specifically waived by the CISO in writing in advance)* is visible to *the enterprise gateway and network security monitoring tools*.

SI-4(11) Information System Monitoring | Analyze Communications Traffic Anomalies

Justification to Select: SI-4(11) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If the organization does not analyze outbound communications traffic at the external boundary of the information system, and selected interior points to discover anomalies, then insider threat related communications would not be detected.

Parameter Value(s): The organization analyzes outbound communications traffic at the external boundary of the information system and selected *interior points within the system (e.g., subnetworks, subsystems)* to discover anomalies.

SI-4(12) Information System Monitoring | Automated Alerts

Justification to Select: SI-4(12) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If the organization does not employ automated mechanisms to alert security personnel of inappropriate or unusual insider threat activities, then those individuals would not be able to take prompt action to assess and mitigate the insider threat activity.

Automated alerting of incident response personnel for inappropriate or unusual activities enables them to take prompt action in response to insider threat activities.

Parameter Value(s): The organization employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications: *when there are threats identified by authoritative sources (e.g., CTOs) and in accordance with CJCSM 6510.01B.*

SI-4(14) Information System Monitoring | Wireless Intrusion Detection

Justification to Select: SI-4(14) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If the organization does not employ a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system, then an insider threat might misuse a wireless device to conduct malicious activities without detection.

Wireless and wired intrusion detection systems shall be used to monitor for unauthorized access to the network and to detect malicious wireless activities including those initiated by an insider threat.

Regulatory/Statutory Reference(s): CNSSP 17 Section 6.d.4

SI-4(15) Information System Monitoring | Wireless to Wireline Communications

Justification to Select: SI-4(15) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If the organization does not employ an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wireline networks, then an insider threat might misuse a wireless device to conduct malicious activities without detection.

Wireless and wired intrusion detection systems shall be used to monitor for unauthorized access to the network and to detect malicious wireless activities including those initiated by an insider threat.

Regulatory/Statutory Reference(s): CNSSP 17 Section 6.d.4

SI-4(16) Information System Monitoring | Correlate Monitoring Information

Justification to Select: SI-4(16) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If the organization does not correlate information from monitoring tools employed throughout the information system, then related, but distributed, insider threat activities would not be properly assessed.

SI-4(19) Information System Monitoring | Individuals Posing Greater Risk

Justification to Select: SI-4(19) is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization implements *additional monitoring* of individuals who have been identified by *trusted and reliable sources (e.g., human resource records, intelligence agencies, law enforcement organizations and/or other credible sources)* as posing an increased level of risk.

SI-4(20) Information System Monitoring | Privileged User

Justification to Select: SI-4(20) is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: Organizations should develop and implement risk-based control measures, such as a two-person rule, workflow review processes, or automated means for Tier 3 Privileged Users consistent with mission need and organizational risk management practices. These measures shall limit, to the extent practicable, unilateral actions by individuals with the highest accesses and privileges, and minimize unobserved or uncontrolled access to the most sensitive information or resources. The goal is to prevent the use of incorrect or unauthorized procedures with respect to the network tasks being performed or the information being accessed by Privileged Users. Such controls shall be incorporated using a risk management approach.

Parameter Value(s): The organization implements *additional monitoring* of privileged users.

Regulatory/Statutory Reference(s): NDAA for Fiscal Year 2017, Subtitle F, Section 951, paragraph (a)(4); and Office of the Secretary of Defense Insider Threat Mitigation, 12 July 2013.

SI-4(22) Information System Monitoring | Unauthorized Network Services

Justification to Select: SI-4(22) is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The information system detects network services that have not been authorized or approved by *at a minimum, ISSM or ISSO* and *alerts the ISSM or ISSO*.

SI-4(23) Information System Monitoring | Host-Based Devices

Justification to Select: SI-4(23) is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system or the organization does not implement host-based monitoring mechanisms on information system components, then insider threat activity at the host level would not be promptly detected.

Parameter Value(s): The organization implements *a host-based security solution* at *all components*.

