Classified Information Overlay

1. Identification

This overlay identifies security control specifications needed to safeguard classified information stored, processed, or transmitted by national security systems (NSS).

The following documents were used to create this overlay:

- Executive Order (EO) 13526, *Classified National Security Information*, January 2010.
- EO 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, October 2011.
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013.[1]
- Committee on National Security Systems (CNSS) Instruction (CNSSI) No. 1253, *Security Categorization and Control Selection for National Security Systems*, March 2014.
- CNSSI No. 1253 Appendix F Attachment 1, *Security Control Overlays Template*, August 2013.
- CNSSI No. 1253 Appendix F Attachment 3, *Cross Domain Solution (CDS) Overlay*, September 2013.
- CNSSI No. 1001, *National Instruction on Classified Information Spillage*, February 2008.
- CNSSI No. 4009, *National Information Assurance (IA) Glossary*, April 2010.
- CNSSI No. 7000, *TEMPEST Countermeasures for Facilities*, May 2004.
- National Security Telecommunications and Information Systems Security (NSTISS) Instruction (NSTISSI) No. 7002, *TEMPEST Glossary*, March, 1995.
- CNSS Policy (CNSSP) No. 15, *National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems*, October 2012.
- CNSSP No. 17, *Policy on Wireless Systems*, January 2014.
- CNSSP No. 25, *National Policy for Public Key Infrastructure in National Security Systems*, March 2009.
- CNSSP No. 26, *National Policy on Reducing the Risk of Removable Media for National Security*, July 2013.
- CNSS Directive (CNSSD) No. 504, *Directive on Protecting NSS from Insider Threat*, February 2014.
- White House Memorandum, February 2014, Subject: *Near-term Measures to Reduce the Risk of High-Impact Unauthorized Disclosures*.
- White House Memorandum, November 2012, Subject: *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs.*

[1] Includes errata updates through January 2014.

2. Overlay Characteristics

This overlay applies to NSS that store, process, or transmit classified information. Information may be considered for classification when there is a reasonable expectation that unauthorized disclosure of the information could cause damage to national security[2]. There are three levels of classification: Top Secret (exceptionally grave damage), Secret (serious damage), and Confidential (damage).

Types of classified information include information that pertains to military plans, weapon systems, or operations; intelligence activities; foreign relations and government information; scientific, technological, or economic matters related to national security; safeguarding nuclear materials or facilities; development and use of weapons of mass destruction; and vulnerabilities and capabilities of NSS. Classified information on an information system requires protections and handling methods that are in addition to those required to protect unclassified information, because of the information's nature and potential harm that would result from unauthorized disclosure.

Impact values for confidentiality are not equivalent to classification levels. A loss of confidentiality is different than an unauthorized disclosure of classified information. Confidentiality impact values represent levels of impact on organizational operations and assets, individuals, other organizations, and the Nation. In contrast, classification levels represent the degrees of damage to national security. The categorization decision (i.e., the impact values for confidentiality, integrity, and availability) is independent of the classification decision.

Organizations are required by EO 13526 to establish uniform procedures to ensure information systems prevent access by unauthorized persons and ensure the integrity of the information. These procedures consist of safeguards to properly reproduce, transfer, and destroy classified information. Methods for safeguarding classified information include, but are not limited to, clearing personnel, having personnel sign non-disclosure agreements (NDAs), and only allowing access to information if personnel have the appropriate clearance and a need to know. Proper marking is also essential for appropriate handling of classified information.

The assumptions that underlie the security control selections and serve as the basis to justify the allocation of controls in the Classified Information Overlay include:

- The information system stores, processes, or transmits classified information.
- The information system does not store, process, or transmit classified information that requires protection within any Special Access Program (SAP), which includes sensitive compartmented information (SCI).[3]

[2] EO 13526 provides the complete definition of classified information in Section 6.1.

[3] SAP is defined in EO 13526, Section 4.3. If the information system stores, processes or transmits classified information that requires protection within a SAP established by the Director of National Intelligence, the specifications in the Intelligence Overlay apply. If the information system stores, processes, or transmits classified information that requires protection within a SAP established by another authority, consult that authority for appropriate specifications.

- All persons authorized for access to the information system have been granted a security clearance for the highest classification of information stored, processed, or transmitted by the information system; however, all may not have a need to know.
- All persons authorized for access to the information system are U.S. citizens.
- The organization provides facility and personnel security to ensure only personnel with security clearances for all information stored, processed, or transmitted by the system are allowed unescorted access to the facility and/or areas within the facility where the information system resides.
- If the information system is interconnected to other information systems that provide access to users who have NOT been granted a security clearance for the highest classification of information stored, processed, or transmitted by this information system, the organization ensures that interconnection is made through a cross domain solution (CDS) providing protections consistent with the CDS Overlay. The organization also ensures that the appropriate security control specifications for that CDS are addressed in the CDS security plan.

3. Applicability

Use the following question to determine the applicability of the Classified Information Overlay:

Does the information system of interest by intent and design[4] store, process, or transmit classified information? If yes, this overlay does apply. If no, this overlay does not apply.

4. Overlay Summary

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

- A plus sign ("+") indicates the control should be selected.
- Two dashes ("-") indicates the control should not 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 this overlay defines a value for an organizational-defined parameter for the control.
- The letter "R" indicates there is at least one regulatory/statutory reference that requires the control selection or that the control helps to meet the regulatory/statutory requirements.

[4] The specifications in this overlay do not apply to information systems that store, process, or transmit classified information only for a limited time as a consequence of an information spill.

