

# Classified System Overlay

## 1. Purpose and Scope

The Classified System Overlay identifies security control specifications needed to safeguard classified information stored, processed, or transmitted by national security systems (NSS). This overlay is baseline independent and can be used with any NSS baseline (security and privacy) to safeguard classified information. As a result, there may be overlap of controls between an NSS baseline and controls identified in this overlay.<sup>1</sup>

Organizations must effectively manage security and privacy risks related to safeguarding classified information. To do so, the security and privacy control baselines are implemented together to support risk management decisions related to confidentiality, integrity, and/or availability as well as manage enterprise privacy risks. The Classified System Overlay provides details on why it is necessary to apply specified controls for safeguarding classified information.

The security and privacy baselines in CNSSI No. 1253 are “starting points” to guide an organization in controls applicable to their system once categorization is complete. Organizations are permitted to tailor<sup>2</sup> the applied baseline to address specific mission or business needs and risks. Controls identified in this overlay generally have a legal/regulatory requirement associated with them and should not be tailored out without significant justification. For example, AT-2 (Literacy Training and Awareness) is in all NSS Security Control Baselines and the NSS Privacy Control Baseline because it is required by a regulatory requirement. An organization may tailor AT-2 out based on a risk assessment of the sufficiency of training and awareness provided. However, if an organization has a system with classified information on it and this overlay is applied, this overlay specifically identifies AT-2 as a control to support the safeguarding of classified information. While tailoring AT-2 out may have minimal risk to unclassified NSS, there could be significant risk to systems processing classified information if users with access to such systems and classified information on those systems are not properly and regularly trained on their responsibilities regarding protection of classified information.

For NSS that process personally identifiable information (PII) and must address system-specific privacy risks<sup>3</sup>, the Privacy Overlays may apply. Security and dissemination restrictions provided by classified systems are separate and distinct from privacy controls and handling requirements for addressing privacy risk. Organizations must ensure appropriate privacy control specifications are applied to classified systems that process<sup>4</sup> PII consistent with the Privacy Overlay, and document them (e.g., in the privacy plan). Consult the Privacy Overlay to determine whether a system has PII and therefore must apply the Privacy Overlay in addition to applying this overlay.

---

<sup>1</sup> Refer to CNSSI No 1253 Section 2.5, “Relationship between Baselines and Overlays”, and Section 3.2, “RMF Step: Select” for further general NSS guidance related to controls.

<sup>2</sup> Refer to CNSSI No. 1253 Section 3.2.2, “Task S-2, Control Tailoring.”

<sup>3</sup> Refer to CNSSI No. 1253 Section 2.5.1, “Relationship between Privacy Control Baseline and Privacy Overlays” for further guidance.

<sup>4</sup> This includes systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of information (collectively referred to as “process”).

This overlay does not include control specifications for cross domain solutions (CDS), intelligence systems (to include Special Access Program or Sensitive Compartmented Information), or networks on which non-US persons have or may have access. For guidance on those areas, refer to the appropriate overlay.<sup>5</sup>

## 2. Authoritative References

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

The following documents were used to create this overlay:

- Executive Order (EO) 13526, *Classified National Security Information*, 29 December 2009.
- EO 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, 7 October 2011.
- EO 13764, *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.
- EO 13873, *Securing the Information and Communications Technology and Services Supply Chain*, 15 May 2019.
- EO 14032, *Addressing the Threat from Securities Investments that Finance Certain Companies of the People's Republic of China*, 07 June 2021.
- National Security Memorandum (NSM) 8, *Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems*, 19 January 2022.
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, September 2020.<sup>6</sup>
- NIST SP 800-53B, *Control Baselines for Information Systems and Organizations*, October 2020.<sup>7</sup>
- CNSS Directive (CNSSD) No. 504, *Directive on Protecting NSS from Insider Threat*, September 2021.
- CNSSD No. 505, *Supply Chain Risk Management (SCRM)*, November 2021.
- CNSS Policy (CNSSP) No. 15, *Use of Public Standards for Secure Information Sharing*, October 2016.
- CNSSP No. 17, *Policy on Wireless Systems*, January 2014.
- CNSSP No. 18, *National Policy on Classified Information Spillage*, May 2021.

---

<sup>5</sup> An overlay is separate and distinct from a NIST Cybersecurity Framework Profile. Profiles provide guidance to address strategic mission/business objectives and reduce cybersecurity risk and identify specific cybersecurity activities to support mission/business success. Overlays identify specific sets of controls (and control enhancements) to apply to systems and support implementation of the NIST Risk Management Framework. CNSSI No. 1253 focuses on the applicability and use of CNSS-defined overlays.

<sup>6</sup> Includes errata updates as of 10 December 2020.

<sup>7</sup> Includes errata updates as of 10 December 2020.

- CNSSP No. 25, *National Policy for Public Key Infrastructure in National Security Systems*, December 2017.
- CNSSP No. 26, *National Policy on Reducing the Risk of Removable Media for National Security*, July 2021.
- CNSSP No. 32, *Policy on Cloud Security*, May 2022.
- Committee on National Security Systems (CNSS) Instruction (CNSSI) No. 1001, *National Instruction on Classified Information Spillage*, June 2021.
- CNSSI No. 1253, *Categorization and Control Selection for National Security Systems*, July 2022.
- CNSSI No. 1253 Appendix E Attachment 1, *Security Control Overlays Template*, August 2013.
- CNSSI No. 1253 Appendix E Attachment 3, *Cross Domain Solution (CDS) Overlays*, September 2017.
- CNSSI No. 4009, *Committee on National Security Systems (CNSS) Glossary*, March 2022.
- White House Memorandum, November 2012, *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*.

### 3. 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<sup>8</sup>. There are three levels of classification: Top Secret (exceptionally grave damage), Secret (serious damage), and Confidential (damage). This overlay does not apply to NSS that store, process, or transmit only information that is unclassified, to include Controlled Unclassified Information (CUI).