SI-5 Security Alerts, Advisories, and Directives

Justification to Select: SI-5 is selected in the CNSSI 1253 baseline for all systems and in the Privacy Overlay for PHI. SI-5 is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization:
a. Receives information system security alerts, advisories, and directives from *USCYBERCOM and the US-CERT* on an ongoing basis;
b. Generates internal security alerts, advisories, and directives as deemed necessary;
c. Disseminates security alerts, advisories, and directives to: *ISSMs, ISSOs, System Security Administrators and System Administrators*; and
d. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.

SI-6 Security Functionality Verification

Justification to Select: SI-6 is selected in the CNSSI 1253 baseline for systems categorized High for Integrity and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The information system:
a. Verifies the correct operation of *all security functions*;

b. Performs this verification *upon system startup and/or system restart, upon command by a privileged user, and at least every 30 days*;
c. Notifies *the ISSO, ISSM and system/security administrator* of failed security verification tests; and
d. *Notifies the system/security administrator* when anomalies are discovered.

SI-6(3) Security Function Verification | Report Verification Results

Justification to Select: SI-6(3) is selected in the CNSSI 1253 baseline for systems categorized High for Integrity and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization reports the results of security function verification to *the responsible security personnel, at a minimum, the ISSO and the ISSM*.

SI-7 Software and Information Integrity

Justification to Select: SI-7 is selected in the CNSSI 1253 baseline for systems categorized Moderate or High for Integrity and in the Privacy Overlay for all Privacy Impact Levels. SI-7 is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization employs integrity verification tools to detect unauthorized changes to *all security-relevant software, firmware, and information as documented in the SSP*.

SI-7(1) Software, Firmware, and Information Integrity | Integrity Checks

Justification to Select: SI-7(1) is selected in the CNSSI 1253 baseline for systems categorized Moderate or High for Integrity and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The information system performs an integrity check of *security-relevant software, firmware, and information at startup and at least every 180 days (every 30 days for CDS)*.

SI-7(2) Software, Firmware, and Information Integrity | Automated Notifications of Integrity Violations

Justification to Select: SI-7(2) is selected in the CNSSI 1253 baseline for systems categorized High for Integrity and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization employs automated tools that provide notification to *system security administrator, system administrator and the ISSO* upon discovering discrepancies during integrity verification.

SI-7(5) Software, Firmware, and Information Integrity | Automated Response to Integrity Violations

Justification to Select: SI-7(5) is selected in the CNSSI 1253 baseline for systems categorized High for Integrity and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The information system automatically *shuts the information system down or restarts the information system* when integrity violations are discovered.

SI-7(6) Software, Firmware, and Information Integrity | Cryptographic Protection

Justification to Select: SI-7(6) is selected in the Privacy Overlay for all Privacy Impact Levels and is therefore applicable to systems or activities that directly support the Insider Threat Program.

SI-7(7) Software, Firmware, and Information Integrity | Integration of Detection and Response

Justification to Select: SI-7(7) is selected in the CNSSI 1253 baseline for systems categorized Moderate or High for Integrity and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization incorporates the detection of unauthorized *security-relevant changes to the information system* into the organizational incident response capability.

SI-7(8) Software, Firmware, and Information Integrity | Auditing Capability for Significant Events

Justification to Select: SI-7(8) is selected in the CNSSI 1253 baseline for systems categorized Moderate or High for Integrity including systems or activities that directly support the Insider Threat Program. Although this control is not selected in the baseline for Low impact systems, it is typically implemented by organizations for all information systems.

Supplemental Guidance: If a system does not, upon detection of a potential integrity violation, provide the capability to audit the event and initiate predefined response actions, then insider threat activity would not be promptly responded to and mitigated.

Monitoring for, auditing, and alerting on, software, firmware, and information integrity violations enable security personnel to promptly assess and react to and mitigate insider threat activities.

Parameter Value(s): The information system, upon detection of a potential integrity violation, provides the capability to audit the event and initiates the following actions: *generates an audit record and alerts, at a minimum, the system security administrator, ISSO, and Security Control Assessor (SCA).*

SI-7(14) Software, Firmware, and Information Integrity | Binary or Machine Executable Code

Justification to Select: SI-7(14) is selected in the CNSSI 1253 baseline for all systems and is therefore applicable to systems or activities that directly support the Insider Threat Program.