Table 1: Classified Information Overlay Security Controls

CONTROL	CLASSIFIED INFORMATION OVERLAY
AC-3(2)	+VR
AC-3(4)	+R
AC-5	+GR
AC-6	+R
AC-6(7)	+R
AC-11	+EVR
AC-11(1)	+R
AC-16	+GR
AC-16(5)	+GR
AC-16(6)	+GR
AC-16(7)	+GR
AC-18	+R
AC-18(3)	+R
AC-18(4)	+R
AC-19	+GR
AC-20	+R
AC-20(1)	+R
AC-20(2)	+R
AC-20(3)	+EGR
AC-20(4)	+R
AC-23	+R
AT-2	+EVR
AT-2(2)	+R
AU-6	+R
AU-6(4)	+R
AU-6(5)	+VR
AU-6(8)	+R
AU-6(9)	+R
AU-12	+R
AU-14	+R
AU-16	+R
AU-16(1)	+R
AU-16(2)	+VR
CA-3	+ER

CONTROL	CLASSIFIED INFORMATION OVERLAY
CA-3(2)	+R
CM-3(6)	+VR
CM-5(5)	+VR
IA-2	+R
IA-2(1)	+R
IA-2(2)	+R
IR-9	+R
IR-9(1)	+R
IR-9(2)	+R
IR-9(4)	+R
MA-3(3)	+R
MA-5(1)	+R
MP-1	+ER
MP-2	+R
MP-3	+R
MP-4	+VR
MP-5	+EVR
MP-5(3)	+ER
MP-5(4)	+ER
MP-6	+VR
MP-6(1)	+R
MP-6(2)	+R
MP-6(3)	+R
MP-7	+R
MP-8	+GR
MP-8(1)	+GR
MP-8(2)	+GR
MP-8(4)	+GR
PE-2(3)	+GVR
PE-3(2)	+ER
PE-3(3)	+R
PE-4	+R
PE-5(3)	+VR
PE-19	+R

CONTROL	CLASSIFIED INFORMATION OVERLAY
PE-19(1)	+R
PS-3(1)	+GR
PS-4	+VR
PS-4(1)	+R
PS-6(2)	+R
PS-6(3)	+R
RA-6	+R
SA-4(6)	+R
SA-15(9)	+ER
SC-2	+R
SC-3	+R
SC-8	+VR
SC-8(1)	+R

CONTROL	CLASSIFIED INFORMATION OVERLAY
SC-8(3)	+R
SC-8(4)	+R
SC-12(2)	+VR
SC-12(3)	+GVR
SC-13	+VR
SC-15(3)	+GR
SC-28	+GVR
SC-28(1)	+R
SC-42	+GR
SC-42(3)	+GVR
SI-4(14)	+R
SI-4(19)	+R
SI-4(21)	+R

5. Detailed Overlay Control Specifications

This section is a comprehensive view of the security control specifications as they apply to this overlay. The guidance provided in this section elaborates on the guidance in NIST SP 800-53. For controls that should either be selected or not selected, a justification is provided based on the defined overlay characteristics. In addition to a justification, a security control may have other specifications that include control extensions, supplemental guidance, parameter values, and regulatory/statutory references. The specifications in this section are summarized in Section 4, Table 1.

Per NIST SP 800-53, control enhancements are not intended to be selected independently (i.e., if a control enhancement is selected, then the corresponding base security control must also be selected). Security controls and enhancements are explicitly identified in an overlay only if they directly support the overlay topic. Ensure that the base controls associated with the enhancements in the overlay are tailored as appropriate in the final control set.

AC-3, ACCESS ENFORCEMENT

Control Enhancement: 2

> Justification to Select: 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.

Parameter Value: The information system enforces dual authorization for *all transfers of data from a classified computer network to removable media.*

Regulatory/Statutory Reference(s): EO 13587, Sec 6.1; White House Memorandum, *Near-term Measures to Reduce the Risk of High-Impact Unauthorized Disclosures*, Task D-1.

Control Enhancement: 4

Justification to Select: EO 13526 requires that classified information be accessible only to those with the appropriate need-to-know. Discretionary access controls provide a means to reduce the opportunities cleared individuals may have to gain access to information for which they do not have a need-to-know.

Regulatory/Statutory Reference(s): EO 13526, Sec 4.1, para. (a).

AC-5, SEPARATION OF DUTIES

Justification to Select: EO 13587 requires the establishment of an insider threat program for deterring, detecting, and mitigating insider threats, including the safeguarding of classified information from exploitation, compromise, or other unauthorized disclosure. White House Memorandum, *Near-term Measures to Reduce the Risk of High-Impact Unauthorized Disclosures*, requires the implementation of the separation of duties. Separation of duties provides a means to safeguard the information by reducing the opportunities individuals may have to gain access to information.

Supplemental Guidance: Organizations should separate roles for network or database administration from other sensitive functions, such as cryptographic key management, hardware management, removable media data transfer, system security management, or access to particularly sensitive information.

Regulatory/Statutory Reference(s): EO 13587, Sec 6.1; White House Memorandum, *Near-term Measures to Reduce the Risk of High-Impact Unauthorized Disclosures*, Tasks C-1 and C-3.

AC-6, LEAST PRIVILEGE

Justification to Select: EO 13526 requires that classified information be accessible only to those with the appropriate need-to-know. Implementing least privilege provides a means to reduce the opportunities individuals may have to gain access to information for which they do not have a need-to-know. White House Memorandum, *Near-term Measures to Reduce the Risk of High-Impact Unauthorized Disclosures*, requires the implementation of least privilege.

Regulatory/Statutory Reference(s): EO 13526, Sec 4.1, para. (a); White House Memorandum, *Near-term Measures to Reduce the Risk of High-Impact Unauthorized Disclosures*, Tasks C-1 and C-3.

Control Enhancement: 7

Justification to Select: The White House Memorandum, *Near-term Measures to Reduce the Risk of High-Impact Unauthorized Disclosures*, requires the review of all privileged users and ensures they have the appropriate clearances, roles, and scope to perform their duties.