Types of classified information include information that pertains to military plans, weapon systems, or operations; foreign government information; intelligence activities (including covert action), intelligence sources or methods or cryptology; foreign relations or foreign activities of the United States, including confidential sources; scientific, technological, or economic matters relating to the national security; United States Government programs for safeguarding nuclear materials or facilities; vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security; or the development, production, or use of weapons of mass destruction. Classified information on systems requires protections and handling methods that are in addition to those required to protect unclassified information, because of the classified 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 from 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

---

<sup>8</sup> EO 13526 provides the complete definition of classified information in Section 6.1.

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 systems prevent access by unauthorized persons and ensure the integrity of the information. These procedures consist of safeguards to properly store, reproduce, transfer, and destroy classified information. Methods for safeguarding classified information include, but are not limited to, requiring personnel clearances, signed non-disclosure agreements (NDAs), and the appropriate clearance and need to know for information access. 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 System Overlay include:

- The system stores, processes, or transmits classified information.<sup>9</sup>
- The system does not store, process, or transmit classified information that requires protection within any Special Access Program (SAP), which includes sensitive compartmented information (SCI).<sup>10</sup>
- All persons authorized for access to the system have been granted a security clearance for the highest classification of information stored, processed, or transmitted by the system; however, all may not have a need to know.
- All persons authorized for access to the 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 system resides.

## 4. Applicability

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

Does the system of interest by intent and design<sup>11</sup> store, process, or transmit classified information? If yes, this overlay does apply. If no, this overlay does not apply.

---

<sup>9</sup> Safeguards for protecting classified information are not equivalent to addressing safeguarding needs to address the risks related to impact levels for information types as these two concepts are mutually exclusive. As a result, safeguards (including to address regulatory requirements for an information type) may be needed to address information type risk in addition to safeguards to protect classified information.

<sup>10</sup> SAP is defined in EO 13526, Section 4.3. If the system stores, processes or transmits classified information that requires protection within a SAP established by the Director of National Intelligence, the specification in the Intelligence Overlay apply. If the system stores, processes, or transmits, classified information that requires protection within a SAP established by another authority, consult that authority for appropriate specifications.

<sup>11</sup> The specifications in this overlay do not apply to systems that store, process, or transmit classified information only for a limited time as a consequence of an information spill.

## 5. Summary of Control Specifications

Table 1 (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.
- The letter “G” indicates there is guidance related to the control.
- The letter “R” indicates there is a reference(s) that requires the control selection or that the control helps to meet the regulatory, statutory, or other legal requirements.
- The letter “V” indicates this overlay defines a parameter value for the control.

Salmon pink shading indicates controls that are new in NIST SP 800-53 Rev 5.

The Privacy Implementation Considerations column identifies controls that are not added to the CNSS Privacy Control Baseline but, if implemented, may have a privacy impact and require coordination with the Senior Agency Official for Privacy (SAOP) or designee to address privacy considerations prior to implementation. Checkmarks in this column include a subscripted number(s) that correlates to the following list of typical implications to consider when implementing the control:

1. Coordinate an approach between security and privacy to manage privacy risk
2. Design choices may mitigate privacy risks
3. Identify and address hidden privacy risks
4. Ensure PII does not flow through or into a system that is not authorized to process PII

Refer to Table 2 for controls that may be required when certain conditions are met by systems containing classified information to ensure security and privacy concerns related to the specified control are adequately addressed.

**Table 1: Classified System Overlay Summary of Control Specifications**

Control ID	Control Name	Classified System Overlay	Privacy Implementation Considerations
AC-1	(Access Control) Policy and Procedures	+GR	
AC-3(2)	Access Enforcement   Dual Authorization	+R	
AC-3(4)	Access Enforcement   Discretionary Access Control	+R	
AC-5	Separation of Duties	+GR	
AC-6	Least Privilege	+R	
AC-6(7)	Least Privilege   Review of User Privileges	+R	
AC-11	Device Lock	+VR	
AC-11(1)	Device Lock   Pattern-Hiding Displays	+R	
AC-16	Security and Privacy Attributes	+GR	
AC-16(5)	Security and Privacy Attributes   Attribute Displays on Objects to be Output	+GR	

<b>Control ID</b>	<b>Control Name</b>	<b>Classified System Overlay</b>	<b>Privacy Implementation Considerations</b>
AC-16(6)	Security and Privacy Attributes   Maintenance of Attribute Association	+GR	
AC-16(7)	Security and Privacy Attributes   Consistent Attribute Interpretation	+GR	
AC-18	Wireless Access	+R	
AC-18(3)	Wireless Access   Disable Wireless Networking	+R	
AC-18(4)	Wireless Access   Restrict Configurations by Users	+R	
AC-19	Access Control for Mobile Devices	+GR	
AC-19(4)	Access Control for Mobile Devices   Restrictions for Classified Information	+GR	
AC-20	Use of External Systems	+R	
AC-20(1)	Use of External Systems   Limits on Authorized Use	+R	
AC-20(2)	Use of External Systems   Portable Storage Devices – Restricted Use	+R	
AC-20(3)	Use of External Systems   Non-Organizationally Owned Systems – Restricted Use	+GR	
AC-20(4)	Use of External Systems   Network Accessible Storage Devices – Prohibited Use	+R	
AC-21	Information Sharing	+GR	
AC-23	Data Mining Protection	+GR	$\sqrt{3}$
AT-2	Literacy Training and Awareness	+GVR	
AT-2(2)	Literacy Training and Awareness   Insider Threat	+R	
AU-6	Audit Record Review, Analysis, and Reporting	+GR	$\sqrt{1}$
AU-6(4)	Audit Record Review, Analysis, and Reporting   Central Review and Analysis	+GR	$\sqrt{2}$
AU-6(5)	Audit Record Review, Analysis, and Reporting   Integrated Analysis of Audit Records	+GVR	$\sqrt{2}$
AU-6(8)	Audit Record Review, Analysis, and Reporting   Full Text Analysis of Privileged Commands	+R	
AU-6(9)	Audit Record Review, Analysis, and Reporting   Correlation with Information from Nontechnical Sources	+GR	$\sqrt{3}$
AU-12	Audit Record Generation	+R	
AU-14	Session Audit	+GR	$\sqrt{1}$
AU-16	Cross-Organizational Audit Logging	+GR	$\sqrt{4}$
AU-16(1)	Cross-Organizational Audit Logging   Identify Preservation	+GR	$\sqrt{2}$
AU-16(2)	Cross-Organizational Audit Logging   Sharing of Audit Information	+GVR	$\sqrt{2}$
CA-3	Information Exchange	+GVR	
CM-3(6)	Configuration Change Control   Cryptography Management	+R	
CM-5(5)	Access Restrictions for Change   Privilege Limitation for Production and Operation	+VR	

