CNSSI No. 1253
29 July 2022

CATEGORIZATION AND CONTROL SELECTION FOR NATIONAL SECURITY SYSTEMS

THIS INSTRUCTION PRESCRIBES MINIMUM STANDARDS
YOUR DEPARTMENT OR AGENCY MAY REQUIRE FURTHER
IMPLEMENTATION

NATIONAL MANAGER

FOREWORD

1. The Committee on National Security Systems (CNSS) Instruction No. 1253, *Categorization and Control Selection for National Security Systems*, provides all Federal Government departments, agencies, bureaus, and offices with guidance on the Categorize and Select steps of the Risk Management Framework (RMF) for national security systems (NSS). This Instruction builds on and is a companion document to National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 Revision 2, *Risk Management for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, NIST SP 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, and NIST SP 800-53B, *Control Baselines for Information Systems and Organizations*. Recognizing the close relationship between security and privacy, both NIST and CNSS incorporated a privacy control baseline to provide further guidance on identifying and protecting personally identifiable information (PII) processed by NSS. This Instruction should be used by information systems security and privacy engineers, authorizing officials, senior information security officers, senior agency officials for privacy and their designees, and others to select and agree upon appropriate protections for an NSS.

2. The authority to issue this Instruction is derived from National Security Directive 42, *National Policy for the Security of National Security Telecommunications and Information Systems*, which outlines the roles and responsibilities for securing NSS, consistent with applicable law, Executive Order 12333, *United States Intelligence Activities*, as amended, and other Presidential directives. Nothing in this Instruction shall alter or supersede the authorities of the Director of National Intelligence.

3. CNSSI No. 1253 appendices will be reviewed and updated, as required, to reflect changes to protect NSS.

4. All CNSS member organizations should be aware that overlays are published independently as attachments to Appendix E of this Instruction. Organizations should periodically check the CNSS site for new or updated overlays.

5. This Instruction supersedes CNSSI No. 1253 dated March 27, 2014.

6. This Instruction may be obtained from the CNSS website: https://www.cnss.gov.

FOR THE NATIONAL MANAGER

/s/

Robert E. Joyce

Deputy National Manager for National Security Systems

CNSS Secretariat. National Security Agency. 9800 Savage Road, STE 6716. Ft Meade, MD 20755-6716
Office: (410) 854-6805 CNSS@nsa.gov

TABLE OF CONTENTS

TABLE OF FIGURES AND TABLES

1. INTRODUCTION

The CNSS has worked with representatives from the Civil, Defense, and Intelligence Communities, as part of the Joint Task Force Transformation Initiative Working Group to produce a unified information security and privacy framework. As a result of this collaboration, NIST published the following six transformational documents[1]:

- NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments;*
- NIST SP 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy;*
- NIST SP 800-39 Revision 1, *Managing Information Security Risk: Organization, Mission, and Information System View*;
- NIST SP 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations*;
- NIST SP 800-53A Revision 5, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans;* and
- NIST SP 800-53B, *Control Baselines for Information Systems and Organizations*.

The intent of this unified framework is to improve information security and privacy, strengthen risk management processes, and encourage reciprocity among federal agencies.

1.1 Purpose and Scope

The CNSS collaborates with NIST to ensure NIST SP 800-37, NIST SP 800-53, and NIST SP 800-53B address security and privacy safeguards to meet the requirements of NSS[2] to the extent possible and provide a common foundation for information security and privacy across the United States (U.S.) Federal Government. CNSSI No. 1253 is a companion document to the NIST publications relevant to the RMF Steps, Categorize and Select (i.e., NIST SP 800-37; NIST SP 800-53[3]; NIST SP 800-53B; NIST SP 800-60, Volume I, *Guide for Mapping Types of Information and Information Systems to Security Categories*; NIST SP 800-60, Volume II, *Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories*; and Federal Information Processing Standards Publication [FIPS] 199, *Standards for Security Categorization of Federal Information and Information Systems*).

CNSSI No. 1253 provides the security and privacy control baselines for NSS[4]. This Instruction also provides NSS-specific information on tailoring, developing, and applying overlays for the

[1] Unless otherwise stated, currently published versions of NIST documents are referenced.

[2] NIST SP 800-59, *Guidelines for Identifying an Information System as a National Security System*, provides guidelines developed in conjunction with the Department of Defense (DoD), including the National Security Agency, for identifying an information system as a national security system. The basis for these guidelines is the Federal Information Security Modernization Act of 2014 (Title III, Public Law 113-283, December 18, 2014), which defines the phrase "national security system," and provides government-wide requirements for information security.

[3] NIST SP 800-53 Revision 5 incorporates new control families for Program Management (PM), Personally Identifiable Information Processing and Transparency (PT), and Supply Chain Risk Management (SR) into its control catalog.

[4] Consistent with NIST SP 800-53B, CNSSI No. 1253 uses the baseline control selection approach to provide predefined sets of controls for consistency across the national security community.

national security community, and parameter values for NIST SP 800-53 controls that are applicable to all NSS.

CNSSI No. 1253 applies to all NSS. For NSS, where differences between the NIST documentation and this Instruction occur, this Instruction takes precedence.

1.2 Differences Between CNSSI No. 1253 and NIST Publications

The major differences between this Instruction and the NIST publications relevant to the RMF Steps Categorize and Select are:

- This Instruction does not adopt the high-water mark (HWM) concept from FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, for categorizing NSS (see Section 2.1).
- The associations of confidentiality, integrity, and/or availability to controls in NSS baselines are explicitly defined in this Instruction (see Appendix D, Tables D-1 through D-20).
- The use of control overlays as defined in this Instruction is consistent with NIST SP 800-53B but is specific to the national security community (see Section 2.4 and Appendix E).
- The NSS privacy control baseline represents the privacy controls necessary for an agency to manage enterprise privacy risks.
- Controls specific to systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of (collectively referred to as "process")[5] PII have been removed from the NIST privacy control baseline and incorporated into the Privacy Overlays. The determination whether a system processes PII and whether the Privacy Overlay applies must be approved by the Senior Agency Official for Privacy (SAOP) or designee.
- Tables D-1 through D-20 in Appendix D include a Privacy Implementation Considerations column that identifies controls not included in the NSS privacy control baseline, but if such controls are implemented, they may introduce privacy risks and so require coordination with the SAOP or designee.

[5] See NIST SP 800-53, Revision 5, Chapter 2.4, Security and Privacy Controls.

2. THE FUNDAMENTALS

This chapter presents the fundamental concepts associated with categorization and control selection.

2.1 Adoption of NIST SP 800-37, NIST SP 800-53, NIST SP 800-53B, and FIPS 199

The CNSS adopts NIST SP 800-37[6], as documented in this Instruction, for the national security community. The focus of this Instruction is on the RMF Categorize and Select steps.[7] These steps are informed by activities conducted during the Prepare step. The Prepare step identifies tasks at the organization level[8] that produce artifacts (e.g., organization risk management strategy, organizationally tailored control baselines, common controls that may be inherited by organizational systems, an organization-wide strategy for monitoring control effectiveness) and decisions that could impact Categorize and Select activities and decisions. Similarly, the Prepare step identifies tasks at the system level[9] that will impact Categorize and Select activities and decisions (e.g., identifying information types, including any information types with PII). As a result, those individuals with the responsibilities of categorizing a system or selecting controls must be aware of and incorporate the decisions made during the Prepare step. Decisions and actions at the system level should be shared with organizational stakeholders as those decisions and actions may impact organizational risk management decisions.

The CNSS adopts NIST SP 800-53[10] and NIST SP 800-53B, as documented in this Instruction, for the national security community. The CNSS adopts FIPS 199, establishing the security category for NSS with three discrete components: one impact level (low, moderate, or high) for each of the three security objectives (confidentiality, integrity, and availability). Preserving the three discrete components, rather than using the FIPS 200 HWM, provides specificity in allocating controls to baselines and reduces the need for subsequent tailoring (see Appendix D Tables D-1 through D-20.

2.2 Privacy Risk in NSS

Personally identifiable information (PII) processed in systems (such as in mission or administrative systems or resident in audit logs) creates privacy risk. All organizations have some systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of (collectively referred to as "process") PII; therefore, privacy risk must be addressed at both the organizational and system levels. Failure to address privacy risk can cause individuals and organizations to experience other types of risk (e.g., psychological, reputational, financial, legal, compliance, operational security, and mission) as well as loss of trust and impact to information sharing and missions. Increasingly, failure to properly protect or manage PII may result in

[6] See CNSSP No. 22, *Cybersecurity Risk Management*, Annex A, for applicability of NIST publications.

[7] The seven RMF Steps are Prepare, Categorize, Select, Implement, Assess, Authorize, and Monitor.

[8] RMF Prepare tasks P-1 through P-7.

[9] RMF Prepare tasks P-8 through P-18.

[10] See CNSSP No. 22, *Cybersecurity Risk Management*, Annex A, for applicability of NIST publications.

misuse of PII data sets (e.g., leveraging credentials of a legitimate user for adversarial purposes causing harm to national security interests, the organization, or individuals).

While security and privacy are independent and separate disciplines, they are closely related. It is essential for organizations to take a coordinated approach to identifying and managing security and privacy risks and complying with applicable requirements. Security controls are the safeguards or countermeasures employed within a system or an organization to protect the confidentiality, integrity, and availability of the system and its information and to manage information security risk. Privacy controls are the administrative, technical, and physical safeguards employed within a system or an organization to manage privacy risks and to ensure compliance with applicable privacy requirements.

2.3 Relationship Between Security and Privacy Control Baselines

For organizations to effectively manage security and privacy risks, the security and privacy control baselines are implemented together. Security and privacy programs must collaborate throughout the organization's RMF implementation, especially where their objectives overlap. This collaboration will help ensure organizations have the information they need to make informed security and privacy decisions.