SI-10 Information Input Validation

Justification to Select: SI-10 is selected in the CNSSI 1253 baseline for all systems and in the Privacy Overlay for Privacy Impact Levels of Moderate or High. SI-10 is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The information system checks the validity of *all inputs to web/application servers, database servers, and any system or application input that might receive a crafted exploit targeted at some weakness in the system's code, such as a buffer overflow or other flaw*.

SI-10(3) Information Input Validation | Predictable Behavior

Justification to Select: SI-10(3) is selected in the CNSSI 1253 baseline for systems categorized Moderate or High for Integrity and is therefore applicable to systems or activities that directly support the Insider Threat Program.

SI-11 Error Handling

Justification to Select: SI-11 is selected in the CNSSI 1253 baseline for all systems and in the Privacy Overlay for all Privacy Impact Levels, and for PHI. SI-11 is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The information system:
a. Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and
b. Reveals error messages only to *the ISSO, ISSM, SCA, or other specifically designated and authorized individuals with a need for the information in the performance of their duties*.

SI-12 Information Handling and Retention

Justification to Select: SI-12 is selected in the CNSSI 1253 baseline for all systems and in the Privacy Overlay for all Privacy Impact Levels, and for PHI. SI-12 is therefore applicable to systems or activities that directly support the Insider Threat Program.

SI-16 Memory Protection

Justification to Select: SI-16 is selected in the CNSSI 1253 baseline for systems categorized Moderate or High for Integrity and is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The information system implements *hardware-enforced or software-enforced security safeguards (e.g., data execution prevention and address space layout randomization)* to protect its memory from unauthorized code execution.

PM-11 Mission/Business Process Definition

Justification to Select: PM-11 is selected in the CNSSI 1253 baseline for all systems and in the Privacy Overlay for all Privacy Impact Levels, and for PHI. PM-11 is therefore applicable to systems or activities that directly support the Insider Threat Program.

PM-12 Insider Threat Program

Justification to Select: PM-12 is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Control Extension(s) and Parameter Value(s):

The organization:

a. Develops, documents, and disseminates to *all personnel*:

1. An insider threat policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organization entities, and compliance; and

2. Procedures to facilitate the implementation of the insider threat policy and associated controls; and

b. Reviews and updates the current:

1. insider threat policy *annually*; and

2. insider threat procedures *annually*.

The organization develops and maintains an implementation plan for the Insider Threat Program, submits the plan to the agency head, and annually prepares a report regarding progress and/or status within that agency.

The organization designates a senior official(s) with authority to provide management, accountability, and oversight of the organization's Insider Threat Program, to coordinate, develop, implement, and maintain an organization-wide Insider Threat Program, and to make resource recommendations to the appropriate agency official.

The organization establishes oversight mechanisms or procedures to ensure proper handling and use of records and data, and ensure that access to such records and data is restricted to insider threat personnel who require the information to perform their authorized functions.

The organization conducts an effectiveness review of the Insider Threat Program *at least annually, which involves* performing a self-assessments of compliance with insider threat policies and standards, the results of which is reported to *the Senior Information Sharing and Safeguarding Steering Committee*.

The organization coordinates with *general counsel and civil liberties or privacy officers* during planning, implementation and management of the Insider Threat Program to ensure that legal and privacy issues are appropriately addressed.

The organization involves *the Chief Information Officer (CIO), Senior Information Security Officer (SISO/CISO), Cybersecurity and Information Assurance program, Counterintelligence (where available), Anti-Terrorism/Force Protection (where available), Physical Security, human resources components (including personnel security)* in the Insider Threat Program.

The Organization verifies Insider Threat Program implementation and policy conformance by contractors and other non-DoD entities that have authorized access to NSS resources as required by contract or agreement.