<b>Control ID</b>	<b>Control Name</b>	<b>Classified System Overlay</b>	<b>Privacy Implementation Considerations</b>
IA-2	Identification and Authentication (Organizational Users)	+GR	$\sqrt{3}$
IA-2(1)	Identification and Authentication (Organizational Users)   Multi-factor Authentication to Privileged Accounts	+R	
IA-2(2)	Identification and Authentication (Organizational Users)   Multi-factor Authentication to Non-Privileged Accounts	+R	
IA-5(6)	Authenticator Management   Protection of Authenticators	+GR	
IR-6	Incident Reporting	+VR	
IR-9	Information Spillage Response	+GVR	
IR-9(2)	Information Spillage Response   Training	+R	
IR-9(4)	Information Spillage Response   Exposure to Unauthorized Personnel	+GR	$\sqrt{3}$
MA-3(3)	Maintenance Tools   Prevent Unauthorized Removal	+R	
MA-5(1)	Maintenance Personnel   Individuals without Appropriate Access	+GR	$\sqrt{2,3}$
MP-1	(Media Protection) Policy and Procedures	+GR	
MP-2	Media Access	+R	
MP-3	Media Marking	+R	
MP-4	Media Storage	+VR	
MP-5	Media Transport	+VR	
MP-5(3)	Media Transport   Custodians	+GR	
MP-6	Media Sanitization	+VR	
MP-6(1)	Media Sanitization   Review, Approve, Track, Document, and Verify	+R	
MP-6(2)	Media Sanitization   Equipment Testing	+R	
MP-6(3)	Media Sanitization   Nondestructive Techniques	+R	
MP-7	Media Use	+R	
MP-8	Media Downgrading	+GR	
MP-8(1)	Media Downgrading   Documentation of Process	+R	
MP-8(2)	Media Downgrading   Equipment Testing	+GVR	
MP-8(4)	Media Downgrading   Classified Information	+GR	
PE-2(3)	Physical Access Authorizations   Restrict Unescorted Access	+GVR	
PE-3(2)	Physical Access Control   Facility and Systems	+GR	
PE-3(3)	Physical Access Control   Continuous Guards	+R	
PE-4	Access Control for Transmission	+R	
PE-19	Information Leakage	+R	
PE-19(1)	Information Leakage   National Emissions Policies and Procedures	+R	
PE-22	Component Marking	+VR	
PM-12	Insider Threat Program	+GR	$\sqrt{2}$

<b>Control ID</b>	<b>Control Name</b>	<b>Classified System Overlay</b>	<b>Privacy Implementation Considerations</b>
PS-3(1)	Personnel Screening   Classified Information	+GR	
PS-4	Personnel Termination	+GVR	$\checkmark_1$
PS-4(1)	Personnel Termination   Post-Employment Requirements	+R	
PS-6(2)	Access Agreements   Classified Information Requiring Special Protection	+R	
PS-6(3)	Access Agreements   Post-Employment Requirements	+R	
PS-9	Position Descriptions	+GR	
RA-3(2)	Risk Assessment   Use of All-Source Intelligence	+R	
RA-5	Vulnerability Monitoring and Scanning	+R	
RA-6	Technical Surveillance Countermeasures Survey	+GR	$\checkmark_3$
RA-10	Threat Hunting	+GR	$\checkmark^2$
SA-3(2)	System Development Life Cycle   Use of Live or Operational Data	+GR	
SA-4(6)	Acquisition Process   Use of Information Assurance Products	+R	
SC-2	Separation of System and User Functionality	+R	
SC-3	Security Function Isolation	+R	
SC-7(26)	Boundary Protection   Classified National Security System Connections	+VR	
SC-8	Transmission Confidentiality and Integrity	+VR	
SC-8(1)	Transmission Confidentiality and Integrity   Cryptographic Protection	+VR	
SC-8(3)	Transmission Confidentiality and Integrity   Cryptographic Protection for Message Externals	+R	
SC-8(4)	Transmission Confidentiality and Integrity   Conceal or Randomize Communications	+R	
SC-12	Cryptographic Key Establishment and Management	+GVR	$\checkmark_1$
SC-12(2)	Cryptographic Key Establishment and Management   Symmetric Keys	+VR	
SC-12(3)	Cryptographic Key Establishment and Management   Asymmetric Keys	+GVR	
SC-13	Cryptographic Protection	+VR	
SC-15(3)	Collaborative Computing Devices and Applications   Disabling and Removal in Secure Work Areas	+GR	
SC-28	Protection of Information at Rest	+GVR	
SC-28(1)	Protection of Information at Rest   Cryptographic Protection	+R	
SC-41	Port and I/O Device Access	+R	
SC-42	Sensor Capability and Data	+GR	$\checkmark_3$
SI-4(14)	System Monitoring   Wireless Intrusion Detection	+GR	$\checkmark_{2,3}$
SI-4(19)	System Monitoring   Risk for Individuals	+GR	$\checkmark_{2,3}$
SI-4(21)	System Monitoring   Probationary Periods	+GR	$\checkmark_{2,3}$

<b>Control ID</b>	<b>Control Name</b>	<b>Classified System Overlay</b>	<b>Privacy Implementation Considerations</b>
SR-3	Supply Chain Controls and Processes	+R	
SR-3(2)	Supply Chain Controls and Processes   Limitation of Harm	+R	
SR-4	Provenance	+R	
SR-7	Supply Chain Operations Security	+R	
SR-12	Component Disposal	+VR	

### **Controls with Implementation Considerations**

Table 2 (below) identifies controls that may be required when certain conditions are met by systems containing classified information to ensure security and privacy concerns related to the specified control are adequately addressed. If selected (e.g., part of a baseline, part of another overlay, tailoring decision), special consideration must be applied when these controls are allocated to any system handling classified information.