Regulatory/Statutory Reference(s): EO 13526, Sec 4.1, para. (a); White House Memorandum, *Near-term Measures to Reduce the Risk of High-Impact Unauthorized Disclosures*, Tasks A-1, and C-1.

AC-11, SESSION LOCK

Justification to Select: EO 13526 requires organizations to establish uniform procedures to ensure information systems that store, process, or transmit classified information prevent access by unauthorized persons. Requiring a session lock after a specified period of inactivity or receiving a request from a user helps to prevent unauthorized users from physically using an authorized user's session as a means to gain unauthorized access to classified information.

Control Extension: Organizations require users to initiate a session lock of information system workstations before leaving them unattended.

Parameter Value: (a) The information system prevents further access to the system by initiating a session lock after *a period not to exceed 15 minutes* of inactivity or upon receiving a request from a user.

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

Control Enhancement: 1

Justification to Select: Requiring the information system to conceal the information previously visible on the display after session lock helps to prevent unauthorized users from viewing an authorized user's display as a means to gain unauthorized access to classified information.

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

AC-16, SECURITY ATTRIBUTES

Justification to Select: EO 13526 defines classification levels and requires organizations to mark classified information to reflect its classification.

Supplemental Guidance: For classification and control markings, the organization determines the permitted attributes and permitted values consistent with the policies applicable to the organization and based on the classification level and related security characteristics of the information stored, processed, or transmitted by the information system.

Regulatory/Statutory Reference(s): EO 13526, Sec 1.2, para. (a), Sec 1.6, para. (a), and Sec 2.1, para. (a-b).

Control Enhancement: 5, 6, 7

Justification to Select: See justification for AC-16.

Supplemental Guidance: See supplemental guidance for AC-16.

Regulatory/Statutory Reference(s): EO 13526, Sec 1.6, para. (a) and Sec 2.1, para. (a-b).

AC-18, WIRELESS ACCESS

Justification to Select: EO 13526 requires organizations to establish procedures and controls to prevent access by unauthorized persons to classified information. The use, or potential for use, of wireless technologies presents unique challenges for protecting classified information; the AC-18 base control and its selected enhancements are needed to address these challenges. Regardless of whether the organization *intends* to use wireless access for the information system of interest, these controls must be selected to ensure the organization defines the limitations on wireless access. Many information technology products are developed to have wireless capabilities. If those wireless capabilities are enabled, either inadvertently or intentionally, there is a risk of unauthorized access to, and exfiltration of, classified information. Selecting these controls does not imply intent to allow wireless access, but instead serves to ensure the organization takes conscious actions to either allow and to establish appropriate restrictions on its use, or disallow its use.

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

Control Enhancement: 3, 4

Justification to Select: See justification for AC-18.

Regulatory/Statutory Reference(s): EO 13526, Sec 4.1, para. (f) and (g).

AC-19, ACCESS CONTROL FOR MOBILE DEVICES

Justification to Select: EO 13526 requires organizations to establish procedures and controls to prevent access by unauthorized persons to classified information. The use, or potential for use, of mobile devices presents unique challenges for protecting classified information; AC-19, AC-19(4), and AC-19(5) are needed to address these challenges.

Supplemental Guidance: Regardless of whether the organization *intends* to use mobile devices as part of the information system of interest, this control must be selected. Advances in mobile technology have led to more powerful, smaller devices. These devices are used by a large percentage of the population and, as a result, unique countermeasures must be developed. Mobile devices may pose a risk of unauthorized access to, and exfiltration of, classified information. Selecting this control does not imply intent to allow mobile devices, but instead serves to ensure the organization takes conscious actions to either allow and to establish appropriate restrictions on their use or disallow their use.

Regulatory/Statutory Reference(s): EO 13526, Sec 4.1, para. (f) and (g); EO 13587, Sec 5.2, para. (a); CNSSP No. 17.

AC-20, USE OF EXTERNAL INFORMATION SYSTEMS

Justification to Select: EO 13526 requires organizations to establish procedures and controls to prevent access by unauthorized persons to classified information. The use of external information systems presents unique challenges for protecting classified information; AC-20 and its enhancements are needed to address these challenges.

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

Control Enhancement: 1, 2, 4

Justification to Select: See justification for AC-20.

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

Control Enhancement: 3

Justification to Select: See justification for AC-20.

Control Extension: The organization restricts the use of non-organizationally owned information systems, system components, or devices to process, store, or transmit classified information.

Supplemental Guidance: Some organizations may choose to establish trust relationships with other organizations to enable use of non-organizationally owned information systems, system components, or devices that process, store, or transmit classified organizational information. In cases of media devices, the organization should restrict use.

Regulatory/Statutory Reference(s): EO 13526, Sec 4.1, para. (f) and (g).

AC-23, DATA MINING PROTECTION

Justification to Select: EO 13587 requires the establishment of an insider threat program for deterring, detecting, and mitigating insider threats, including the safeguarding of classified information from exploitation, compromise, or other unauthorized disclosure. AC-23 requires organizations to identify appropriate techniques to prevent and detect unnecessary or unauthorized data mining, which can be used by an insider to collect organizational information for the purpose of exfiltration.

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

AT-2, SECURITY AWARENESS TRAINING

Justification to Select: EO 13526 requires organizations to provide training on the proper safeguarding of classified information.

Control Extension: The organization provides training on the proper safeguarding of classified information and on the criminal, civil, and administrative sanctions that may be imposed on an individual who fails to protect classified information from unauthorized disclosure. This training is provided upon granting a person a clearance and at least annually for as long as the information system user has access to the system.

Parameter Value: (c) *annually for as long as the user has access to the system*.