The security and privacy control baselines, documented in Appendix D Tables D-1 through D-20, include controls and control enhancements that address risks that arise from the loss of confidentiality, integrity, and availability for systems and information (including PII) as well as controls and control enhancements that manage privacy responsibilities under Federal Information Security Modernization Act (FISMA), Office of Management and Budget (OMB) Circular A-130, and designated Federal Information Processing Standards (FIPS) as well as privacy risks to individuals.

The security and privacy control baselines are not mutually exclusive. Some controls address both privacy risks and security risks. Similarly, within the security control baselines, a control may address a confidentiality risk, an integrity risk, an availability risk, or any combination of the three.

2.3.1 Privacy Implementation Considerations

It is possible for organizations to introduce unintended privacy risk when implementing security controls. Coordination between the cybersecurity and privacy officials is an effective means to identify and address any such unintended risks at the earliest opportunity and improve cybersecurity and privacy decision making. The new Privacy Implementation Considerations column in Appendix D (Tables D-1 through D-20) is intended to manage this risk. This column identifies controls that are not included in the privacy control baseline but may introduce privacy risk if selected to meet security objectives.[11] If a control is selected that includes a checkmark in the Privacy Implementation Considerations column, the system owner must confer with the

[11] For example, control PE-6(3) "Monitoring Physical Access: Video Surveillance" addresses employing video surveillance for the purpose of subsequent review. This control is not required for the privacy control baseline, but there are privacy implications to filming individuals' physical activities and behavior. If such controls are selected, the SAOP or designee must be consulted before implementation.

SAOP, or designee, to address any privacy risks and mitigation considerations that may arise from implementing controls listed under privacy implementation considerations. Controls with checkmarks are a starting point for discussions between the AO and SAOP or their designees.

2.4 Assumptions Related to Control Baselines

Assumptions related to control baselines are intended to represent a majority of federal systems and serve as the basis to justify the allocation of controls in the baselines. While some federal systems do not share these characteristics, it is more efficient for organizations to start with a baseline and tailor it to meet the needs of those systems. Systems or environments that diverge from the assumptions listed below must tailor their control set to compensate for the differences in assumptions, through application of an overlay, system-specific tailoring of selected controls and enhancements, or both.

This Instruction accepts all assumptions from NIST SP 800-53B by adopting the NIST security and privacy control baselines[12] as the foundation for the NSS baselines defined in Appendix D Tables D-1 through D-20. The NIST SP 800-53B assumptions are:

- Information in organizational systems is relatively persistent.
- Organizational systems are multi-user (either serially or concurrently) in operation.
- Some information in organizational systems is not shareable with other users who have authorized access to the same systems.
- Organizational systems exist in networked environments and are general purpose in nature.
- Organizations have the necessary structure, resources, and infrastructure to implement the controls.

This Instruction also addresses additional assumptions through the NSS baselines. The NSS baselines are not intended to address these assumptions completely, but rather to a degree that represents the minimal protection that should be provided. The additional assumptions are:

- Insider threats exist within NSS organizations.
- Advanced persistent threats (APTs) are targeting NSS and may already exist within NSS.
- Additional best practices beyond those defined in the NIST baselines are necessary to protect NSS.

If any of the above assumptions are not valid, the control selections must be revisited to ensure the selected controls are appropriate for the environment of use and associated threats consistent with the results of organization- and system-level risk assessments. See Section 2.6, Tailoring Guidance.

[12] See NIST SP 800-53B, Chapter 3, The Control Baselines.

These situations are specifically not addressed in the NSS baselines:

- Classified information is processed, stored, or transmitted by organizational systems.[13]
- Select information requires specialized protection based on federal law, directives, regulations, or policies.[14]
- Organizational systems need to communicate with other systems across different security domains.[15]

Overlays specific to these and other situations may be available and should be applied as part of the tailoring process, as appropriate. Additional information on overlays is available in Appendix E.

2.5 Relationship Between Baselines and Overlays

NSS baselines are a combination of NIST SP 800-53B baselines and the NIST SP 800-53 controls appropriate for NSS. The NSS baselines constitute a starting point in the process of determining the controls needed for a particular system prior to system-specific tailoring. NSS security control baselines represent the controls necessary to address the impact should there be a loss of confidentiality, integrity, or availability, as reflected by the system's security categorization. The NSS privacy control baseline represents the privacy controls necessary for an agency to manage enterprise privacy risks.

Overlays are a set of controls and a form of bulk tailoring agreed to by subject matter experts. Overlays are applied to address divergence from the assumptions used to create the NSS baselines (see Section 2.4), when specific controls are needed to protect a particular technology, or to address particular threats or additional requirements when processing certain types of information. The need to apply an overlay is determined by answering the applicability questions in each overlay. Overlays may or may not be baseline independent. Baseline independent overlays can be applied to any NSS baseline. As a result, there may be overlap of controls between an NSS baseline and controls identified in an overlay(s).[16]

2.5.1 Relationship between Privacy Control Baseline and Privacy Overlays

Privacy is the only focus area for which there is a control baseline as well as a set of overlays available for organizations to use. Like the NSS security control baselines, the NSS privacy control baseline is applicable to all NSS to manage organizational PII risks. Unlike the privacy control baseline, the Privacy Overlays address system-specific privacy risks and are applicable only to systems that process PII (e.g., PII is identified during the Categorize step [see Section 3.1.1]).

[13] Refer to the Classified NSS Overlay.

[14] This includes overlays such as the Space Platform Overlay, Privacy Overlays, and Intelligence (INT) Overlays.

[15] Refer to the Cross Domain Solutions (CDS) Overlay.

[16] If the use of multiple overlays results in conflicts between the application and removal of security controls, see Section 3.2. for guidance.

- All systems will implement the NSS privacy control baseline to manage organizational PII risks.
- Systems that process[17] PII will implement both the NSS Privacy Control Baseline and the appropriate Privacy Overlay.

While some systems may be designed specifically to process PII, in other systems PII may appear in unexpected ways, such as the administration of user accounts or logs of how individuals utilized the system. For systems that do not process PII, and do not have user accounts or associated logs, the NSS privacy control baseline will be sufficient. In instances in which the system processes PII, is designed to process PII, or the organization determines it must utilize the user account and associated logs for accountability, security, and/or counterintelligence purposes, then a Privacy Overlay must be applied. The SAOP or designee must approve the determination as to whether a system does or does not process PII. Similarly, if the organization determines it must employ one of the controls designated as having a privacy implementation consideration, the SAOP or designee must be consulted to determine if additional steps are required to protect privacy.

It is important to note that decisions made regarding sufficiency of security and privacy controls cannot be made once and assumed to be unchangeable for the entire system life cycle. As a system's usage evolves over time, additional data collection, data aggregation, changes in use, or other factors may necessitate the implementation of additional security and privacy controls. This may also include the application of a more stringent privacy overlay. Maintaining communications between security and privacy experts is essential to ensuring privacy information is appropriately protected over the life of the system and its information.

2.6 Tailoring Guidance

NSS are exposed to different threats than non-NSS influenced by such factors as the nature of the missions they support, areas where NSS are deployed, and users who have access. As a result, tailoring is a critical activity to ensure informed risk management decisions reflect safeguards needed to support an organization's ability to execute its mission.

The baselines are a starting point designed to address a typical system, as described in the assumptions (see Section 2.4). Few systems completely align with those assumptions; therefore, tailoring is necessary to address differences specific to those systems or technologies and to ensure risks specific to the mission, system, information, and environment are appropriately identified and mitigated.

Controls, regardless of source (baseline or overlays), may be tailored unless required to meet legislative, regulatory, or policy requirements. A control may be tailored out if there is no risk for which the control is designed to mitigate. For situations where there is risk and the baseline control cannot be implemented, compensating controls may be appropriate.[18] All tailoring decisions must be defensible based on mission and business needs, a sound rationale, and explicit

[17] Processing PII is defined by NIST as "create, collect, use, process, store, maintain, disseminate, disclose, or dispose of." See NIST SP 800-53, Revision 5, Chapter 2.4, Security and Privacy Controls.

[18] For additional guidance, see NIST SP 800-53B Section 2.4 "Tailoring Control Baselines."

risk-based determinations. All decisions, to include the justification for the decision, must be documented in the system security and privacy plan(s) and/or the plan of action and milestones to ensure senior officials are able to make risk-informed decisions.

Controls may not be tailored out due to inability to satisfy a control (e.g., resource constraints). These controls are still applicable and need to be documented for risk management decisions.

Tailoring decisions may be influenced by inputs such as an organization's risk management strategy, organizational risk assessments, current threat information, environment of operation, business impact analysis or criticality analysis.[19]

The NSS control baselines in Appendix D Tables D-1 through D-20 provide additional factors to consider during tailoring. These factors are presented in the Tailoring Considerations columns and include Assurance, Resiliency, and ATT&CK. Assurance is the measure of confidence in the security or privacy capability provided by the controls; it is the grounds for justified confidence that a security or privacy claim has been or will be achieved. Resiliency is the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruption. Resiliency includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents. MITRE ATT&CK®[20] is a globally accessible curated knowledge base of adversary tactics and techniques based on real-world observations. A checkmark in the column indicates the factor applies to the corresponding control. If more assurance and/or resiliency is desired but those assurance- or resiliency-related controls are not in the baseline, organizations may consider tailoring them in. Conversely, before tailoring out assurance- or resiliency-related controls or controls mapped to ATT&CK, organizations may consider how doing so will impact assurance, resiliency, or the ability to respond to adversary tactics and techniques.