See Section 7, Implementation Considerations, for additional information about these controls.

**Table 2: Controls with Implementation Considerations**

<b>Control ID</b>	<b>Control Name</b>
AC-18(1)	Wireless Access   Authentication and Encryption
AC-18(5)	Wireless Access   Antennas and Transmission Power Levels
AC-19(5)	Access Control for Mobile Devices   Full Device or Container-Based Encryption
SA-9(8)	External System Services   Processing and Storage Location—U.S. Jurisdiction
SI-20	Tainting

## 6. Detailed Overlay Control Specifications

This section is a comprehensive view of the 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 be selected, a justification is provided based on the defined overlay characteristics. In addition to a justification, a control may have other specifications that include guidance, parameter values, and regulatory/statutory references. The specifications in this section are summarized by Section 5, Table 1.

Per NIST SP 800-53, control enhancements cannot be selected independently from or without also selecting the corresponding base security control (i.e., if a control enhancement is selected, then the corresponding base control must also be selected). Controls and enhancements are explicitly identified in an overlay only if they directly support the overlay topic. Tailor all controls and enhancements in the final control set as appropriate using the general tailoring guidance in CNSSI No. 1253. Controls and enhancements in a baseline or overlay either meet regulatory requirements or mitigate an anticipated threat. During tailoring, care must be taken that controls are not removed without a thorough understanding of the system, mission, environment, threats present (in the operational or development environment), regulatory requirements, and network, as removal may affect meeting a regulatory requirement and the security posture of the system, ultimately jeopardizing a system authorization.

### **AC-1, (Access Control) Policy and Procedures**

Justification to Select: CNSSD No. 504 requires the implementation of standardized access control methodologies (e.g., Identify and Access Management) for classified information. Organizations that process classified information must include appropriate content in their access control policy and procedures.

Guidance: The tighter coupling of the identity to a trusted credential will enhance the ability to enforce, control, and manage the access of users on NSS and prevent the threat of a malicious insider inappropriately using another user's credentials in an attempt to obfuscate involvement in the misuse of national security information.

Reference(s): EO 13526, Sec. 4.1, para. (d); CNSSD No. 504.

### **AC-3(2), Access Enforcement | Dual Authorization**

Justification to Select: CNSSD No. 504 requires the implementation of two-person controls (review and concurrence of a second person) for operations when protection is necessary to prevent significant disruptions and reduce the risk related to insider threats.

Reference(s): EO 13587, Sec 6.1.; CNSSD No. 504.

## **AC-3(4), Access Enforcement | Discretionary Access Controls**

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.

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. CNSSD No. 504 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.

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

Reference(s): EO 13587, Sec 6.1; CNSSD No. 504.

## **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. CNSSD No. 504 requires the implementation of least privilege.

Reference(s): EO 13526, Sec 4.1, para. (a); CNSSD No. 504.

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

Justification to Select: CNSSD No. 504 requires the review of all privileged users and ensures they have the appropriate clearances, roles, and scope to perform their duties and make changes as needed.

Reference(s): EO 13526, Sec 4.1, para. (a); CNSSD No. 504.

## **AC-11, Device Lock**

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

Parameter Value:

- a. Prevent further access to the system by *initiating a device lock after a period not to exceed 15 minutes of inactivity, requiring the user to initiate a device lock before leaving the system unattended;*

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

## **AC-11(1), Device Lock | Pattern-Hiding Displays**

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

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

## **AC-16, Security and Privacy Attributes**

Justification to Select: EO 13526 defines classification levels and requires organizations to label classified information to reflect its classification. Labeling refers to internal labels that the software can read, such as fields attached to information that might be used in a CDS or multilevel system, or for message routing.

Guidance: For classification and control labeling, 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 system. (For marking guidance, see MP-3.)

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

## **AC-16(5), Security and Privacy Attributes | Attribute Displays on Objects to be Output**

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

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 system.

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

## **AC-16(6), Security and Privacy Attributes | Maintenance of Attribute Association**

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

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 system.

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

## **AC-16(7), Security and Privacy Attributes | Consistent Attribute Interpretation**

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

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 system.

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

## **AC-18, Wireless Access**

Justification to Select: Regardless of whether the organization *intends* to use wireless access for the system of interest, this control 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. 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.

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

### **AC-18(3), Wireless Access | Disable Wireless Networking**

Justification to Select: Regardless of whether the organization *intends* to use wireless access for the system of interest, this control 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. 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.

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

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

Justification to Select: Regardless of whether the organization *intends* to use wireless access for the system of interest, this control 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. 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.

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.

Guidance: Regardless of whether the organization *intends* to use mobile devices as part of the system of interest, these controls 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.

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

## **AC-19(4), Access Control for Mobile Devices | Restrictions for Classified Information**

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.

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

Reference(s): EO 13526, Sec 4.1, para. (g); EO 13587, Sec 5.2, para. (a); CNSSD No. 510; CNSSP No. 17.

## **AC-20, Use of External 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 systems presents unique challenges for protecting classified information; AC-20 and its enhancements are needed to address these challenges.

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

## **AC-20(1), Use of External Systems | Limits on Authorized Use**

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 systems present unique challenges for protecting classified information; AC-20 enhancements are needed to address these challenges.

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

## **AC-20(2), Use of External Systems | Portable Storage Devices – Restricted Use**

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 systems present unique challenges for protecting classified information; AC-20 enhancements are needed to address these challenges.

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

## **AC-20(3), Use of External Systems | Non-Organizationally Owned System – Restricted Use**

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 systems present unique challenges for protecting classified information; AC-20 enhancements are needed to address these challenges.

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

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

## **AC-20(4), Use of External Systems | Network Accessible Storage Devices – Prohibited Use**

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 systems present unique challenges for protecting classified information; AC-20 enhancements are needed to address these challenges.

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

## **AC-21, Information Sharing**

Justification to Select: EO 13526 requires that classified information be accessible only to those with the appropriate clearance and need-to-know. Sharing information without conducting due diligence to ensure information products are appropriately marked, the recipients are authorized to access such information, and appropriate protections are in place can result in policy violations.