Supplemental Guidance: If the organization does not implement an Insider Threat Program that includes a cross-discipline insider threat incident handling team, then insider threat activities would not be promptly and properly detected, assessed, responded to, and mitigated.

Organizations should designate a senior official or officials, who shall be principally responsible for establishing a process to gather, integrate, and centrally analyze, and respond to Counterintelligence (CI), Security, Information Assurance (IA), Human Resource (HR), Law Enforcement (LE), and other relevant information indicative of a potential insider threat. Senior Officials(s) shall ensure:

(1) The establishment of guidelines and procedures for the retention of records and documents necessary to complete assessments required by Executive Order 13587.
(2) The timely resolution of each insider threat matter

The organizations should promulgate guidance, if needed, to reflect unique mission requirements, but not inhibit meeting the minimum standards issued by the Insider Threat Task force (ITTF). Organizational policy should include internal guidelines and procedures for the implementation of community insider threat standards and policies, and be approved by the agency head. Organizations should develop policies, guidelines and procedures for documenting each insider threat matter reported and for properly protecting, interpreting, storing, and limiting access to user activity monitoring methods and results to authorized personnel.

Organizations should establish and promote an internal network site, accessible to all cleared employees, to provide insider threat reference material, including indicators of insider threat behavior, applicable reporting requirements and procedures, and provide a secure electronic means of reporting matters to the Insider Threat Program.

Organizations should establish or maintain a multi-disciplinary threat management capability to conduct and integrate the monitoring, analysis, reporting, and response to insider threats and establish procedures for a multi-disciplinary threat management capability that complies with the Privacy Act and HIPAA.

Organizations should implement measures to protect sensitive information that may be utilized for insider threat purposes including establishing oversight mechanisms or procedures to ensure proper handling and use of the data. Organizations should ensure the agency's Insider Threat Program is developed and implemented in consultation with that agency's Office of General Counsel and civil liberties and privacy officials so that all Insider Threat Program activities, to include training, are conducted in accordance with applicable laws, whistleblower, protections, and civil liberties and privacy policies.

The organization’s Insider Threat Program should facilitate timely, informed decision-making by ensuring the following subject matter expertise and multi-disciplinary capabilities are readily available to all commanders (or civilian equivalents):

(1) Law Enforcement
(2) Counterintelligence
(3) Mental Health
(4) Security
(5) Civilian and Military Personnel Management
(6) Legal Counsel
(7) Cybersecurity
(8) Civil Liberties/Privacy Officials

Organizations should establish insider threat management forums to monitor implementation.

An Insider Threat Program should include considerations for the Information and Communications Technology (ICT) supply chain infrastructure.

Data obtained by the Insider Threat Program shall be maintained to the extent consistent with applicable law and policy and in accordance with applicable records control schedules.

At a minimum, the annual reports shall document annual accomplishments, resources allocated, insider threat risks to the agency, recommendations and goals for program improvement, and major impediments or challenges.

Regulatory/Statutory Reference(s): White House Memo - National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, Sections B.4, B.5, B.6, B.7, B.8, D.1, D.2, D.3, D.4, D.5, D.6, D.7, E.3, H.2, and I.3; NIST SP 800-161; CNSSD 504, 6.c, 6.d, 6.e, and B.2; and DoD Directive 5205.16

PM-15 Contacts with Security Groups and Associations

Justification to Select: PM-15 is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If the organization does not establish and institutionalize contact with selected groups and associations within the insider threat security community, then they would not be able to: maintain and regularly update their insider threat training with the most current information; maintain currency with security practices, techniques, and technologies; and share insider threat lessons learned.

Organizations shall ensure Insider Threat Programs have timely access, as otherwise permitted, to available United States Government intelligence and counterintelligence reporting information and analytic products pertaining to adversarial threats.

If the organization does not establish and institutionalize contact with external groups and associations within the Insider Threat community, then the organization will not be able to educate and train its personnel on the latest Insider Threat prevention, detection and mitigation techniques.

Regulatory/Statutory Reference(s): NIST SP 800-53and White House Memo - National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, Section G.4.