[19] See NIST SP 800-37 RMF tasks P-3 (Risk Assessments – Organizations) and S-2 (Control Tailoring) for more information.

[20] For more information, see attack.mitre.org.

3. THE CATEGORIZE AND SELECT PROCESSES

This chapter describes the processes of categorization and security control selection. Except where the guidance in this document differs from that in NIST SP 800-37, the national security community will implement the RMF Categorize and Select steps consistent with NIST SP 800-37. It is advantageous to include individuals with risk decision making responsibilities, such as an AO (or AO's designee) and the SAOP (or designee), in Categorize and Select decisions to ensure the appropriate set of controls are identified and applied to a system, and are consistent with the results of risk assessments, risk management strategies, and organizational mission and business objectives.

3.1 RMF Step: Categorize

For NSS, the Security Categorization task (Task C-2) is to:

1. Determine security impact levels: (i) for the information type(s)[21] processed, stored, transmitted, or protected by the system; and (ii) for the system.
2. Retain the three impact levels of Low, Moderate, or High for each security objective (i.e., confidentiality, integrity, and availability).

When determining impact levels, each organization must be consistent with the impact levels established by the information owner. Information owners may not reside in the organization that owns and/or operates the system, and there may be multiple information owners associated with a system. All information owners must be identified to provide inputs to this activity. Each information owner sets the impact level for their information type. See Section 2.2 for a discussion about privacy risk in NSS.

Sections 3.1.1 and 3.1.2 provide the activities to complete system categorization.

3.1.1 Determine Impact Levels for Information Types

To determine impact levels for information types, the following activities are completed:

1. Identify all types of information processed, stored, or transmitted by the system, including whether the information is PII. The determination whether a system processes PII must be approved by the SAOP or designee.
2. Determine each information type's provisional security impact level, and adjust the information types' provisional security impact levels (see FIPS 199, NIST SP 800-60, Volume I, Section 4, and NIST SP 800-60, Volume II[22]). If the system processes PII, the provisional security impact levels may need to be adjusted to address PII impact levels.[23] If the information type is not identified in NIST SP 800-60 Volume II, document the information type consistent with the guidance in NIST SP 800-60, Volume I.

---

[21] An information type is a specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor-sensitive, security management), defined by an organization or, in some instances, by a public law, executive order, directive, policy, or regulation. Reference FIPS 199 and NIST SP 800-60, Volume 1.

[22] NIST SP 800-60 Volume II does not address specific national security or mission information, but impact levels can be set for that information using the approach documented in NIST SP 800-60 Volume I.

[23] The Privacy Overlays discuss the different impact levels of PII.

3.1.2 Determine Impact Levels for the System

Once the potential security impact level for each information type on the system is determined, the overall high water mark for each security objective must be determined which is the security categorization for the system. To do this:

1. For each security objective, determine the overall high water mark for information types on the system (see FIPS 199) and make any necessary adjustments (see NIST SP 800-160, Volume I, Section 4.4.2). This results in three distinct high water marks, one for each security objective (confidentiality, integrity, and availability), shown as a trigraph categorization (e.g., L-L-L, M-M-H). The security categorization of a system must not be changed or modified to reflect management decisions to allocate more stringent or less stringent security controls. The tailoring guidance in Section 3.2.2 should be used to address these issues.
2. Document the security categorization results in the security plan.
3. Obtain the SAOP's, or designee's, approval of the security categorization for systems that process PII.
4. Obtain AO's or AO's designated representative's approval of the security categorization.

3.2 RMF Step: Select

The RMF Select step is consistent with the guidance in NIST SP 800-37. For NSS, the additional guidance here focuses on the first two tasks under the Select Step:

1. Task S-1, Control Selection
2. Task S-2, Control Tailoring

3.2.1 Task S-1, Control Selection

Once the security categorization of the system is determined, organizations begin the control selection process. To select an NSS baseline, the following activities are completed:

1. Select the NSS security control baseline contained in Appendix D Tables D-1 through D-20 corresponding to the security categorization of the system (i.e., the impact levels determined for each security objective [confidentiality, integrity, and availability]).
2. Include the NSS privacy control baseline contained in Appendix D Tables D-1 through D-20, which is a default for all NSS.
3. As appropriate, coordinate with privacy program officials or representatives to ensure privacy risk is addressed as informed by the Privacy Implementation Considerations column in Tables D-1 through D-20 in Appendix D.

3.2.2 Task S-2, Control Tailoring

The tailoring process is used to modify and align an NSS baseline to account for conditions affecting the specific system (e.g., conditions related to organizational missions/business functions, systems, types of technology, or environments of operation). During the tailoring process, a risk assessment – either informal or formal – should be conducted. The results from a

risk assessment provide information about the necessity and sufficiency of controls and enhancements during the tailoring process.

To tailor a selected NSS baseline, the following activities must be completed:

1. Apply any applicable overlay(s). To determine applicability of an overlay, refer to the questions provided in the Applicability section of each overlay document. The SAOP or designee must approve the determination as to whether a system processes PII and whether the Privacy Overlay applies.
2. If the use of multiple overlays results in conflicts between the application or removal of security or privacy controls, the AO (or designee) and SAOP (or designee), in coordination with the information owner/steward, information system owner, and risk executive (function) resolve the conflict.
3. Use tailoring guidance from Section 2.6 and NIST SP 800-53B, Section 2.4 to:
    a. Identify and designate common controls, and the common control provider(s)
    b. Apply scoping considerations:
        i. Control implementation, applicability, and placement considerations
        ii. Operational and environmental considerations
        iii. Technology considerations
        iv. Mission and business considerations
        v. Security objective considerations
        vi. Legal and policy considerations
    c. Select compensating controls if baseline controls cannot be implemented
    d. Assign values to organization-defined control parameters
    e. Supplement baselines with additional controls and control enhancements
    f. Provide specification information for control implementation[24]
4. Use risk assessments, established risk tolerances, or other risk information (e.g., privacy risk assessments if appropriate) to inform tailoring. Evaluate the baseline controls to determine if there are any controls that do not address risks faced by the system; controls that may unnecessarily increase complexity, long term maintenance and assessment costs; or controls that may result in decreased trustworthiness and assurance. Controls should be removed only because of risk-based determinations and not because of an inability to implement a control.

[24] Since controls and control enhancements are statements of security or privacy functions or capabilities that are conveyed at higher levels of abstraction, the controls may lack sufficient information for implementation. Therefore, additional details may be necessary to fully define the intent of a given control for implementation purposes and to ensure the security and privacy requirements related to that control are satisfied.

5. Determine if additional assurance-related controls are needed to increase the level of trustworthiness in the system. If so, tailor the set of controls accordingly. (Refer to Appendix D Tables D-1 through D-20 and NIST SP 800-53 Appendix C.)
6. Document in the security and privacy plans the relevant decisions made during the tailoring process, providing a sound risk-based rationale for those decisions.
7. Document and justify in the security and privacy plans any controls from the selected NSS baseline that cannot or will not be implemented in the system and for which no compensating control(s) will be substituted. This information, and the associated risks, must also be included in the corresponding plan of action and milestones.

The security and privacy plans, including all tailoring decisions, must be approved by the AO (security plan) and the SAOP (privacy plan) or their designees.

Appendix A References

LAWS, POLICIES, DIRECTIVES, REGULATIONS, MEMORANDA, STANDARDS, AND GUIDELINES

Appendix A provides the references used within CNSSI No. 1253.

Laws and Executive Orders

- 44 U.S.C. § 3552, January 2012.
- Federal Information Security Modernization Act, P.L. 113-283 § 2(a), December 2014.
- The Privacy Act of 1974, 5 U.S.C. § 552a.
- Executive Order 12333, *United States Intelligence Activities,* December 4, 1981.
- Executive Order 13526, *Classified National Security Information,* December 29, 2009.
- Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, 7 October 2011.
- National Security Directive 42, *National Policy for the Security of National Security Telecommunications and Information Systems*, July 1990.
- National Security Memorandum 8 (NSM-8), *Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems*, January 2022.

Regulations, Directives, Plans, and Policies

- Office of Management and Budget Circular No. A-130, *Managing Information as a Strategic Resource*, 28 July 2016.

National Institute of Standards and Technology (NIST) Standards and Special Publications (SP)

- Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.
- Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.
- NIST SP 800-30, *Guide for Conducting Risk Assessments,* September 2012.
- NIST SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, December 2018.
- NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, March 2011.

- NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, September 2020.[25]
- NIST SP 800-53A, Revision 5, *Assessing Security and Privacy Controls in Information Systems and Organizations*, January 2022.
- NIST SP 800-53B, *Control Baselines for Information Systems and Organizations*, October 2020.[26]
- NIST SP 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003.
- NIST SP 800-60, Revision 1, *Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008.
- NIST SP 800-60, Revision 1, *Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008.
- NIST SP 800-160, Volume 1, *Systems Security Engineering - Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, March 2018.[27]
- NIST SP 800-160, Volume 2, Revision 1, *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*, December 2021.

CNSS Issuances

- CNSS Directive (CNSSD) No. 504, *Directive on Protecting National Security Systems from Insider Threat*, September 2021.
- CNSSD No. 505, *Supply Chain Risk Management (SCRM)*, November 2021.
- CNSS Instruction (CNSSI) No. 1015, *Enterprise Audit Management Instruction for National Security Systems (NSS)*, September 2013.
- CNSSI No. 4009, *Committee on National Security Systems (CNSS) Glossary*, March 2022.
- CNSS Policy (CNSSP) No. 11, *Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products*, June 2013.
- CNSSP No. 15, *Use of Public Standards for Secure Information Sharing*, October 2016.
- CNSSP No. 17, *Policy on Wireless Systems*, January 2014.
- CNSSP No. 22, *Cybersecurity Risk Management Policy*, September 2021.
- 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.
- CNSS White Paper, *Security-Focused Configuration Management*, April 2014.