Regulatory/Statutory Reference(s): EO 13526, Sec 4.1, para. (b).

Control Enhancement: 2

Justification to Select: The White House Memorandum, *Minimum Standards for Executive Branch Insider Threat Programs*, requires that organizations provide insider threat awareness training to all cleared employees.

Regulatory/Statutory Reference(s): White House Memorandum, *Minimum Standards for Executive Branch Insider Threat Programs*, Tab 2, Sec I.

AU-6, AUDIT REVIEW, ANALYSIS, AND REPORTING

Justification to Select: EO 13587 requires the establishment of an insider threat program for deterring, detecting, and mitigating insider threats, including the safeguarding of classified information from exploitation, compromise, or other unauthorized disclosure. The White House Memorandum, *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*, requires agencies to monitor and audit user activity on classified networks. Reviewing and analyzing audit records support the detection of insider threat activities.

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

Control Enhancement: 4

Justification to Select: See justification for AU-6. The White House Memorandum, *Minimum Standards for Executive Branch Insider Threat Programs*, requires the organization to gather information for centralized analysis, reporting and response.

Regulatory/Statutory Reference(s): White House Memorandum, *Minimum Standards for Executive Branch Insider Threat Programs*, Tab 2, Sec E.1.

Control Enhancement: 5

Justification to Select: See justification for AU-6. The White House Memorandum, *Minimum Standards*, requires the organization 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 counterintelligence, security, information assurance, human resources, law enforcement, the monitoring of user activity, and other sources as necessary and appropriate.

Parameter Value: The organization integrates analysis of audit records with the 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): White House Memorandum, *Minimum Standards for Executive Branch Insider Threat Programs*, Tab 2, Sec E.1.

Control Enhancement: 8

Justification to Select: See justification for AU-6. 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*.

Regulatory/Statutory Reference(s): White House Memorandum, *Near-term Measures to Reduce the Risk of High-Impact Unauthorized Disclosures*, Task C-5; White House Memorandum, *National Insider Threat Policy*, Tab 1, Sec B.2(1) and *Minimum Standards for Executive Branch Insider Threat Programs*, Tab 2, Sec H.

Control Enhancement: 9

Justification to Select: See justification for AU-6.

Regulatory/Statutory Reference(s): White House Memorandum, *National Insider Threat Policy*, Tab 1, Sec B.2(2, 4) and *Minimum Standards for Executive Branch Insider Threat Programs*, Tab 2, Sec E.1.

AU-12, AUDIT GENERATION

Justification to Select: EO 13587 requires the establishment of an insider threat program for deterring, detecting, and mitigating insider threats, including the safeguarding of classified information from exploitation, compromise, or other unauthorized disclosure. The White House Memorandum, *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*, requires agencies to monitor and audit user activity on classified networks. Generating audit records supports the detection of insider threat activities.

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

AU-14, SESSION AUDIT

Justification to Select: 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 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 classified information against insider threat. Classified information is more likely to be targeted for espionage than unclassified information.

Regulatory/Statutory Reference(s): White House Memorandum, *National Insider Threat Policy*, Tab 1, Sec B.2(1) and *Minimum Standards for Executive Branch Insider Threat Programs*, Tab 2, Sec H.1.

AU-16, CROSS-ORGANIZATIONAL AUDITING

Justification to Select: EO 13587 requires the establishment of an insider threat program for deterring, detecting, and mitigating insider threats, including the safeguarding of classified information from exploitation, compromise, or other unauthorized disclosure. Coordinating audit information across organizations supports the detection of insider threat activities.

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

Control Enhancement: 1

Justification to Select: See justification for AU-16. Preserving the identities of individuals in cross-organization audit trails facilitates the detection of insider threats on all classified networks.

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

Control Enhancement: 2

Justification to Select: See justification for AU-16. Providing cross-organizational audit information is required to facilitate the detection and mitigation of insider threats on all classified networks.

Parameter Value: The organization provides cross-organizational audit information to *the organization's insider threat program, at a minimum* based on [*Assignment: organization-defined cross-organizational sharing agreements*].

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

CA-3, SYSTEM INTERCONNECTIONS

Justification to Select: EO 13526 requires organizations to ensure classified information disseminated outside the executive branch is protected in a manner equivalent to that provided within the executive branch. An Interconnection Security Agreement (ISA), as required by CA-3, is the appropriate means to convey the expectations for the associated security requirements.

Control Extension: For interconnections of information systems processing classified information that serve to disseminate classified information outside the executive branch;

the organization ensures via the use of an ISA, the protection of the information in a manner equivalent to that provided within the executive branch.

The organization prohibits the interconnection of a classified NSS to information systems operating at a different classification level, other than through a CDS that is managed and maintained consistent with the security control specifications in the CDS Overlay.

Regulatory/Statutory Reference(s): EO 13526, Sec 4.1, para. (e).

Control Enhancement: 2

Justification to Select: EO 13526 requires organizations to establish procedures and controls to provide adequate protection of classified information while stored, processed, or when transmitted and to prevent access by unauthorized persons to classified information. Organizations may not have control over external networks; therefore the interconnection of an information system to an external network presents unique challenges for protecting classified information. An appropriate boundary protection device is needed to address these challenges. Interconnections of classified NSS to information systems operating at different classification levels introduce the risk of unauthorized persons accessing classified information. A CDS is needed to address this risk.

Regulatory/Statutory Reference(s): EO 13526, Sec 4.1, para. (g); EO 13587, Sec 5.2, para. (a).

CM-3, CONFIGURATION CHANGE CONTROL

Control Enhancement: 6

Justification to Select: EO 13526 requires organizations to establish procedures and controls to prevent access by unauthorized persons to classified information. Cryptographic mechanisms are required (per the specifications in this overlay for SC-8 (1)) to protect the confidentiality of transmitted classified information. Configuration management of the cryptographic mechanisms employed helps to ensure that the required protections remain in effect.