PM-16 Threat Awareness Program

Justification to Select: PM-16 is selected in the CNSSI 1253 baseline for all systems, including systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If the organization does not include a cross-organization information sharing capability for insider threats in its threat awareness program, then the organization will not be aware of new threats and new or evolving threat abilities and methods and will not be able to protect against them.

Organizations shall provide a representative to departmental and interagency forums engaged in countering insider threats.

Regulatory/Statutory Reference(s): DoD Directive 5205.16.

PRIVACY CONTROLS

AP-1 Authority to Collect

Justification to Select: AP-1 is selected in the Privacy Overlay for all Privacy Impact Levels and is therefore applicable to systems or activities that directly support the Insider Threat Program.

AP-2 Purpose Specification

Justification to Select: AP-2 is selected in the Privacy Overlay for all Privacy Impact Levels and is therefore applicable to systems or activities that directly support the Insider Threat Program.

AR-2 Privacy Impact and Risk Assessment

Justification to Select: AR-2 is selected in the Privacy Overlay for all Privacy Impact Levels, and for PHI. AR-2 is therefore applicable to systems or activities that directly support the Insider Threat Program.

AR-3 Privacy Requirements for Contractors and Service Providers

Justification to Select: AR-3 is selected in the Privacy Overlay for all Privacy Impact Levels, and for PHI. AR-3 is therefore applicable to systems or activities that directly support the Insider Threat Program.

AR-5 Privacy Awareness and Training

Justification to Select: AR-5 is selected in the Privacy Overlay for all Privacy Impact Levels, and for PHI. AR-5 is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization:

a. Develops, implements, and updates a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures;

b. Administers basic privacy training *upon and individual reporting, and then at least annually thereafter* and targeted, role-based privacy training for personnel having responsibility for personally identifiable information (PII) or for activities that involve PII *upon increase in responsibility or change of duties, and then at least annually thereafter*; and

c. Ensures that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements *at least annually*.

AR-7 Privacy-Enhanced System Design and Development

Justification to Select: AR-7 is selected in the Privacy Overlay for all Privacy Impact Levels, and for PHI. AR-7 is therefore applicable to systems or activities that directly support the Insider Threat Program.

AR-8 Accounting of Disclosures

Justification to Select: AR-8 is selected in the Privacy Overlay for all Privacy Impact Levels, and for PHI. AR-8 is therefore applicable to systems or activities that directly support the Insider Threat Program.

DM-1(1) Minimization of Personally Identifiable Information | Locate / Remove / Redact / Anonymize PII

Justification to Select: Although DM-1(1) is not selected in the CNSSI 1253 baseline or an overlay, DM-1(1) is commonly implemented when PII is collected as part of insider threat monitoring by removing, redacting, or anonymizing the PII to minimize the potential for unauthorized PII disclosure or spillage.

DM-2 Data Retention and Disposal

Justification to Select: DM-2 is selected in the Privacy Overlay for all Privacy Impact Levels, and for PHI. DM-2 is therefore applicable to systems or activities that directly support the Insider Threat Program.

Parameter Value(s): The organization:
a. Retains each collection of personally identifiable information (PII) for *the time period specified by the NARA-approved Records Schedule and the Privacy Act System of Records Notice.* to fulfill the purpose(s) identified in the notice or as required by law;
b. Disposes of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and
c. Uses *techniques or methods in accordance with DoD 5400.11-R* to ensure secure deletion or destruction of PII (including originals, copies, and archived records).

DM-3 Minimization of PII Used in Testing, Training, and Research

Justification to Select: DM-3 is selected in the Privacy Overlay for all Privacy Impact Levels, and for PHI. DM-3 is therefore applicable to systems or activities that directly support the Insider Threat Program.

DM-3(1) Minimization of PII Used in Testing, Training, and Research | Risk Minimization Techniques

Justification to Select: DM-3(1) is selected in the Privacy Overlay for PHI and is therefore applicable to systems or activities that directly support the Insider Threat Program.