[25] Includes errata update as of 10 December 2020.

[26] Includes errata update as of 10 December 2020.

[27] Includes errata update as of 21 March 2020.

Appendix B Glossary

COMMON TERMS AND DEFINITIONS

The terms in this document are defined in the NIST Joint Task Force Transformation Initiative Working Group documents and CNSSI No. 4009, except for those listed below.

NSS baselines [CNSSI No. 4009, Adapted]	The combination of NIST SP 800-53B baselines (represented by an "X") and the NIST SP 800-53 security and privacy controls appropriate for NSS (represented by a "+" or a "--").
NSS Best Practice	A method or technique that has been generally accepted by the national security community to address an identified risk as the standard way of safeguarding NSS; the method or technique must be implementable, replicable, transferable, and adaptable across national security systems or missions.
Control Extension	A statement, used in control overlays, that extends the basic capability of a control by specifying additional functionality, altering the strength mechanism, or adding or limiting implementation options.

Appendix C Acronyms and Abbreviations

The acronyms and abbreviations used in this Instruction are included below.

AO	Authorizing Official
APT	Advanced Persistent Threat
CDS	Cross Domain Solution
CIO	Chief Information Officer
CISO	Chief Information Security Officer (see also SISO, SAISO)
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
DoD	Department of Defense
E.O.	Executive Order
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
FOUO	For Official Use Only
HWM	High Water Mark
ISSO	Information System Security Officer
ISSM	Information System Security Manager
NIST	National Institute of Standards and Technology
NSM	National Security Memorandum
NSS	National Security System
OMB	Office of Management and Budget
PII	Personally Identifiable Information
P.L.	Public Law

PV	Parameter Value
RMF	Risk Management Framework
SAISO	Senior Agency Information Security Officer (see also CISO, SISO)
SAOP	Senior Agency Official for Privacy
SISO	Senior Information Security Officer (see also CISO, SAISO)
SP	Special Publication
SWG	Safeguarding Working Group
U.S.	United States
U.S.C.	United States Code

Appendix D NSS Control Baselines and Supporting Information

Tables D-1 through D-20 identify controls included in the NIST SP 800-53B baselines plus the additional controls needed to protect NSS. The tables contain the following columns:

- **ID** – NIST control identifier (combination of abbreviated family identifier and control number); new NIST SP 800-53 Revision 5 controls are indicated by salmon shading.
- **Title** – Name of the control or enhancement.
- **Privacy Control Baseline** – Controls indicated with an "X" or a "+" in this column are required for all NSS.
- **Privacy Implementation Considerations** – Controls that if selected to meet a security objective may have a privacy impact and require coordination with the SAOP or designee to address privacy considerations prior to implementation. Checkmarks in this column include a subscripted number(s) that correlate to implications to consider when implementing the control. The controls indicated in this column impact privacy risk in that:
    1. Close coordination between security and privacy is needed to manage privacy risks
    2. Design choices may mitigate privacy risks
    3. Implementation choices may create unintended privacy risks
    4. PII should not flow through or into a system that is not authorized to process PII
- **Security Control Baselines Confidentiality (C)/Integrity (I)/Availability (A)** – Columns showing the association of a control to the security objective (confidentiality, integrity, availability) and at what impact level (low, moderate, high) based on inclusion of an “X” or a “+”.
- **Justification for NSS** – Controls selected to address NSS assumptions identified by a “+” include a justification for what NSS need the control is intended to address (e.g., Insider Threat[28], Advanced Persistent Threat [APT], NSS Best Practice). No justification is provided for any other controls (i.e., those with an “X” or a blank cell).
- **Parameter Value** – Contains minimum values specified for NSS; parameter values not appropriate for CNSS to define for all NSS are not included. Parameter values apply to both privacy and security baselines.
- **Tailoring Considerations** – Columns for Assurance (control or control enhancement contributes to the confidence that a security claim has been or will be achieved as noted in NIST SP 800-53 Tables C-1 through C-20), Resiliency (control or control enhancement contributes to supporting resiliency of the system [i.e., desired effects on

[28] See CNSSD No. 504, *Directive on Protecting NSS from Insider Threat*, for more information.

threats per NIST SP 800-160 Vol 2]); and ATT&CK (control is identified in the mapping as a resource to assess control coverage against real-world threats[29]). For more information on the use and benefit of tailoring considerations, see Section 2.6.

Symbols used in Tables D-1 through D-20 include:

- "X": Identifies applicability of NIST SP 800-53B baselines for NSS.
- "+": Identifies a control needed to protect NSS and therefore added to the NSS baselines.
- "--": Identifies a control selected for NIST baseline (security or privacy) but not selected for an NSS baseline (security or privacy). Privacy controls selected for a NIST baseline but not selected for an NSS baseline are specific to systems that process PII and are addressed in the Privacy Overlay. Any control can still be selected during tailoring if needed.
- Blank space: A control not selected for a baseline nor allocated to a particular security objective; no parameter value specific to NSS is provided for the control; or the control is not applicable to an Assurance, Resiliency, or ATT&CK mapping. If not indicated with an "X" or "+", the control may still be selected during the tailoring process.
- "√": Identifies applicability of a control to Privacy Implementation Considerations, Assurance, Resiliency, or ATT&CK.

Controls that are designated as "Withdrawn" indicate they are no longer in the NIST SP 800-53 control catalog.[30] Withdrawn controls are indicated by italicized font as well as either light gray shading (control withdrawn in NIST SP 800-53 Revision 4) or dark gray shading (control withdrawn in NIST SP 800-53 Revision 5).

Association of NIST Controls to Confidentiality, Integrity, and Availability: The security objectives of confidentiality, integrity, and availability are defined in 44 United States Code (U.S.C.), Section 3552. The NIST SP 800-53B baselines do not characterize controls as having relationships with security objectives. Tables D-1 through D-20 associate the controls from NIST SP 800-53, Revision 5, with the three security objectives for only those controls included in NSS baselines which can be used to inform tailoring decisions.

Parameter values specified for NSS: The parameter values are defined to flow within the control text, and their placement/position within the control is noted since the entirety of the control text is not included. For example, 2nd PV indicates the value being provided is for the second parameter value within the control text. Where controls contain multiple paragraphs (e.g., a., b., c.) and possibly subparagraphs within those paragraphs (e.g., a.1., a.2, a.3), then the paragraph/subparagraph to which the value applies is provided. If a control has a parameter value in paragraph a. and paragraph c. for which values are being provided, but no parameter value to define for paragraph b., then the notation will only identify paragraph a. and c. and will not contain a reference to paragraph b. Where multiple values may be defined within a paragraph or

[29] The Center for Threat-Informed Defense (Center) developed a set of mappings between ATT&CK and NIST SP 800-53 with supporting documentation and resources. This mapping is available at: https://github.com/center-for-threat-informed-defense/attack-control-framework-mappings.

[30] Changes to the control catalog are under the authority of NIST.

subparagraph, their position will be noted using 1st PV or 2nd PV as appropriate. If the parameter value contains no annotation regarding its placement, then this indicates there is only one value to define for the control and annotation of its placement within the control is not needed. It should be noted that sometimes a parameter value begins with the word "a" which should not be confused with a paragraph annotation of "a."

If a control or control enhancement does not include a parameter value in the tables below, then:

- The control language does not have a parameter value to define;
- The control language has a parameter value, but it is not appropriate for CNSS to define the parameter value for all NSS; or
- The control language has a parameter value, but the control is not in any NSS baseline, so CNSS does not define the parameter value.

Organizations may address a parameter value in organizational policy if the policy meets or exceeds the NSS-defined parameter value.

Table D-1: Access Control (AC) Family

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
AC-1	**Policy and Procedures**	X		X	X	X	X	X	X	X	X	X		c.1., c.2. 1st PV: at least annually	√		
AC-2	**Account Management**			X	X	X	X	X	X					h.1. 24 hours h.2. 24 hours h.3. 24 hours j. at least quarterly			√
AC-2(1)	Automated System Account Management				X	X		X	X								
AC-2(2)	Automated Temporary and Emergency Account Management				X	X		X	X					1st PV: disable 2nd PV: not to exceed 72 hours			
AC-2(3)	Disable Accounts				X	X		X	X					1st PV: not to exceed 72 hours d. 90 days			
AC-2(4)	Automated Audit Actions			+	X	X	+	X	X				Insider Threat CNSSI No. 1015				
AC-2(5)	Inactivity Logout			+	X	X	+	X	X	+	X	X	Insider Threat	it is the end of a user's standard work period			

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
AC-2(6)	Dynamic Privilege Management															√	
AC-2(7)	Privileged User Accounts			+	+	+	+	+	+				Insider Threat CNSSI No. 1015				
AC-2(8)	Dynamic Account Management															√	
AC-2(9)	Restrictions on Use of Shared and Group Accounts			+	+	+	+	+	+				Insider Threat				
AC-2(10)	***Shared and Group Account Credential Termination***	***Withdrawn***															
AC-2(11)	Usage Conditions					X			X			X					
AC-2(12)	Account Monitoring for Atypical Usage		√3	+	+	X	+	+	X				Insider Threat			√	
AC-2(13)	Disable Accounts for High-Risk Individuals			+	X	X	+	X	X				Insider Threat	1st PV: 30 minutes			
AC-3	**Access Enforcement**			X	X	X	X	X	X								√
AC-3(1)	*Restricted Access to Privileged Functions*	*Withdrawn*															