Parameter Value: The organization ensures that cryptographic mechanisms used to provide *safeguarding of classified information from unauthorized access or modification* are under configuration management.

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

CM-5, ACCESS RESTRICTIONS FOR CHANGE

Control Enhancement: 5

Justification to Select: EO 13526 requires organizations to establish procedures and controls to prevent access by unauthorized persons to classified information. Limiting privileges to change information system components reduces the opportunities for insiders to grant access to classified information by unauthorized personnel.

Parameter Value: (b) The organization reviews and reevaluates privileges *at least quarterly*.

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

IA-2, IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)

Justification to Select: EO 13587 requires the establishment of an insider threat program for deterring, detecting, and mitigating insider threats, including the safeguarding of classified information from exploitation, compromise, or other unauthorized disclosure. Uniquely identifying and authenticating users limits access to authorized users and is a foundational component of detecting potentially malicious insiders.

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

Control Enhancement: 1, 2

Justification to Select: CNSS Directive 504 Annex C requires that agencies implement standardized access control methodologies, specifically multifactor authentication.

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

IR-9, INFORMATION SPILLAGE RESPONSE

Justification to Select: EO 13526 requires organizations to establish procedures and controls to prevent access by unauthorized persons to classified information. When classified information is spilled, organizations must execute procedures to minimize access to that information by unauthorized persons.

Regulatory/Statutory Reference(s): EO 13526, Sec 4.1, para. (g); CNSSI No. 1001.

Control Enhancement: 1, 2, 4

Justification to Select: See justification for IR-9.

Regulatory/Statutory Reference(s): EO 13526, Sec 4.1, para. (g); CNSSI No. 1001.

MA-3, MAINTENANCE TOOLS

Control Enhancement: 3

Justification to Select: EO 13526 prohibits the removal of classified information from official premises without proper authorization. Maintenance tools may contain classified information and their unauthorized removal from the premises may result in the loss of classified information; therefore, the removal of maintenance tools must be appropriately conducted.

Regulatory/Statutory Reference(s): EO 13526, Sec. 4.1, para. (d).

MA-5, MAINTENANCE PERSONNEL

Control Enhancement: 1

Justification to Select: EO 13526 requires organizations to establish procedures and controls to prevent access by unauthorized persons to classified information. The use of maintenance personnel that lack required clearances or are not U.S. citizens presents challenges for protecting classified information; MA-5 (1) is needed to address these challenges.

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

MP-1, MEDIA PROTECTION POLICY AND PROCEDURES

Justification to Select: EO 13526 states that classified information may not be removed from official premises without proper authorization. Organizations that process classified information must include appropriate content in their media protection policy and procedures.

Control Extension: The organization includes in media protection policy and/or procedures: (i) how authorizations for removing classified information from official premises are determined and documented; (ii) the appropriate means for controlling, protecting and monitoring removal of classified information from official premises; (iii) the appropriate means for transporting classified non-digital media, and classified and unclassified digital media, outside of the organization's controlled areas; and (iv) procedures for identifying areas as controlled vs. uncontrolled.

Regulatory/Statutory Reference(s): EO 13526, Sec. 4.1, para. (d).

MP-2, MEDIA ACCESS

Justification to Select: Media devices are resources that can be used to exfiltrate classified information and access to the devices should limited to authorized personnel. EO 13526 states that classified information may not be removed from official premises

without proper authorization. EO 13587 requires the establishment of an insider threat program for deterring, detecting, and mitigating insider threats, including the safeguarding of classified information from exploitation, compromise, or other unauthorized disclosure.

Regulatory/Statutory Reference(s): EO 13526, Sec 4.1, para. (d); EO 13587, Sec 5.2 and Sec 6.1.

MP-3, MEDIA MARKING

Justification to Select: EO 13526 requires organizations to mark classified information to reflect its classification.

Regulatory/Statutory Reference(s): EO 13526, Sec 1.6, para. (a) and Sec 2.1, para. (a) and (b); CNSSP No. 26.

MP-4, MEDIA STORAGE

Justification to Select: EO 13526 requires organizations to establish procedures and controls to prevent access by unauthorized persons to classified information. Physically controlling and securely storing media is necessary to protect the classified information contained within the media.

Parameter Value: Physically controls and securely stores *digital and non-digital media containing classified information* within *an area and/or container approved for processing and storing media based on the classification of the information contained within the media.*

Regulatory/Statutory Reference(s): EO 13526, Sec 4.1, para. (g); CNSSP No. 26.

MP-5, MEDIA TRANSPORT

Justification to Select: EO 13526 states that classified information may not be removed from official premises without proper authorization and that it must be stored under conditions that provide adequate protection and prevent access by unauthorized persons. Protection of classified information during transport, which includes maintaining accountability, documenting transport activities, and employing cryptographic measures, is essential to satisfy these requirements.

Control Extensions: The organization maintains accountability for media containing classified information during transport outside of controlled areas.

Parameter Value(s): The organization protects and controls *digital media containing classified information* during transport outside controlled areas using [*Assignment: organization-defined security safeguards*]. The organization protects and controls *non-digital media containing classified information* during transport outside controlled areas

using *double-wrapping in opaque enclosures and transport only by personnel with a security clearance for the classification of the media being transported.*

Regulatory/Statutory Reference(s): EO 13526, Sec. 4.1, para. (d) and (g); EO 13587, Sec 5.2, para. (a); CNSSP No. 26.

Control Enhancement: 3

Justification to Select: See justification for MP-5.

Control Extension: The organization employs an identified custodian during transport of classified information system media outside of controlled areas.