Guidance: Organizations need to define information sensitivity and classification level before sharing information from systems handling classified information. Protections commensurate with information sensitivity and classification level are essential for avoiding potential data spillage.

Reference(s): EO 13526, Sec 4.1.

## **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.

Guidance: This control has been identified as having privacy implementation considerations (see Table 1).

Reference(s): EO 13587, Sec. 2.1(b) and Sec 5.2; CNSSD No. 504.

## **AT-2, Literacy Awareness Training**

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

Guidance: 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 user has access to the system.

Parameter Value:

- a.1.: As part of initial training for new users and *annually for as long as the user has access to the system* thereafter;
- c.: Update literacy training and awareness content *at least annually* and following [Assignment: organization-defined events];

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

## **AT-2(2), Literacy Awareness Training | Insider Threat**

Justification to Select: CNSSD No. 504 requires, as part of an organization's insider threat program, insider threat awareness training to all cleared employees.

Reference(s): CNSSD No. 504.

## **AU-6, Audit Record 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. CNSSD No. 504 requires agencies to monitor and audit user activity on classified networks. Reviewing and analyzing audit records support the detection of insider threat activities.

Guidance: This control has been identified as having privacy implementation considerations (see Table 1).

Reference(s): EO 13587, Sec 2.1(b) and Sec 5.2; CNSSD No. 504.

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

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

Guidance: This control has been identified as having privacy implementation considerations (see Table 1).

Reference(s): White House Memorandum, *Minimum Standards for Executive Branch Insider Threat Programs*, Tab 2, Sec E.1.; CNSSD No. 504.

### **AU-6(5), Audit Record Review, Analysis, and Reporting | Integrated Analysis of Audit Records**

Justification to Select: The White House Memorandum, *Minimum Standards for Executive Branch Insider Threat Programs*, 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.

Guidance: This control has been identified as having privacy implementation considerations (see Table 1).

Parameter Value: Integrate analysis of audit records with the analysis of *vulnerability scanning information, performance data, system monitoring information, counterintelligence, security, cybersecurity, 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.

Reference(s): White House Memorandum, *Minimum Standards for Executive Branch Insider Threat Programs*, Tab 2, Sec E.1; CNSSD No. 504.

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

Justification to Select: CNSSD No. 504 requires organizations' insider threat programs to include full text analyses of all privileged user commands.

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; CNSSD No 504.

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

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. CNSSD No. 504 requires agencies to monitor and audit user activity on classified networks. Correlating audit records support the detection of insider threat activities.

Guidance: This control has been identified as having privacy implementation considerations (see Table 1).

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; CNSSD No. 504.

## AU-12, Audit Record 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.

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.; CNSSD No. 504.

## 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.

Guidance: This control has been identified as having privacy implementation considerations (see Table 1).

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; CNSSD No. 504.

## AU-16, Cross-Organizational Audit Logging

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.

Guidance: This control has been identified as having privacy implementation considerations (see Table 1).

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; CNSSD No. 504.

## AU-16(1), Cross-Organizational Audit Logging | Identity Preservation

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

Guidance: This control has been identified as having privacy implementation considerations (see Table 1).

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; CNSSD No. 504.

## AU-16(2), Cross-Organizational Audit Logging | Sharing of Audit Information

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

Guidance: This control has been identified as having privacy implementation considerations (see Table 1).

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

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; CNSSD No. 504.

## CA-3, Information Exchange

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) is the appropriate means to convey the expectations for the associated security requirements.

Guidance: For interconnections of systems processing classified information that serve to disseminate classified information outside the executive branch, the organization ensures the protection of the information in a manner equivalent to that provided within the executive branch using an ISA.

The organization prohibits the interconnection between classified and unclassified NSS unless using approved technologies (e.g., CDS) (see CDS Overlay for further guidance).

Parameter Value:

- a. Approve and manage the exchange of information between the system and other systems using *interconnection security agreements*;
- c. Review and update the agreements *at least annually or as changes to the systems or connections change*.

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

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

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 justification 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. Organizations must ensure that cryptographic mechanisms used to provide safeguarding of classified information from unauthorized access or modification are under configuration management.

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

## **CM-5(5), Access Restrictions for Change | Privilege Limitation for Production and Operation**

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 system components reduces the opportunities for insiders to grant access to classified information by unauthorized personnel.

Parameter Value: (b) Review and reevaluate privileges *at least quarterly*.

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, and other unauthorized disclosure. Uniquely identifying and authenticating users limits access to authorized users and is a foundational component of detecting potentially malicious insiders.

Guidance: This control has been identified as having privacy implementation considerations (see Table 1).

Reference(s): EO 13587, Sec 2.1 (b) and Sec 5.2 (a).

## **IA-2(1), Identification and Authentication (Organizational Users) | Multi-Factor Authentication to Privileged Accounts**

Justification to Select: Per NSM-8, agencies shall implement multifactor authentication and encryption for NSS data-at-rest and data-in-transit. CNSSD No. 504 Annex C requires that agencies implement standardized access control methodologies, specifically multifactor authentication for users with privileged roles.

Reference(s): NSM-8 Sec 1(b)(iii); CNSSD No. 504.

## **IA-2(2), Identification and Authentication (Organizational Users) | Multi-Factor Authentication to Non-Privileged Accounts**

Justification to Select: Per NSM-8, agencies shall implement multifactor authentication and encryption for NSS data-at-rest and data-in-transit. CNSSD No. 504 Annex A requires that agencies implement standardized access control methodologies, specifically multifactor authentication.

Reference(s): NSM-8 Sec 1(b)(iii); CNSSD No. 504.

## **IA-5(6), Authentication Management | Protection of Authenticators**

Justification to Select: CNSSP No. 25 requires NSA review and approval of PKI cryptographic components, to include tokens used for accessing Secret-level networks.

Guidance: In general, authenticators must be protected commensurate with the highest security classification of information on the system. Organizations should refer to the authoritative guidance to ensure compliance and understand how to appropriately protect authenticators. For hardware smart card-based tokens that users could use on Secret Internet Protocol Router Network (SIPRNet) workstations and still be carried by the user into unclassified spaces, NSA developed criteria that smart cards are required to meet to allow access to Secret data but be considered unclassified when not in use.