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
AC-3(2)	Dual Authorization															√	
AC-3(3)	Mandatory Access Control																
AC-3(4)	Discretionary Access Control			+	+	+	+	+	+				NIST Assumption: Some user data/information in organizational information systems is not shareable with other users who have authorized access to the same systems.				
AC-3(5)	Security-Relevant Information																
AC-3(6)	*Protection of User and System Information*	*Withdrawn*															
AC-3(7)	Role-Based Access Control															√	
AC-3(8)	Revocation of Access Authorizations																
AC-3(9)	Controlled Release																
AC-3(10)	Audited Override of Access Control Mechanisms																

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
AC-3(11)	Restrict Access to Specific Information Types															√	
AC-3(12)	Assert and Enforce Application Access															√	
AC-3(13)	Attribute-Based Access Control															√	
AC-3(14)	Individual Access	--											Privacy implementation is specific to systems with PII				
AC-3(15)	Discretionary and Mandatory Access Control																
AC-4	**Information Flow Enforcement**		√4		X	X		X	X								√
AC-4(1)	Object Security and Privacy Attributes		√4														
AC-4(2)	Processing Domains		√4													√	
AC-4(3)	Dynamic Information Flow Control		√4													√	
AC-4(4)	Flow Control of Encrypted Information		√4			X			X								
AC-4(5)	Embedded Data Types		√4														

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
AC-4(6)	Metadata		√4														
AC-4(7)	One-Way Flow Mechanisms																
AC-4(8)	Security and Privacy Policy Filters		√4													√	
AC-4(9)	Human Reviews		√4														
AC-4(10)	Enable and Disable Security or Privacy Policy Filters		√4														
AC-4(11)	Configuration of Security or Privacy Policy Filters		√4														
AC-4(12)	Data Type Identifiers															√	
AC-4(13)	Decomposition into Policy-Relevant Subcomponents																
AC-4(14)	Security or Privacy Policy Filter Constraints		√4														
AC-4(15)	Detection of Unsanctioned Information																
AC-4(16)	*Information Transfers on Interconnected Systems*	*Withdrawn*															
AC-4(17)	Domain Authentication															√	

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
AC-4(18)	*Security Attribute Binding*	*Withdrawn*															
AC-4(19)	Validation of Metadata																
AC-4(20)	Approved Solutions																
AC-4(21)	Physical or Logical Separation of Information Flows															√	
AC-4(22)	Access Only																
AC-4(23)	Modify Non-Releasable Information																
AC-4(24)	Internal Normalized Format																
AC-4(25)	Data Sanitization																
AC-4(26)	Audit Filtering Actions																
AC-4(27)	Redundant/Independent Filtering Mechanisms															√	
AC-4(28)	Linear Filter Pipelines																
AC-4(29)	Filter Orchestration Engines															√	

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
AC-4(30)	Filter Mechanisms Using Multiple Processes															√	
AC-4(31)	Failed Content Transfer Prevention																
AC-4(32)	Process Requirements for Information Transfer																
AC-5	**Separation of Duties**			+	X	X	+	X	X				Insider Threat				√
AC-6	**Least Privilege**			+	X	X	+	X	X				Insider Threat Consistent with CM-5(5)			√	√
AC-6(1)	Authorize Access to Security Functions			+	X	X	+	X	X				Insider Threat			√	
AC-6(2)	Non-Privileged Access for Non-Security Functions			+	X	X	+	X	X				Insider Threat APT	privileged functions		√	
AC-6(3)	Network Access to Privileged Commands					X			X							√	
AC-6(4)	Separate Processing Domains															√	
AC-6(5)	Privileged Accounts			+	X	X	+	X	X				Insider Threat APT			√	
AC-6(6)	Privileged Access by Non-Organizational Users															√	

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
AC-6(7)	Review of User Privileges			+	X	X	+	X	X				Insider Threat			√	
AC-6(8)	Least Privilege Levels for Code Execution			+	+	+	+	+	+				APT			√	
AC-6(9)	Log Use of Privileged Functions		√3	+	X	X	+	X	X				Insider Threat APT CNSSI No. 1015				
AC-6(10)	Prohibit Non-Privileged Users from Executing Privileged Functions			+	X	X	+	X	X				Insider Threat APT			√	
AC-7	**Unsuccessful Logon Attempts**			X	X	X	X	X	X	X	X	X		b. notify system administrator			√
AC-7(1)	*Automatic Account Lock*	*Withdrawn*															
AC-7(2)	Purge or Wipe Mobile Device																
AC-7(3)	Biometric Attempt Limiting																
AC-7(4)	Use of Alternate Authentication Factor															√	
AC-8	**System Use Notification**	+		X	X	X	X	X	X				Ensure security and privacy collaborate on notice content				√

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
AC-9	**Previous Logon Notification**																
AC-9(1)	Unsuccessful Logons																
AC-9(2)	Successful and Unsuccessful Logons																
AC-9(3)	Notification of Account Changes																
AC-9(4)	Additional Logon Information																
AC-10	**Concurrent Session Control**				+	X		+	X		+	X	Insider Threat APT	1st PV: all accounts 2nd PV: maximum of 3 sessions			√
AC-11	**Device Lock**			+	X	X	+	X	X				Insider Threat	a. initiating a device lock after a period not to exceed 30 minutes; requiring the user to initiate a device lock before leaving the system unattended			√
AC-11(1)	Pattern-Hiding Displays			+	X	X							Insider Threat				
AC-12	**Session Termination**			+	X	X	+	X	X				NSS Best Practice			√	√

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
AC-12(1)	User-Initiated Logouts			+	+	+	+	+	+				NSS Best Practice NIST Assumption: Some user data/information in organizational information systems is not shareable with other users who have authorized access to the same systems.	all resources			
AC-12(2)	Termination Message			+	+	+	+	+	+				NSS Best Practice				
AC-12(3)	Timeout Warning Message																
AC-13	*Supervision and Review — Access Control*	*Withdrawn*															
AC-14	**Permitted Actions Without Identification or Authentication**			X	X	X	X	X	X								√
AC-14(1)	*Necessary Uses*	*Withdrawn*															
AC-15	*Automated Marking*	*Withdrawn*															
AC-16	**Security and Privacy Attributes**				+	+		+	+				NSS Best Practice	f. 2nd PV: 90 days			√
AC-16(1)	Dynamic Attribute Association																

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
AC-16(2)	Attribute Value Changes by Authorized Individuals																
AC-16(3)	Maintenance of Attribute Associations by System																
AC-16(4)	Association of Attributes by Authorized Individuals																
AC-16(5)	Attribute Displays on Objects to be Output																
AC-16(6)	Maintenance of Attribute Association				+	+		+	+				NSS Best Practice				
AC-16(7)	Consistent Attribute Interpretation				+	+		+	+				NSS Best Practice				
AC-16(8)	Association Techniques and Technologies																
AC-16(9)	Attribute Reassignment - Regrading Mechanism																
AC-16(10)	Attribute Configuration by Authorized Individuals																
AC-17	**Remote Access**			X	X	X	X	X	X								√
AC-17(1)	Monitoring and Control			+	X	X	+	X	X				Insider Threat				

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
AC-17(2)	Protection of Confidentiality and Integrity Using Encryption			+	X	X	+	X	X				NSS Best Practice				
AC-17(3)	Managed Access Control Points			+	X	X	+	X	X				NSS Best Practice				
AC-17(4)	Privileged Commands and Access			+	X	X	+	X	X				NSS Best Practice				
AC-17(5)	*Monitoring for Unauthorized Connections*	*Withdrawn*															
AC-17(6)	Protection of Mechanism Information			+	+	+							NSS Best Practice				
AC-17(7)	*Additional Protection for Security Function Access*	*Withdrawn*															
AC-17(8)	*Disable Nonsecure Network Protocols*	*Withdrawn*															
AC-17(9)	Disconnect or Disable Access			+	+	+	+	+	+				APT				
AC-17(10)	Authenticate Remote Commands					+			+				NSS Best Practice				
AC-18	**Wireless Access**			X	X	X	X	X	X								√
AC-18(1)	Authentication and Encryption			+	X	X	+	X	X				NSS Best Practice	users and devices			

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
AC-18(2)	*Monitoring Unauthorized Connections*	*Withdrawn*															
AC-18(3)	Disable Wireless Networking			+	X	X	+	X	X				NSS Best Practice				
AC-18(4)	Restrict Configurations by Users			+	+	X	+	+	X				Insider Threat				
AC-18(5)	Antennas and Transmission Power Levels					X			X								
AC-19	**Access Control for Mobile Devices**			X	X	X	X	X	X								√
AC-19(1)	*Use of Writable and Portable Storage Devices*	*Withdrawn*															
AC-19(2)	*Use of Personally Owned Portable Storage Devices*	*Withdrawn*															
AC-19(3)	*Use of Portable Storage Devices with No Identifiable Owner*	*Withdrawn*															
AC-19(4)	Restrictions for Classified Information																
AC-19(5)	Full Device or Container-Based Encryption			+	X	X	+	X	X				NSM-8	2nd PV: all mobile computers/devices that process organization data			

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
AC-20	**Use of External Systems**			X	X	X	X	X	X								√
AC-20(1)	Limits on Authorized Use			+	X	X	+	X	X				NSS Best Practice				
AC-20(2)	Portable Storage Devices — Restricted Use			+	X	X							Insider Threat APT				
AC-20(3)	Non-Organizationally Owned Systems — Restricted Use			+	+	+	+	+	+				Insider Threat APT				
AC-20(4)	Network Accessible Storage Devices — Prohibited Use																
AC-20(5)	Portable Storage Devices — Prohibited Use																
AC-21	**Information Sharing**				X	X											√
AC-21(1)	Automated Decision Support																
AC-21(2)	Information Search and Retrieval		√3														
AC-22	**Publicly Accessible Content**			X	X	X								d. quarterly or as new information is posted			
AC-23	**Data Mining Protection**		√3		+	+							Insider Threat			√	√