Regulatory/Statutory Reference(s): EO 13526, Sec 4.1, para. (d), (e), (f), and (g); EO 13587, Sec 5.2, para. (a); CNSSP No. 26.

Control Enhancement: 4

Justification to Select: See justification for MP-5.

Control Extension: The information system implements approved mechanisms to protect the confidentiality and integrity of classified information stored on digital media during transport outside of controlled areas.

Regulatory/Statutory Reference(s): EO 13526, Sec 4.1, para. (d), (e), (f), and (g); EO 13587, Sec 5.2, para. (a).

MP-6, MEDIA SANITIZATION

Justification to Select: EO 13526 states that all classified information must be destroyed under conditions that provide adequate protection and prevent access by unauthorized personnel. Sanitization and the verification of destruction of all types of media, physical and digital, help to meet this requirement.

Parameter Value: (a) Sanitizes *all digital and non-digital information system media containing classified information* prior to disposal, release out of organizational control, or release for reuse using [*Assignment: organization-defined sanitization techniques and procedures*] in accordance with applicable federal and organizational standards and policies.

Regulatory/Statutory Reference(s): EO 13526, Sec 4.1, para. (g); EO 13587, Sec 5.2, para. (a).

Control Enhancement: 1, 2, 3

Justification to Select: See justification for MP-6.

Regulatory/Statutory Reference(s): EO 13526, Sec 4.1, para. (g); EO 13587, Sec 5.2, para. (a).

MP-7, MEDIA USE

Justification to Select: EO 13526 requires organizations to establish procedures and controls to prevent access by unauthorized persons to classified information. Removable media provides a means for personnel to move classified data from official premises without proper authorization, and then in turn provide the classified information to unauthorized personnel. Restricting the use of removable media on systems that store, process or transmit classified information decreases the opportunities for unauthorized disclosure of classified information.

Regulatory/Statutory Reference(s): EO 13526, Sec. 4.1, para. (d); EO 13587, Sec 2.1(b) and Sec 5.2.

MP-8, MEDIA DOWNGRADING

Justification to Select: EO 13526 requires organizations to establish procedures and controls to prevent access by unauthorized persons to classified information. Classified information must be removed from media so that the classified information cannot be removed or reconstructed.

Supplemental Guidance: An alternative to downgrading is to replicate the unclassified or lower classified information to media that is designated for the classification level.

Regulatory/Statutory Reference(s): EO 13526, Sec 4.1, para. (g); EO 13587, Sec 5.2, para. (a).

Control Enhancement: 1, 2, 4

Justification to Select: See MP-8 justification to select.

Supplemental Guidance: See MP-8 supplemental guidance.

Regulatory/Statutory Reference(s): EO 13526, Sec 4.1, para. (g); EO 13587, Sec 5.2, para. (a).

PE-2, PHYSICAL ACCESS AUTHORIZATIONS

Control Enhancement: 3

Justification to Select: EO 13526 requires organizations to establish procedures and controls to prevent access by unauthorized persons to classified information. Restricting unescorted access is necessary to protect the classified information contained within the facility.

Supplemental Guidance: Organizations manage their facilities and provide adequate protections to ensure personnel do not have unescorted access to areas operating at classification levels higher than the clearance they have been granted. The organization may provide additional guidance to address their mission needs for areas within facilities or information systems with components operating at different classification levels.

Parameter Value(s): The organization restricts unescorted access to the facility where the information system resides to personnel with *security clearances for all information contained within the system*.

Regulatory/Statutory Reference(s): EO 13526, Sec 4.1, para. (g); EO 13587, Sec 5.2, para. (a).

PE-3, PHYSICAL ACCESS CONTROL

Control Enhancement: 2

Justification to Select: EO 13526 states that information may not be removed from official premises without proper authorization. Conducting security checks at random or a pre-defined frequency helps mitigate the risk of unauthorized removal of classified materials.

Control Extension: The organization monitors for unauthorized exfiltration of classified information.

Regulatory/Statutory Reference(s): EO 13526, Sec. 4.1, para. (d).

Control Enhancement: 3

Justification to Select: EO 13526 requires organizations to establish procedures and controls to prevent access by unauthorized persons to classified information. Employing guards or alarms at each access point helps mitigate the risk of authorized removal of classified material.

Regulatory/Statutory Reference(s): EO 13526, Sec 4.1, para. (g); EO 13587, Sec 5.2, para. (a).

PE-4, ACCESS CONTROL FOR TRANSMISSION MEDIUM

Justification to Select: EO 13526 requires organizations to establish procedures and controls to prevent access by unauthorized persons to classified information. Physically controlling the access to distribution and transmission lines helps mitigate the risk of unauthorized access to classified information.

Regulatory/Statutory Reference(s): EO 13526, Sec 4.1, para. (g); EO 13587, Sec 5.2, para. (a).

PE-5, ACCESS CONTROL FOR OUTPUT DEVICES

Control Enhancement: 3

Justification to Select: EO 13526 requires organizations to establish procedures and controls to prevent access by unauthorized persons to classified information. Marking output devices to indicate the classification level of information permitted to be output from them is an organizational procedure that serves to remind users that classified information of the specified level exists within the information system. Users should, as a result, be more aware and ready to guard output against access by uncleared personnel passing through the facility.

Parameter Value(s): The organization marks *all output devices in facilities containing information systems that that store, process, or transmit classified information* indicating the appropriate security marking of the information permitted to be output from the device.

Regulatory/Statutory Reference(s): EO 13526, Sec 4.1, para. (g); EO 13587, Sec 5.2, para. (a).

PE-19, INFORMATION LEAKAGE

Justification to Select: EO 13526 directs the safeguarding of classified information while stored, processed, or when transmitted. Information leakage through electromagnetic signals must be protected against to ensure the confidentiality of the classified information.