IP-1 Consent

Justification to Select: IP-1 is selected in the Privacy Overlay for all Privacy Impact Levels, and for PHI. IP-1 is therefore applicable to systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: User consent is obtained through the implementation of user agreements and consent banners. See also Security Control AC-8.

Regulatory/Statutory Reference(s): CNSSI 1015; and White House Memo - National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, Section H.4.

IP-2 Individual Access

Justification to Select: IP-2 is selected in the Privacy Overlay for all Privacy Impact Levels, and for PHI. IP-2 is therefore applicable to systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: See the Department of Defense (DoD) Insider Threat Management and Analysis Center (DITMAC) System of Records Notice (SORN) for details regarding how individuals can access information about themselves in the DITMAC or component's system of record. However, the DITMAC SORN also exempts Component's from complying with subsection (d) of the Privacy Act that addresses access to records.

Regulatory/Statutory Reference(s): Department of Defense (DoD) Insider Threat Management and Analysis Center (DITMAC) System of Records Notice (SORN); DoD Regulation 5400.11; and 32 CFR 310.

IP-3 Redress

Justification to Not Select: Although IP-3 is selected in the Privacy Overlay for all Privacy Impact Levels, and for PHI, IP-3 is not applicable to systems or activities that directly support the Insider Threat Program. The DITMAC SORN exempts Component's from complying with subsection (d) of the Privacy Act that addresses requesting and making amendments to the Insider Threat records.

Regulatory/Statutory Reference(s): DITMAC SORN.

IP-4 Complaint Management

Justification to Select: IP-4 is selected in the Privacy Overlay for all Privacy Impact Levels, and for PHI. IP-4 is therefore applicable to systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: The DoD rules for accessing records and for contesting or appealing agency determinations are published in DoD Regulation 5400.11 and 32 CFR 310.

Regulatory/Statutory Reference(s): DITMAC SORN; DoD Regulation 5400.11; and 32 CFR 310.

SE-2 Privacy Incident Response

Justification to Select: SE-2 is selected in the Privacy Overlay for all Privacy Impact Levels, and for PHI. SE-2 is therefore applicable to systems or activities that directly support the Insider Threat Program.

Supplemental Guidance: If a system or the organization does not develop and implement a Privacy Incident Response Plan, then the organization would not be able to provide an organized and effective response to privacy incidents, including those related to insider threat activities.

CNSSI 1015 directs organizations to ensure that notice of any unauthorized access, use or sharing of audit data containing personally identifiable information is handled consistent with applicable data breach notification policies. An organization's Privacy Incident Response Plan is typically developed at the enterprise level.

Regulatory/Statutory Reference(s): CNSSI 1015

UL-1 Internal Use

Justification to Select: UL-1 is selected in the Privacy Overlay for all Privacy Impact Levels, and for PHI. UL-1 is therefore applicable to systems or activities that directly support the Insider Threat Program.

UL-2 Information Sharing with Third Parties

Justification to Select: UL-2 is selected in the Privacy Overlay for all Privacy Impact Levels, and for PHI. UL-2 is therefore applicable to systems or activities that directly support the Insider Threat Program.

6. Tailoring Considerations

Organizations should consider the following insider threat specific control guidance when tailoring information systems in addition to using the general tailoring guidance in CNSSI 1253.

[TBD]

7. Definitions

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

8. Acronyms

AO	Authorizing Official
APT	Advanced Persistent Threat
BC/DR	Business Continuity/Disaster Recovery
BOE	Body of Evidence
CAC	Common Access Card
CAP	Controlled Access Program
CCB	Configuration Control Board
CCEVS	Common Criteria Evaluation and Validation Scheme
CCI	Control Correlation Identifier
CD	Compact Disk
CDR	Critical Design Review
CDRW	Compact Disk Read Write
CDS	Cross Domain Solution
CFR	Code of Federal Regulations
CI	Counterintelligence
CIAR	Counterintelligence Awareness and Reporting
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJCSM	Chairman of the Joint Chiefs of Staff Manual
CMP	Configuration Management Plan
CND	Computer Network Defense
CNSS	Committee on National Security Systems
CNSSD	Committee on National Security Systems Directive
CNSSI	Committee on National Security Systems Instruction