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
AC-24	**Access Control Decisions**																
AC-24(1)	Transmit Access Authorization Information																
AC-24(2)	No User or Process Identity																
AC-25	**Reference Monitor**														√		

Table D-2: Awareness and Training (AT) Family

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
AT-1	**Policy and Procedures**	X		X	X	X	X	X	X	X	X	X		a. all personnel c.1., c.2. 1st PV: at least annually	√		
AT-2	**Literacy Training and Awareness**	X		X	X	X	X	X	X	X	X	X		a.1. at least annually	√		
AT-2(1)	Practical Exercises														√	√	
AT-2(2)	Insider Threat			X	X	X	X	X	X	X	X	X			√		
AT-2(3)	Social Engineering and Mining			+	X	X	+	X	X	+	X	X	Insider Threat Consistent with CM-5(5)		√	√	
AT-2(4)	Suspicious Communications and Anomalous System Behavior			+	+	+	+	+	+	+	+	+	Insider Threat Consistent with CM-5(5)		√		
AT-2(5)	Advanced Persistent Threat			+	+	+	+	+	+	+	+	+	Insider Threat APT		√	√	
AT-2(6)	Cyber Threat Environment					+			+			+	APT		√		
AT-3	**Role-Based Training**	X		X	X	X	X	X	X	X	X	X		a.1. at least annually	√		

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
AT-3(1)	Environmental Controls			+	+	+	+	+	+	+	+	+	NSS Best Practice	2nd PV: at least annual	√		
AT-3(2)	Physical Security Controls			+	+	+	+	+	+	+	+	+	Insider Threat	2nd PV: at least annual (NOTE: Significant changes to physical security systems may drive more frequent training.)	√		
AT-3(3)	Practical Exercises														√	√	
AT-3(4)	***Suspicious Communications and Anomalous System Behavior***	***Withdrawn***															
AT-3(5)	Processing Personally Identifiable Information	X												2nd PV: at least annual	√		
AT-4	**Training Records**	X		X	X	X	X	X	X	X	X	X			√		
AT-5	*Contacts with Security Groups and Associations*	*Withdrawn*															

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
AT-6	**Training Feedback**	+				+			+			+	Feedback informs future training NSS Best Practice	1st PV: at least annually or upon discovery of a security incident or privacy breach 2nd PV: employee's supervisor and organizational cybersecurity and privacy officials	√		

Table D-3: Audit and Accountability (AU) Family

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
AU-1	**Policy and Procedures**	X		X	X	X	X	X	X	X	X	X		a. all personnel c.1., c.2. 1st PV: at least annually	√		
AU-2	**Event Logging**	X		X	X	X	X	X	X					a. See the set of auditable events or activities specified in CNSSI No. 1015.			
AU-2(1)	*Compilation of Audit Records from Multiple Sources*	*Withdrawn*															
AU-2(2)	*Selection of Audit Events by Component*	*Withdrawn*															
AU-2(3)	***Reviews and Updates***	***Withdrawn***															
AU-2(4)	*Privileged Functions*	*Withdrawn*															
AU-3	**Content of Audit Records**		√1	X	X	X	X	X	X								
AU-3(1)	Additional Audit Information		√1	+	X	X	+	X	X				CNSSI No. 1015				

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
AU-3(2)	*Centralized Management of Planned Audit Record Content*	*Withdrawn*															
AU-3(3)	Limit Personally Identifiable Information Elements	X															
AU-4	**Audit Log Storage Capacity**									X	X	X					
AU-4(1)	Transfer to Alternate Storage		$\sqrt{}_2$							+	+	+	Insider Threat				
AU-5	**Response to Audit Logging Process Failures**		$\sqrt{}_1$							X	X	X		a. 2nd PV: near real time			
AU-5(1)	Storage Capacity Warning									+	+	X	Insider Threat CNSSI No. 1015	3rd PV: maximum of 75%			
AU-5(2)	Real-Time Alerts											X		3rd PV: minimally but not limited to: auditing software/hardware errors; failures in the audit capturing mechanisms; and audit storage capacity being reached or exceeded			
AU-5(3)	Configurable Traffic Volume Thresholds															√	

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
AU-5(4)	Shutdown on Failure																
AU-5(5)	Alternate Audit Logging Capability																
AU-6	**Audit Record Review, Analysis, and Reporting**		√1	X	X	X	X	X	X					a. 1st PV: at least weekly (seven days)	√	√	
AU-6(1)	Automated Process Integration		√2	+	X	X	+	X	X				CNSSI No. 1015		√		
AU-6(2)	*Automated Security Alerts*	*Withdrawn*															
AU-6(3)	Correlate Audit Record Repositories		√3	+	X	X	+	X	X				APT Insider Threat CNSSI No. 1015		√	√	
AU-6(4)	Central Review and Analysis		√2	+	+	+	+	+	+				CNSSI No. 1015		√		
AU-6(5)	Integrated Analysis of Audit Records		√2			X			X						√	√	
AU-6(6)	Correlation with Physical Monitoring		√2			X			X						√	√	
AU-6(7)	Permitted Actions		√2												√		

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
AU-6(8)	Full Text Analysis of Privileged Commands														√	√	
AU-6(9)	Correlation with Information from Nontechnical Sources		√3												√	√	
AU-6(10)	***Audit Level Adjustment***	***Withdrawn***															
AU-7	**Audit Record Reduction and Report Generation**				X	X		X	X						√		
AU-7(1)	Automatic Processing				X	X		X	X						√		
AU-7(2)	***Automatic Sort and Search***	***Withdrawn***															
AU-8	**Time Stamps**						X	X	X								
AU-8(1)	***Synchronization with Authoritative Time Source***	***Withdrawn***															
AU-8(2)	***Secondary Authoritative Time Source***	***Withdrawn***															
AU-9	**Protection of Audit Information**	+		X	X	X	X	X	X	X	X	X	Preserve accountability of system use				

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
AU-9(1)	Hardware Write-Once Media															√	
AU-9(2)	Protection of Audit Store on Separate Physical Systems or Components					X			X			X		at least weekly		√	
AU-9(3)	Cryptographic Protection								X							√	
AU-9(4)	Access by Subset of Privileged Users						+	X	X				Insider Threat				
AU-9(5)	Dual Authorization								+				Insider Threat	2nd PV: any audit information		√	
AU-9(6)	Read-Only Access							+	+		+	+	Insider Threat			√	
AU-9(7)	Store on Component with Different Operating System															√	
AU-10	**Non-Repudiation**	+						+	X				Preserve accountability of system use Insider Threat		√		
AU-10(1)	Association of Identities		√2												√		

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
AU-10(2)	Validate Binding of Information Producer Identity		√2												√	√	
AU-10(3)	Chain of Custody		√2												√		
AU-10(4)	Validate Binding of Information Reviewer Identity		√2												√		
AU-10(5)	*Digital Signatures*	*Withdrawn*															
AU-11	**Audit Record Retention**	X								X	X	X		the time period identified in the current National Archives and Records Administration (NARA) General Records Schedules (GRS)			
AU-11(1)	Long-Term Retrieval Capability		√3							+	+	+	NSS Best Practice	a retention of capability to access audit records for the duration of the required retention period	√		
AU-12	**Audit Record Generation**	+		X	X	X	X	X	X				Ensure security and privacy collaboration	a. all information systems and network components			
AU-12(1)	System-Wide and Time-Correlated Audit Trail						+	+	X				Insider Threat CNSSI No. 1015	2nd PV: organizational tolerance defined in AU-8			

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
AU-12(2)	Standardized Formats																
AU-12(3)	Changes by Authorized Individuals		√2	+	+	X	+	+	X				Insider Threat				
AU-12(4)	Query Parameter Audits of Personally Identifiable Information		√2														
AU-13	**Monitoring for Information Disclosure**		√1												√	√	
AU-13(1)	Use of Automated Tools		√3												√		
AU-13(2)	Review of Monitored Sites		√3												√		
AU-13(3)	Unauthorized Replication of Information														√	√	
AU-14	**Session Audit**		√1	+	+	+	+	+	+				Insider Threat		√		
AU-14(1)	System Start-Up			+	+	+	+	+	+				Insider Threat		√		
AU-14(2)	***Capture and Record Content***	***Withdrawn***															

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
AU-14(3)	Remote Viewing and Listening		√2	+	+	+							Insider Threat		√		
AU-15	*Alternate Audit Logging Capability*	*Withdrawn*															
AU-16	**Cross-Organizational Audit Logging**		√4					+	+				Insider Threat				
AU-16(1)	Identity Preservation		√2					+	+				Insider Threat				
AU-16(2)	Sharing of Audit Information		√2					+	+				Insider Threat				
AU-16(3)	Disassociability		√3														

Table D-4: Assessment, Authorization, and Monitoring (CA) Family

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
CA-1	**Policies and Procedures**	X		X	X	X	X	X	X	X	X	X		c.1., c.2. 1st PV: at least annually	√		
CA-2	**Control Assessments**	X		X	X	X	X	X	X	X	X	X		d. at least annually, or as stipulated in the organization's continuous monitoring program	√		√
CA-2(1)	Independent Assessors		√3	+	X	X	+	X	X	+	X	X	Insider Threat		√		
CA-2(2)	Specialized Assessments		√3			X			X			X			√		
CA-2(3)	Leveraging Results from External Organizations														√		
CA-3	**Information Exchange**			X	X	X	X	X	X						√		
CA-3(1)	***Unclassified National Security System Connections***	***Withdrawn***															
CA-3(2)	***Classified National Security System Connections***	***Withdrawn***															