Reference(s): CNSSP No. 25.

## **IR-6, Incident Reporting**

Justification to Select: NSM-8 directs the reporting of known or suspected compromise or unauthorized access to NSS (including classified systems) to the National Manager.

Parameter Value:

- a. Require personnel to report suspected incidents to the organizational incident response capability within *2 hours*; and
- b. Report incident information to *the National Manager through the appropriate Federal Cyber Center or other designated central department point of contact (e.g., DoD CERT, IC CERT)*.

Reference(s): NSM-8, Sec 2(b).

## **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.

Guidance: CNSSP No. 18 and CNSSI No. 1001 provide guidance on additional actions that should be take when responding to classified information spills and should be followed when taking corrective action.

Parameter Value:

- a. Assigning, *at a minimum, information owner, the Information Assurance Manager (IAM)/Information System Security Manager (ISSM), the Activity Security Manager, and the responsible Incident Response Center (IRC)* with responsibility for responding to information spills
- c. Alerting *the information owner, the IAM/ISSM, the Activity Security Manager, and the responsible IRC* of the information spill using a method of communication not associated with the spill

Reference(s): EO 13526, Sec 4.1, para. (g); CNSSP No. 18; CNSSI No. 1001.

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

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.

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

## **IR-9(4), Information Spillage Response | Exposure to Unauthorized Personnel**

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.

Guidance: This control has been identified as having privacy implementation considerations (see Table 1).

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

## **MA-3(3), Maintenance Tools | Prevent Unauthorized Removal**

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.

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

## **MA-5(1), Maintenance Personnel | Individuals Without Appropriate Access**

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.

Guidance: This control has been identified as having privacy implementation considerations (see Table 1).

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.

Guidance: 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.

Reference(s): EO 13526, Sec. 4.1, para. (d); CNSSD No. 504.

## **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 be 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.

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

## **MP-3, Media Marking**

Justification to Select: EO 13526 requires organizations to mark classified information to reflect its classification. Marking refers to human readable labels, such as labels on thumb drives. (For labeling guidance, see AC-16.)

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:

- a. Physically control and securely store *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;*

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.

Parameter Value(s):

- a. Protect and control *digital and 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;*

Reference(s): EO 13526, Sec. 4.1, para. (d) and (g); EO 13587, Sec 5.2, para. (a).

## **MP-5(3), Media Transport | Custodians**

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.

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

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, helps to meet this requirement.

Parameter Value:

- a. Sanitize *all classified media* prior to disposal, release out of organizational control, or release for reuse using *approved sanitization techniques and procedures in accordance with applicable federal and organizational standards and policies*;

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

## **MP-6(1), Media Sanitization | Review, Approve, Track, Document, and Verify**

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, helps to meet this requirement.

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

## **MP-6(2), Media Sanitization | Equipment Testing**

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, helps to meet this requirement.

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

## **MP-6(3), Media Sanitization | Nondestructive Techniques**

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, helps to meet this requirement.

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.

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 retrieved or reconstructed.

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

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

## **MP-8(1), Media Downgrading | Documentation of Process**

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 retrieved or reconstructed.

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

## **MP-8(2), Media Downgrading | Equipment Testing**

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 retrieved or reconstructed.

Guidance: Testing of sanitization equipment and procedures should be conducted by qualified and authorized entities.

Parameter Value(s): Test downgrading equipment and procedures *at least annually* to ensure that downgrading actions being achieved.

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

## **MP-8(4), Media Downgrading | Classified Information**

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 retrieved or reconstructed.

Guidance: Downgrading of classified information requires use of approved sanitization tools, techniques, and procedures to ensure only confirmed unclassified information is moved from a classified system to unclassified media.

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

## **PE-2(3), Physical Access Authorizations | Restrict Unescorted Access**

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.

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 systems with components operating at different classification levels.

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

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

## **PE-3(2), Physical Access Control | Facility and Systems**

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.

Guidance: The organization monitors for unauthorized exfiltration of classified information.

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

### **PE-3(3), Physical Access Control | Continuous Guards**

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.

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

### **PE-4, Access Control for Transmission**

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.

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.

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

### **PE-19(1), Information Leakage | National Emissions Policies and Procedures**

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.

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

### **PE-22, Component Marking**

Justification to Select: EO 13526 requires organizations to establish procedures and controls to prevent access by unauthorized persons to classified information. Marking hardware components to indicate the classification level of information permitted to be processed, stored, or transmitted by the hardware component(s) is an organizational procedure that serves to remind users that classified information of the specified level exists within the system. Users should, as a result, be more aware and ready to guard

against access to hardware components by uncleared personnel passing through the facility.

Parameter Value(s): Mark *all system hardware components in facilities containing systems that process, store, or transmit classified information* indicating the impact level or classification level of the information permitted to be processed, stored, or transmitted by the hardware component.

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

## **PM-12, Insider Threat Program**

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.

Guidance: This control has been identified as having privacy implementation considerations (see Table 1).

Reference(s): EO 13587, Sec. 2.1(b) and Sec 5.2; CNSSD No. 504.

## **PS-3(1), Personnel Screening | Classified Information**

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.

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.

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.

Guidance: This control has been identified as having privacy implementation considerations (see Table 1).

Parameter Value: Upon termination of individual employment:

- a. Disable system access within *a time period as soon as possible but not to exceed 5 working days if termination is voluntary; if termination is involuntary, within same day as termination.*
- c. Conduct exit interviews that include a discussion of: *(i) prohibitions against the removal of classified information from the organization's control and (ii) the direction that information be declassified in order to remove it from the organization's control.*<sup>12</sup>

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

## **PS-4(1), Personnel Termination | Post-Employment Requirements**

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.

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

## **PS-6(2), Access Agreements | Classified Information Requiring Special Protection**

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.

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

## **PS-6(3), Access Agreements | Post-Employment Requirements**

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.

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

---

<sup>12</sup> 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-9, Position Descriptions**

Justification to Select: EO 13526 requires that classified information be accessible only to those with the appropriate clearance and need-to-know.

Guidance: Organizations should ensure that individual organizational roles and position descriptions clearly document and provide understanding regarding security or privacy responsibilities associated with the roles, as well as the role-based security and privacy training requirements for the roles. This should include roles and training for roles that require appropriate clearances and need-to-know.