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

Control Enhancement: 1

Justification to Select: CNSSI No. 7000 delineates the TEMPEST policies and procedures for classified NSS.

Regulatory/Statutory Reference(s): CNSSI No. 7000; EO 13587, Sec 5.2, para. (a).

PS-3, PERSONNEL SCREENING

Control Enhancement: 1

Justification to Select: EO 13526 states that all personnel that have access to classified information must be cleared through a determination of eligibility, NDA, and have the appropriate need to know for the information.

Supplemental Guidance: The agency head or agency head's designee must make a favorable determination that the person is eligible for access for information at classification levels up to and including the level specified in the clearance.

Regulatory/Statutory Reference(s): EO 13526, Sec. 4.1, para. (a) and (b); EO 13587, Sec 5.2, para. (a).

PS-4, PERSONNEL TERMINATION

Justification to Select: EO 13526 requires that classified information be accessible only to those with the appropriate clearance and need to know. After an individual ceases to be employed by the organization, they no longer have a need to access classified information and may not remove any classified information from an agency pursuant to the EO. Employees need to be reminded of these and other organizational requirements as part of the termination process to protect the confidentiality of classified information.

Parameter Value: c. The organization, upon termination of individual employment, conducts exit interviews that include a discussion of *prohibitions against: (i) the removal of classified information from the organization's control; and (ii) direction that information be declassified in order to remove it from the organization's control*.[5]

Regulatory/Statutory Reference(s): EO 13526, Sec. 4.1, para. (c).

Control Enhancement: 1

Justification to Select: See justification for PS-4.

Regulatory/Statutory Reference(s): EO 13526, Sec. 4.1, para. (a) and (c).

[5] The intent of this specification is to ensure this information security topic is covered in the exit interview, not to exclude other topics from also being covered.

PS-6, ACCESS AGREEMENTS

Control Enhancement: 2

Justification to Select: EO 13526 states that all personnel that have access to classified information must be cleared through a determination of eligibility, NDA, and have the appropriate need-to-know for the information.

Regulatory/Statutory Reference(s): EO 13526, Sec. 4.1, para. (a).

Control Enhancement: 3

Justification to Select: EO 13526 requires that classified information be accessible only to those with the appropriate clearance and need-to-know. After an individual ceases to be employed by the organization, they may no longer have a need to access classified information and may not remove any classified information from an agency pursuant to the EO. Employees need to be reminded of these and other organizational requirements as part of the termination process to protect the confidentiality of classified information.

Regulatory/Statutory Reference(s): EO 13526, Sec 4.1, para. (a) and (c).

RA-6, TECHNICAL SURVEILLANCE COUNTERMEASURES SURVEY

Justification to Select: EO 13526 requires that classified information be accessible only to those with the appropriate clearance and need-to-know. Many information technology products are vulnerable to inadvertent, or intentional, surveillance actions and need to be countered to prevent information leakage to unauthorized personnel. This control serves to ensure the organization takes conscious actions to minimize the technical surveillance risk and protect the confidentiality of classified information.

Regulatory/Statutory Reference(s): EO 13526, Sec 4.1, para. (a), (g), and (f).

SA-4, ACQUISITION PROCESS

Control Enhancement: 6

Justification to Select: EO 13526 directs the safeguarding of classified information while stored, processed, or when transmitted. The use of an NSA-approved solution protects the transmission of classified information when the network transmitting the information is at a lower classification level.

Regulatory/Statutory Reference(s): EO 13526, Sec. 4.1, para. (f) and (g); CNSSP No. 11. Sec IV, 5 and 7.

SA-15, DEVELOPMENT PROCESS, STANDARDS, AND TOOLS

Control Enhancement: 9

Justification to Select: EO 13526 directs the safeguarding of classified information while stored, processed, or when transmitted. When used in test environments, live data must be protected to preserve authorized restrictions on information access. The use of live data in test environments does not change its classification.

Control Extension: Classified information can only be used in test and simulation environments that are at least at the same classification level as the live data.

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

SC-2, APPLICATION PARTITIONING

Justification to Select: EO 13526 requires that classified information be accessible only to those with the appropriate need-to-know. Application partitioning provides a means to reduce the opportunities individuals may have to gain access to information for which they do not have a need-to-know.

Regulatory/Statutory Reference(s): EO 13526, Sec 4.1, para. (a).

SC-3, SECURITY FUNCTION ISOLATION

Justification to Select: EO 13526 requires that classified information be accessible only to those with the appropriate need-to-know. Security function isolation provides a means to reduce the opportunities cleared individuals may have to gain access to information for which they do not have a need-to-know.

Regulatory/Statutory Reference(s): EO 13526, Sec 4.1, para. (a).

SC-8, TRANSMISSION CONFIDENTIALITY AND INTEGRITY

Justification to Select: EO 13526 directs the safeguarding of classified information while in transmission to ensure the integrity of the information and provide adequate protection from unauthorized access.

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

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

Control Enhancement: 1, 3, 4

Justification to Select: EO 13526 directs the safeguarding of classified information while it is in transmission to ensure the integrity of the information and provide adequate protection from unauthorized access. Classified information in transmission must be protected via cryptography as required by CNSSP No. 15.

Regulatory/Statutory Reference(s): EO 13526, Sec 4.1, para. (a), (f), and (g); EO 13587, Sec 5.2, para. (a); CNSSP No. 15 Sec IV.4.

SC-12, CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

Control Enhancement: 2

Justification to Select: CNSSP No. 15 requires the use of NSA-approved cryptography to protect NSS and the information that resides in the system.

Parameter Value: The organization produces, controls, and distributes symmetric cryptographic keys using *NSA-approved* key management technology and processes.

Regulatory/Statutory Reference(s): CNSSP No. 15 Sec IV.4; Sec 5.b.(3).