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
CA-3(3)	***Unclassified Non-National Security System Connections***	***Withdrawn***															
CA-3(4)	***Connections to Public Networks***	***Withdrawn***															
CA-3(5)	***Restrictions on External System Connections***	***Withdrawn***															
CA-3(6)	Transfer Authorizations				+	X		+	X				Insider Threat APT		√		
CA-3(7)	Transitive Information Exchanges														√		
CA-4	*Security Certification*	*Withdrawn*															
CA-5	**Plan of Action and Milestones**	X		X	X	X	X	X	X	X	X	X			√		
CA-5(1)	Automation Support for Accuracy and Currency														√		

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
CA-6	**Authorization**	X		X	X	X	X	X	X	X	X	X		e. commensurate with the risk to the information in the system and at least every three (3) years (unless the organization and/or system is adequately covered by a continuous monitoring program and has transitioned to ongoing authorizations), when significant security breaches occur, or whenever there is a significant change to the system or to the environment in which the system operates.	√		
CA-6(1)	Joint Authorization — Intra-Organization														√		
CA-6(2)	Joint Authorization — Inter-Organization														√		
CA-7	**Continuous Monitoring**	X		X	X	X	X	X	X	X	X	X			√		√
CA-7(1)	Independent Assessment				X	X		X	X		X	X			√		

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A							
				L	M	H	L	M	H	L	M	H			Assurance	Resiliency	ATT&CK
CA-7(2)	*Types of Assessments*	*Withdrawn*															
CA-7(3)	Trend Analysis			+	+	+	+	+	+	+	+	+	Insider Threat		√	√	
CA-7(4)	Risk Monitoring	X		X	X	X	X	X	X	X	X	X			√		
CA-7(5)	Consistency Analysis			+	+	+	+	+	+	+	+	+	NSS Best Practice		√	√	
CA-7(6)	Automation Support for Monitoring				+	+		+	+		+	+	NSS Best Practice		√	√	
CA-8	**Penetration Testing**					X			X			X			√	√	√
CA-8(1)	Independent Penetration Testing Agent or Team					X			X			X			√	√	
CA-8(2)	Red Team Exercises														√	√	
CA-8(3)	Facility Penetration Testing					+			+			+	Insider Threat		√	√	
CA-9	**Internal System Connections**			X	X	X	X	X	X					d. at least annually	√		
CA-9(1)	Compliance Checks														√		

Table D-5: Configuration Management (CM) Family

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
CM-1	**Policies and Procedures**	X		X	X	X	X	X	X					c.1., c.2. 1st PV: at least annually	√		
CM-2	**Baseline Configuration**						X	X	X					b.1. at least annually	√		√
CM-2(1)	***Reviews and Updates***	***Withdrawn***															
CM-2(2)	Automation Support for Accuracy and Currency							X	X						√		
CM-2(3)	Retention of Previous Configurations							X	X					at least two	√		
CM-2(4)	***Unauthorized Software***	***Withdrawn***															
CM-2(5)	***Authorized Software***	***Withdrawn***															
CM-2(6)	Development and Test Environments														√		
CM-2(7)	Configure Systems and Components for High-Risk Areas							X	X						√	√	

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
CM-3	**Configuration Change Control**						+	X	X				Enables continuous monitoring Insider Threat	e. 1 year or two change cycles of baseline configurations as defined in CM-2(3), whichever is longer	√		√
CM-3(1)	Automated Documentation, Notification, and Prohibition of Changes								X						√		
CM-3(2)	Testing, Validation, and Documentation of Changes							X	X						√		
CM-3(3)	Automated Change Implementation																
CM-3(4)	Security and Privacy Representatives						+	X	X				Consistent with CM-3	1st PV: at a minimum, the cybersecurity representative as a voting member 2nd PV: configuration control element defined in CM-3.g.			
CM-3(5)	Automated Security Response								+				CNSS White Paper, "Security-Focused Configuration Management"				

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
CM-3(6)	Cryptography Management						+	+	X				Insider Threat	all controls that rely on cryptography			
CM-3(7)	Review System Changes						+	+	+				Insider Threat CNSS White Paper, "Security-Focused Configuration Management"	1st PV: annually for Low Integrity, quarterly for Moderate Integrity, and monthly for High Integrity 2nd PV: there is an incident or once planned changes have been performed			
CM-3(8)	Prevent or Restrict Configuration Changes								+				NSS Best Practice (avoids denial of service)	when the configuration change may adversely impact operations or mission (e.g., exercises, real world operations)			
CM-4	**Impact Analyses**	X					X	X	X						√		
CM-4(1)	Separate Test Environments							+	X				NSS Best Practice		√	√	
CM-4(2)	Verification of Controls							X	X						√		
CM-5	**Access Restrictions for Change**						X	X	X								√

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
CM-5(1)	Automated Access Enforcement and Audit Records							+	X				Insider Threat				
CM-5(2)	***Review System Changes***	***Withdrawn***															
CM-5(3)	***Signed Components***	***Withdrawn***															
CM-5(4)	Dual Authorization															√	
CM-5(5)	Privilege Limitation for Production and Operation						+	+	+				Insider Threat Consistent with AC-6	5.b. at least annually		√	
CM-5(6)	Limit Library Privileges						+	+	+				Insider Threat APT			√	
CM-5(7)	*Automatic Implementation of Security Safeguards*	*Withdrawn*															

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
CM-6	**Configuration Settings**		√2				X	X	X					a. organizationally approved guides such as DoD SRGs, STIGs, or NSA SCGs; if such a reference document is not available, the following are acceptable in descending order as available: (1) commercially accepted practices (e.g., SANS) (2) independent testing results (e.g., ICSA) or (3) vendor literature c. 1st PV: all configurable system components.			√
CM-6(1)	Automated Management, Application, and Verification							+	X				Insider Threat CNSSI No. 1015	1st PV: at a minimum, all cybersecurity and cybersecurity-enabled IT products components			
CM-6(2)	Respond to Unauthorized Changes								X								
CM-6(3)	*Unauthorized Change Detection*	*Withdrawn*															
CM-6(4)	*Conformance Demonstration*	*Withdrawn*															

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
CM-7	**Least Functionality**			X	X	X	X	X	X					b. all functions, ports, protocols, software, and services within the system identified to be unnecessary and/or nonsecure			√
CM-7(1)	Periodic Review			+	X	X	+	X	X				Insider Threat APT	a. at least annually or as system changes or incidents occur b. all functions, ports, protocols, software, and services within the information system identified to be unnecessary and/or nonsecure			
CM-7(2)	Prevent Program Execution			+	X	X	+	X	X				Insider Threat			√	
CM-7(3)	Registration Compliance			+	+	+	+	+	+				Insider Threat				
CM-7(4)	Unauthorized Software — Deny-by-Exception															√	

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
CM-7(5)	Authorized Software — Allow-by-Exception			+	X	X	+	X	X				Insider Threat APT CNSSP No. 26	c. at least annually		√	
CM-7(6)	Confined Environments with Limited Privileges														√	√	
CM-7(7)	Code Execution in Protected Environments														√	√	
CM-7(8)	Binary or Machine Executable Code						+	+	+				APT		√		
CM-7(9)	Prohibiting the Use of Unauthorized Hardware						+	+	+				NSS Best Practice (asset inventory)	c. at least annually	√		

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
CM-8	**System Component Inventory**						X	X	X					a.5. minimally but not limited to: hardware specifications (manufacturer, type, model, serial number, physical location), software and software license information, information system/component owner, and for a networked component/device, the machine name b. at least annually	√		√
CM-8(1)	Updates During Installation and Removal							X	X						√		
CM-8(2)	Automated Maintenance						+	+	X				NSS Best Practice		√		
CM-8(3)	Automated Unauthorized Component Detection						+	X	X				Insider Threat APT	a. 2nd PV: continuously	√	√	
CM-8(4)	Accountability Information					X			X					minimally position or role	√		
CM-8(5)	***No Duplicate Accounting of Components***	***Withdrawn***															

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
CM-8(6)	Assessed Configurations and Approved Deviations														√		
CM-8(7)	Centralized Repository														√		
CM-8(8)	Automated Location Tracking		√2,3												√		
CM-8(9)	Assignment of Components to Systems														√		
CM-9	**Configuration Management Plan**						+	X	X				Consistent with the control allocations for the CM family				
CM-9(1)	Assignment of Responsibility																
CM-10	**Software Usage Restrictions**						X	X	X								√
CM-10(1)	Open- Source Software						+	+	+				NSS Best Practice				
CM-11	**User-Installed Software**			X	X	X	X	X	X					c. continuously			√
CM-11(1)	***Alerts for Unauthorized Installations***	***Withdrawn***															

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
CM-11(2)	Software Installation with Privileged Status			+	+	+	+	+	+				Insider Threat APT				
CM-11(3)	Automated Enforcement and Monitoring														√		
CM-12	**Information Location**				X	X		X	X		X	X			√		
CM-12(1)	Automated Tools to Support Information Location				X	X		X	X		X	X			√		
CM-13	**Data Action Mapping**																
CM-14	**Signed Components**							+	+				Insider Threat APT CNSSD No. 505	any software and firmware components	√	√	

Table D-6: Contingency Planning (CP) Family

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
CP-1	**(Contingency Planning) Policy and Procedures**	+		X	X	X	X	X	X	X	X	X	Ensure security and privacy collaboration	a. at a minimum, key cybersecurity and privacy personnel including SAOP or designee c.1., c.2. 1st PV: at least annually	√		
CP-2	**Contingency Plan**									X	X	X		b. key personnel or roles and organizational elements identified in the contingency plan d. at least annually f. key personnel and organizational elements identified in the contingency plan			√
CP-2(1)	Coordinate with Related Plans										X	X				√	
CP-2(2)	Capacity Planning											X					