Reference(s): EO 13526, Sec 4.1 para (a); EO 13764, Sec 1 para (a).

## **RA-3(2), Risk Assessment | Use of All-Source Intelligence**

Justification to Select: Organizations need to identify protections commensurate with an information's classification when developing agreements to share all-source intelligence information or resulting decisions with other organizations to assist in the analysis of risk.

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

## **RA-5, Vulnerability Monitoring and Scanning**

Justification to Select: Classified information may be more appealing to adversaries, who would want to take advantage of any vulnerabilities of a system that has classified information on it. Organizations with classified information on their systems should ensure vulnerability monitoring and scanning is implemented for its system components, ensuring that the potential sources of vulnerabilities—such as infrastructure components (e.g., switches, routers, firewalls, sensors), networked printers, scanners, and copiers—are not overlooked. This will allow organizations to ensure that any new vulnerabilities to systems that process, store, or transmit classified information are identified, mitigated, and reported as quickly as possible.

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

## **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.

Guidance: This control has been identified as having privacy implementation considerations (see Table 1).

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

## **RA-10, Threat Hunting**

Justification to Select: NSM-8 invokes EO 14028, which, in Section 7(b) requires deployment of an Endpoint Detection and Response (EDR) initiative to support proactive detection of cybersecurity incidents within Federal Government infrastructure, active cyber hunting, containment and remediation, and incident response.

Guidance: This control has been identified as having privacy implementation considerations (see Table 1).

Reference(s): NSM-8, Sec 1(e).

## **SA-3(2), System Development Life Cycle | Use of Live or Operational Data**

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 a test environment does not change its classification.

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

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

## **SA-4(6), Acquisition Process | Use of Information Assurance Products**

Justification to Select: EO 13526 directs the safeguarding of classified information while stored, processed, or when transmitted. The use of an NSA-approved cryptographic solution (e.g., Commercial Solutions for Classified program) protects the transmission of classified information when the network transmitting the information is at a lower classification level.

Reference(s): EO 13526, Sec. 4.1, para. (f) and (g); CNSSP No. 11.

## **SC-2, Separation of System and User Functionality**

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.

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.

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

## **SC-7(26), Boundary Protection | Classified National Security System Connections**

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 a system to an external network presents unique challenges for protecting classified information. An appropriate boundary protection device is needed to address these challenges. For interconnections of NSS operating at different classification levels, refer to the CDS Overlay.

Parameter Value: Prohibit the direct connection of a classified national security system to an external network without the use of *an appropriate boundary protection device*.

Reference(s): EO 13526, Sec 4.1, para. (g); EO 13587, Sec 5.2, 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. Per NSM-8, organizations are required to implement encryption for data-at-rest and data-in-transit.

Parameter Value: Protect the *confidentiality and integrity* of transmitted information.

Reference(s): EO 13526, Sec 4.1, para. (a), (f) and (g); EO 13587, Sec 5.2, para. (a); NSM-8, Sec 1(b)(iii).

## **SC-8(1), Transmission Confidentiality and Integrity | Cryptographic Protection**

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. Per NSM-8, organizations are required to implement encryption for data-at-rest and data-in-transit.

Parameter Value: Implement cryptographic mechanisms to *prevent unauthorized disclosure of classified information and detect changes to information during transmission.*

Reference(s): EO 13526, Sec 4.1, para. (a), (f) and (g); EO 13587, Sec 5.2, para. (a); NSM-8 Sec 1(b)(iii); CNSSP No. 15; NSM-8, Sec 1(b)(iii).

### **SC-8(3), Transmission Confidentiality and Integrity | Cryptographic Protection for Message Externals**

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. Per NSM-8, organizations are required to implement encryption for data-at-rest and data-in-transit.

Reference(s): EO 13526, Sec 4.1, para. (a), (f) and (g); EO 13587, Sec 5.2, para. (a); CNSSP No. 15; NSM-8, Sec 1(b)(iii).

### **SC-8(4), Transmission Confidentiality and Integrity | Conceal or Randomize Communications**

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.

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

### **SC-12, Cryptographic Key Establishment and Management**

Justification to Select: CNSSP No. 15 requires the use of NSA-approved cryptography to protect NSS and the information that resides in the system. Per NSM-8, organizations are required to implement encryption for data-at-rest and data-in-transit.

Guidance: NSM-8 requires all organizations use NSA-approved, public-standards-based cryptographic protocols to ensure widespread cryptographic interoperability among NSS. If mission-unique requirements preclude the use of public standards-based cryptographic protocols, NSA-approved mission unique protocols may be used.

This control has been identified as having privacy implementation considerations (see Table 1).

Parameter Value: Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: *for classified NSS, employ NSA-approved cryptographic guidance addressing processes/requirements for key generation, distribution, storage, access, and destruction.*

Reference(s): NSM-8 Sec 1 (b) (iv); CNSSP No. 15.

## **SC-12(2), Cryptographic Key Establishment and Management | Symmetric Keys**

Justification to Select: CNSSP No. 15 requires the use of NSA-approved cryptography to protect NSS and the information that resides in the system. Per NSM-8, organizations are required to implement encryption for data-at-rest and data-in-transit.

Parameter Value: Produce, control, and distribute symmetric cryptographic keys using *NSA-approved key management technology and processes.*

Reference(s): NSM-8 Sec 1 (b) (iv); CNSSP No. 15.

## **SC-12(3), Cryptographic Key Establishment and Management | Asymmetric Keys**

Justification to Select: CNSSP 15 requires the use of NSA-approved cryptography to protect NSS and the information that resides in the system. Per NSM-8, organizations are required to implement encryption for data-at-rest and data-in-transit.

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

Parameter Value: Produce, control, and distribute asymmetric cryptographic keys using *NSA-approved key management technology and processes.*

Reference(s): NSM-8 Sec 1 (b) (iv); CNSSP No. 15; 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:

- b. Implement the following types of cryptography required for each specified cryptographic use: *NSA-approved cryptography for protecting classified information from access by personnel who lack the necessary security clearance.*

Reference(s): EO 13526, Sec. 4.1, para. (f) and (g); CNSSP No. 15.