CNSSP	Committee on National Security Systems Policy
CODEC	Coder Decoder
CONOPS	Concept of Operations
COOP	Continuity of Operations Plan
CPU	Computer Processing Unit
CSfC	Commercial Solutions for Classified
CSS	Central Security Service
CSSP	Cybersecurity Service Provider
CTO	Communications Tasking Order
CUI	Controlled Unclassified Information
D/A	Department/Agency
DAO	Designated Authorizing Official
DISA	Defense Information Systems Agency
DITMAC	DoD Insider Threat Management and Analysis Center
DLSP	Data Loss and Spillage Prevention
DMZ	Demilitarized Zone
DNI	Director of National Intelligence
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DSPAV	DoD Specific Assignment Value
DTM	Directive-Type Memorandum
DTO	Data Transfer Officer
DVD-ROM	Digital Video Disk Read-Only Memory
EAM	Enterprise Asset Management
EO	Executive Order
EOD	Entry on Duty
ESC	Enterprise Service Center

FIPS	Federal Information Processing Standards
FY	Fiscal Year
GMT	Greenwich Mean Time
HBSS	Host Based Security System
HIPAA	Health Insurance Portability and Accountability Act
HIPS	Host-based Intrusion Prevention System
HR	Human Resource
IA	Information Assurance
IAM	Information Assurance Manager
IAO	Information Assurance Officer
IAP	Internet Access Point
IAPC	Information Assurance Protection Center
IAVA	Information Assurance Vulnerability Alert
IAVM	Information Assurance Vulnerability Management
IC	Intelligence Community
ICD	Intelligence Community Directive
IC-IRC	Intelligence Community-Incident Response Center
ICS	Intelligence Community Standard
ICSA	ICSA Lab is a division of MCI Communications Services, Inc. dba Verizon Business Services
ICT	Information and Communications Technology
ICVM	Intelligence Community Vulnerability Management
IP	Internet Protocol
ISSE	Information System Security Engineer
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IT	Information Technology
ITTF	Insider Threat Task Force

JWICS	Joint Worldwide Intelligence Communications System
LE	Law Enforcement
MIME	Multipurpose Internet Mail Extension
NCSC	National Counterintelligence and Security Center
NIAP	National Information Assurance Partnership
NIPRNet	Non-Secure Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NITTF	National Insider Threat Task Force
NOC	Network Operations Center
NSA	National Security Agency
NSS	National Security Systems
OCA	Original Classification Authority
ODNI	Office of the Director of National Intelligence
ONCIX	Office of the National Counterintelligence Executive
OPSEC	Operations Security
PDS	Protected Distribution System
PHI	Protected Health Information
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
RBAC	Role Based Access Control
S/MIME	Secure/Multipurpose Internet Mail Extension
SABI	Secret and Below Interoperability
SANS	SysAdmin, Audit, Network, and Security
SAP	Special Access Program
SCA	Security Control Assessor
SCAP	Security Content Automation Protocol
SCG	Security Configuration Guide

SCI	Sensitive Compartmented Information
SCRM	Supply Chain Risk Management
SDLC	System Development Lifecycle
SFUG	Security Features User Guide
SIPRNet	Secret Internet Protocol Router Network
SISO	Senior Information Security Officer
SLA	Service Level Agreement
SOC	Security Operations Center
SORN	System of Records Notice
SP	Special Publication
SRG	Security Requirements Guide
SSL	Secure Socket Layer
SSP	System Security Plan
STIG	Security Technical Implementation Guide
TO	Task Order
TSABI	Top Secret and Below Interoperability
UAM	User Activity Monitoring
UBE	User Based Enforcement
UCDMO	Unified Cross Domain Management Office
USB	Universal Serial Bus
USCYBERCOM	U.S. Cyber Command
USSTRATCOM	U.S. Strategic Command
UTC	Coordinated Universal Time
VTC	Video Teleconference
WAN	Wide Area network
XCCDF	Extensible Configuration Checklist Description Format
XML	Extensible Markup Language