Control Enhancement: 3

Justification to Select: CNSSP No. 15 requires the use of NSA-approved cryptography to protect NSS and the information that resides in the system.

Supplemental Guidance: CNSSP No. 25 requires that NSS operating at the Secret level obtain PKI support from the NSS-PKI.

Parameter Value: The organization produces, controls, and distributes asymmetric cryptographic keys using *NSA-approved key management technology and processes*.

Regulatory/Statutory Reference(s): CNSSP No. 15 Sec IV.4 and Sec 5.b.(3); CNSSP No. 25.

SC-13, CRYPTOGRAPHIC PROTECTION

Justification to Select: EO 13526 directs the safeguarding of classified information while stored, processed, or when transmitted. This applies to the use of an NSA- approved solution to protect classified information transmitted when the network transmitting the information is at a lower classification level.

Parameter Value: The information system implements *NSA-approved cryptography for protecting classified information from access by personnel who lack the necessary*

security clearance in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

Regulatory/Statutory Reference(s): EO 13526, Sec. 4.1, para. (f) and (g); CNSSP No. 15 Sec IV.4.

SC-15, COLLABORATIVE COMPUTING DEVICES

Control Enhancement: 3

Justification to Select: EO 13526 directs the safeguarding of classified information while in use and when transmitted to provide adequate protection and prevent access by unauthorized persons. Use of collaborative computing devices in unauthorized locations represents an unacceptable risk of disclosure of classified information to unauthorized persons.

Supplemental Guidance: Collaborative devices have an aspect of trust associated with their use (e.g., it is hard to verify how many people are listening through one connection). In secure works areas, it is necessary to disable collaborative devices to prevent unauthorized access to classified information (e.g., through eavesdropping) and to verify that personnel in the room have the necessary authorizations to access classified information.

Regulatory/Statutory Reference(s): EO 13526, Sec 4.1, para. (a) and (f).

SC-28, PROTECTION OF INFORMATION AT REST

Justification to Select: EO 13526 directs the safeguarding of classified information while stored to prevent access by unauthorized persons and to ensure the integrity of the information. Cryptography provides protections for the confidentiality and integrity of information in storage.

Supplemental Guidance: The organization, in accordance with law, Executive Orders, and policy, determines the protection needs for the confidentiality of the information, including who has access to the information and the appropriate means for its protection.

Parameter Value: The information system protects the *confidentiality and integrity* of *classified information at rest*.

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

Control Enhancement: 1

Justification to Select: See justification for SC-28.

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

SC-42, SENSOR CAPABILITY AND DATA

Justification to Select: EO 13587 requires the establishment of an insider threat program for deterring, detecting, and mitigating insider threats, including the safeguarding of classified information from exploitation, compromise, or other unauthorized disclosure. Prohibiting the remote activation 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: The organization may define exceptions to allow remote activation of sensor capabilities such as secure VTC, 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 remote activation of devices with sensor capabilities in those areas.

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

Control Enhancement: 3

Justification to Select: EO 13587 requires the establishment of an insider threat program for deterring, detecting, and mitigating insider threats, including the safeguarding of classified information from exploitation, compromise, or other unauthorized disclosure. 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: The organization may define exceptions to allow sensor capabilities such as secure VTC, 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 Values: 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 [organization-defined areas or devices]*.

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

SI-4, INFORMATION SYSTEM MONITORING

Control Enhancement: 14

Justification to Select: EO 13587 requires the establishment of an insider threat program for deterring, detecting, and mitigating insider threats, including the safeguarding of classified information from exploitation, compromise, or other unauthorized disclosure. Monitoring wireless networks for unauthorized use is necessary to protect classified information as it identifies unsanctioned connections and potential information leaks.

Regulatory/Statutory Reference(s): EO 13526, Sec 4.1, para. (f) and (g); CNSSP No. 17 Sec 5.b.iv; EO 13587, Sec 5.2, para. (a).

Control Enhancement: 19, 21

Justification to Select: EO 13526 requires organizations to establish procedures and controls to prevent access by unauthorized persons to classified information. Monitoring people that may pose greater risk or are in a probationary period is pertinent to verifying that these people continue to be qualified to access classified information.

Regulatory/Statutory Reference(s): EO 13526, Sec 4.1, para. (a) and (b).

6. Tailoring Considerations

Organizations should consider the following specific control guidance when tailoring information systems that are used to store, process, or transmit classified information in addition to using the general tailoring guidance in CNSSI No. 1253.

AC-18, WIRELESS ACCESS

Control Enhancement: 1, 5

Supplemental Guidance: If the organization intends to use wireless access for the information system of interest, then these controls must be selected. If wireless capabilities are enabled, there is a risk of unauthorized access to, and exfiltration of, classified information.

Regulatory/Statutory Reference(s): EO 13526, Sec 4.1, para. (f) and (g).

AC-19, ACCESS CONTROL FOR MOBILE DEVICES

Control Enhancement: 4

Supplemental Guidance: If the organization intends to allow mobile devices in the same facility as the information system of interest, even if not part of the information system, then this control must be selected.

Regulatory/Statutory Reference(s): EO 13526, Sec 4.1, para. (f) and (g). EO 13587, Sec 5.2, para. (a); CNSSP No. 17.

Control Enhancement: 5

Supplemental Guidance: If the organization intends to allow mobile devices as part of the information system of interest, then this control must be selected.

Regulatory/Statutory Reference(s): EO 13526, Sec 4.1, para. (f) and (g); EO 13587, Sec 5.2, para. (a); CNSSP No. 17.

7. Definitions

The terms used in this overlay are all defined in CNSSI No. 4009, *National Information Assurance (IA) Glossary*, or one of the other references listed in section 1 of this document.