### **SC-15(3), Collaborative Computing Devices and Applications | Disabling and Removal in Secure Work Areas**

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.

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 work areas, it is necessary to verify that all personnel have valid authorizations to access classified information and to disable or remove collaborative devices that are at a lower classification level than the secure work area. Disabling lower classification collaborative devices is necessary to prevent unauthorized access to classified information (e.g., through eavesdropping).

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. Per NSM-8, organizations are required to implement encryption for data-at-rest and data-in-transit.

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: Protect the *confidentiality and integrity* of the following information at rest: *classified information at rest*.

Reference(s): EO 13526, Sec 4.1, para. (f); EO 13587, Sec 5.2, para. (a); NSM-8 Sec 1 (b) (iii).

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

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. Per NSM-8, organizations are required to implement encryption for data-at-rest and data-in-transit.

Reference(s): EO 13526, Sec 4.1, para. (f) and (g); EO 13587, Sec 5.2, para. (a); NSM-8 Sec 1(b)(iii).

## **SC-41, Port and I/O Device Access**

Justification to Select: CNSSD No. 504 requires the implementation of trusted network connection restrictions to prevent malicious users from exploiting known vulnerabilities of hard-linking to areas outside of their authorized access, Injecting code, and covering their activities. This control supports holistic endpoint security requirements.

Reference(s): EO 13526, Sec 4.1, para. (f) and (g); CNSSD No. 504.

## **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, and 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.

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.

This control has been identified as having privacy implementation considerations (see Table 1).

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

## **SI-4(14), System Monitoring | Wireless Intrusion Detection**

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, and other unauthorized disclosure. Monitoring wireless networks for unauthorized use is necessary to protect classified information as it identifies unsanctioned connections and potential information leaks.

Guidance: This control has been identified as having privacy implementation considerations (see Table 1).

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

### **SI-4(19), System Monitoring | Risk for Individuals**

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.

Guidance: This control has been identified as having privacy implementation considerations (see Table 1).

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

### **SI-4(21), System Monitoring | Probationary Periods**

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.

Guidance: This control has been identified as having privacy implementation considerations (see Table 1).

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

## **SR-3, Supply Chain Controls and Processes**

Justification to Select: EO 13873 requires the USG to protect against supply chain risks from foreign adversaries, reducing the probability of adversaries successfully identifying and targeting the supply chain, and limiting harm that can be done by unauthorized persons to classified information.

Reference(s): EO 13873 Sec. 1.a.; EO 14032; CNSSD No. 505.

### **SR-3(2), Supply Chain Controls and Processes | Limitation of Harm**

Justification to Select: EO 13873 requires the USG to protect against supply chain risks from foreign adversaries, reducing the probability of adversaries successfully identifying and targeting the supply chain, and limiting harm that can be done by unauthorized persons to classified information.

Reference(s): EO 13873 Sec. 1.a.; CNSSD No. 505.

## **SR-4, Provenance**

Justification to Select: EO 13873 requires the USG to protect against supply chain risks from foreign adversaries, reducing the probability of adversaries successfully identifying and targeting the supply chain, and limiting harm that can be done by unauthorized persons to classified information.

Reference(s): EO 13873 Sec. 1.a.; EO 14032; CNSSD No. 505.

## **SR-7, Supply Chain Operations Security**

Justification to Select: EO 13873 requires continual assessment of threats to the United States from information and communications technology or services designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary. Operational Security (OPSEC) controls support organizational ability to conduct such assessment as part of protecting their supply chains and preventing unauthorized persons access to classified information.

Reference(s): EO 13873 Sec. 5; CNSSD No. 505.

## **SR-12, Component Disposal**

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, helps to meet this requirement. Proper disposal is required to prevent unauthorized reuse.

Parameter Value: Dispose of *all digital and non-digital system media containing classified information* using the following techniques and methods: *approved methods in accordance with the classification of the information processed*.

Reference(s): EO 13526, Sec 4.1, para. (g); CNSSD No. 505.

## **7. Implementation Considerations**

Organizations should consider the following control guidance when implementing specific system capabilities on systems used to process classified information.

Controls that do not warrant selection or exclusion for safeguarding classified information require further consideration when systems containing classified information employ these controls (e.g., part of a baseline, part of another overlay, tailoring decision) to ensure safeguarding considerations related to that control are adequately addressed. For example, AC-18, which discusses use of wireless access, is not mandatory for systems storing, processing,

or transmitting classified information. However, when AC-18 is implemented for systems that contain classified information, organizations must consider how to implement this control in a way that properly protects classified information.

### **AC-18(1), Wireless Access | Authentication and Encryption**

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

If this control applies/is selected, please see EO 13526, Sec 4.1, para. (d), (f) and (g) and CNSSP No. 17.

### **AC-18(5), Wireless Access | Antennas and Transmission Power Levels**

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

If this control applies/is selected, please see EO 13526, Sec 4.1, para. (d), (f) and (g) and CNSSP No. 17.

### **AC-19(5), Access Control for Mobile Devices | Full Device or Container-Based Encryption**

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

If this control applies/is selected, please see EO 13526, Sec 4.1, para. (f) and (g); EO 13587, Sec 5.2, para. (a); and CNSSP No. 17 for guidance.

### **SA-9(8), External System Services | Processing and Storage Location – U.S. Jurisdiction**

Guidance: If the organization intends to process and store classified information on an external system, outside of the United States, then the geographic location must be restricted to facilities located within in the legal jurisdictional boundary of the United States and this control must be selected.

If this control applies/is selected, please refer to EO 13526, Sec 4.1, para. (f) and (g) and CNSSP No. 32.

## **SI-20, Tainting**

Guidance: If the organization intends to implement capabilities on its systems or system components to determine if organizational data has been exfiltrated or improperly removed (whether passively or actively, or from adversaries or unintended user procedures) from the organization, this control must be selected.

If this control applies/is selected, please refer to EO 13526, Sec 4.1, para. (f) and (g).

## **8. Definitions**

The terms used in this overlay are all defined in CNSSI No. 4009, *CNSS Glossary*, or one of the other references listed in Section 2 of this document.