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
CP-2(3)	Resume Mission and Business Functions										X	X		2nd PV: a time period as defined in the contingency plan			
CP-2(4)	***Resume All Mission and Business Functions***	***Withdrawn***															
CP-2(5)	Continue Mission and Business Functions											X				√	
CP-2(6)	Alternate Processing and Storage Sites																
CP-2(7)	Coordinate with External Service Providers																
CP-2(8)	Identify Critical Assets										X	X				√	
CP-3	**Contingency Training**									X	X	X		a.1. 10 working days a.3. annually or as defined in the contingency plan b.1st PV: at least annually	√		
CP-3(1)	Simulated Events											X			√		
CP-3(2)	Mechanisms Used in Training Environments														√		

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
CP-4	**Contingency Plan Testing**									X	X	X		a.1st PV: at a frequency as defined in the contingency plan a. 2nd PV: tests as defined in the contingency plan	√		
CP-4(1)	Coordinate with Related Plans										X	X			√		
CP-4(2)	Alternate Processing Site											X			√		
CP-4(3)	Automated Testing														√		
CP-4(4)	Full Recovery and Reconstitution														√		
CP-4(5)	Self-Challenge														√	√	
CP-5	*Contingency Plan Update*	*Withdrawn*															
CP-6	**Alternate Storage Site**										X	X					√
CP-6(1)	Separation from Primary Site										X	X					
CP-6(2)	Recovery Time and Recovery Point Objectives											X					
CP-6(3)	Accessibility										X	X					

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
CP-7	**Alternate Processing Site**										X	X		a. 1st PV: system operations as defined in the contingency plan a. 2nd PV: a time period as defined in the contingency plan			√
CP-7(1)	Separation from Primary Site										X	X					
CP-7(2)	Accessibility										X	X					
CP-7(3)	Priority of Service										X	X					
CP-7(4)	Preparation for Use											X					
CP-7(5)	*Equivalent Information Security Safeguards*	*Withdrawn*															
CP-7(6)	Inability to Return to Primary Site																

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
CP-8	**Telecommunications Services**										X	X		1st PV: system operations as defined in the contingency plan 2nd PV: a time period as defined in the contingency plan			
CP-8(1)	Priority of Service Provisions										X	X					
CP-8(2)	Single Points of Failure										X	X					
CP-8(3)	Separation of Primary and Alternate Providers											X				√	
CP-8(4)	Provider Contingency Plan											X					
CP-8(5)	Alternate Telecommunication Service Testing											+	NSS Best Practice				

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
CP-9	**System Backup**			X	X	X	X	X	X	X	X	X		a. 2nd PV: at least weekly or as defined in the contingency plan b. at least weekly or as defined in the contingency plan c. when created, received, updated, or as defined in the contingency plan		√	√
CP-9(1)	Testing for Reliability and Integrity							X	X		X	X		at least monthly or as defined in the contingency plan		√	
CP-9(2)	Test Restoration Using Sampling											X					
CP-9(3)	Separate Storage for Critical Information											X					
CP-9(4)	*Protection from Unauthorized Modification*	*Withdrawn*															
CP-9(5)	Transfer to Alternate Storage Site										+	X	Consistent with CP-6				
CP-9(6)	Redundant Secondary System															√	

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
CP-9(7)	Dual Authorization for Deletion or Destruction															√	
CP-9(8)	Cryptographic Protection			+	X	X	+	X	X	+	X	X	NSS Best Practice			√	
CP-10	**System Recovery and Reconstitution**									X	X	X		a time period as defined in the contingency plan			√
CP-10(1)	*Contingency Plan Testing*	*Withdrawn*															
CP-10(2)	Transaction Recovery										X	X					
CP-10(3)	*Compensating Security Controls*	*Withdrawn*															
CP-10(4)	Restore Within Time-Period											X					
CP-10(5)	*Failover Capability*	*Withdrawn*															
CP-10(6)	Component Protection											+	APT				
CP-11	**Alternate Communications Protocols**															√	
CP-12	**Safe Mode**														√	√	
CP-13	**Alternative Security Mechanisms**															√	

Table D-7: Identification and Authentication (IA) Family

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
IA-1	**Policy and Procedures**	+		X	X	X	X	X	X				Ensure security and privacy collaboration	c.1., c.2. 1st PV: at least annually	√		
IA-2	**Identification and Authentication (Organizational Users)**		√3	X	X	X	X	X	X								√
IA-2(1)	Multifactor Authentication to Privileged Accounts			X	X	X	X	X	X								
IA-2(2)	Multifactor Authentication to Non-Privileged Accounts			X	X	X	X	X	X								
IA-2(3)	***Local Access to Privileged Accounts***	***Withdrawn***															
IA-2(4)	***Local Access to Non-Privileged Accounts***	***Withdrawn***															
IA-2(5)	Individual Authentication with Group Authentication			+	+	X	+	+	X				Insider Threat				
IA-2(6)	Access to Accounts — Separate Device			+	+	+	+	+	+				Insider Threat APT	1st PV: local, network, and remote 2nd PV: privileged and non-privileged accounts		√	

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
IA-2(7)	***Network Access to Non-Privileged Accounts — Separate Device***	***Withdrawn***															
IA-2(8)	Access to Accounts — Replay Resistant			X	X	X	X	X	X					privileged accounts, at a minimum			
IA-2(9)	***Network Access to Non-Privileged Accounts — Replay Resistant***	***Withdrawn***															
IA-2(10)	Single Sign-On																
IA-2(11)	***Remote Access — Separate Device***	***Withdrawn***															
IA-2(12)	Acceptance of PIV Credentials			X	X	X	X	X	X								
IA-2(13)	Out-Of-Band Authentication															√	
IA-3	**Device Identification and Authentication**		√3	+	X	X	+	X	X				APT				√
IA-3(1)	Cryptographic Bidirectional Authentication				+	+		+	+				Insider Threat APT CNSSP No. 17			√	

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
IA-3(2)	*Cryptographic Bidirectional Network Authentication*	*Withdrawn*															
IA-3(3)	Dynamic Address Allocation																
IA-3(4)	Device Attestation																
IA-4	**Identifier Management**		√3	X	X	X	X	X	X					d. at least a year for individuals, groups, roles			√
IA-4(1)	Prohibit Account Identifiers as Public Identifiers																
IA-4(2)	***Supervisor Authorization***	***Withdrawn***															
IA-4(3)	***Multiple Forms of Certification***	***Withdrawn***															
IA-4(4)	Identify User Status			+	X	X	+	X	X				Insider Threat				
IA-4(5)	Dynamic Management																
IA-4(6)	Cross-Organization Management																
IA-4(7)	***In-Person Registration***	***Withdrawn***															

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
IA-4(8)	Pairwise Pseudonymous Identifiers																
IA-4(9)	Attribute Maintenance and Protection		√3	+	+	+	+	+	+				Consistent with desired allocation of IA-2, IA-3, IA-8, and IA-9.				
IA-5	**Authenticator Management**		√3	X	X	X	X	X	X					f. 1st PV: not to exceed 180 days for passwords			√
IA-5(1)	Password-Based Authentication			X	X	X	X	X	X					a. at least quarterly h. a case sensitive 12-character mix of uppercase letters, lowercase letters, numbers, and special characters in including at least one of each; modify at least 50% of the characters when new passwords are created			
IA-5(2)	Public Key-Based Authentication				X	X		X	X								
IA-5(3)	***In-Person or Trusted External Party Registration***	***Withdrawn***															

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
IA-5(4)	***Automated Support for Password Strength Determination***	***Withdrawn***															
IA-5(5)	Change Authenticators Prior to Delivery																
IA-5(6)	Protection of Authenticators				X	X		X	X								
IA-5(7)	No Embedded Unencrypted Static Authenticators			+	+	+							NSS Best Practice				
IA-5(8)	Multiple System Accounts			+	+	+	+	+	+				Insider Threat APT	precautions including advising users that they must not use the same password for any of the following: domains of differing classification levels; more than one domain of a classification level (e.g., internal agency network and Intelink); more than one privilege level (e.g., user, administrator)			
IA-5(9)	Federated Credential Management																
IA-5(10)	Dynamic Credential Binding																

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
IA-5(11)	***Hardware Token-Based Authentication***	***Withdrawn***															
IA-5(12)	Biometric Authentication Performance																
IA-5(13)	Expiration of Cached Authenticators			+	+	+	+	+	+				NSS Best Practice				
IA-5(14)	Managing Content of PKI Trust Stores			+	+	+	+	+	+				CNSSP No. 25				
IA-5(15)	GSA-Approved Products and Services																
IA-5(16)	In-Person or Trusted External Party Authenticator Issuance			+	+	+	+	+	+				In support of IA-12(4) Insider Threat APT				
IA-5(17)	Presentation Attack Detection for Biometric Authenticators																
IA-5(18)	Password Managers																
IA-6	**Authenticator Feedback**			X	X	X											√
IA-7	**Cryptographic Module Authentication**			X	X	X	X	X	X								√

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
IA-8	**Identification and Authentication (Non-Organizational Users)**		√3	X	X	X	X	X	X								√
IA-8(1)	Acceptance of PIV Credentials from Other Agencies			X	X	X	X	X	X								
IA-8(2)	Acceptance of External Party Credentials						X	X	X								
IA-8(3)	***Use of FICAM-Approved Products***	***Withdrawn***															
IA-8(4)	Use of Defined Profiles						X	X	X								
IA-8(5)	Acceptance of PIV-I Credentials																
IA-8(6)	Disassociability																
IA-9	**Service Identification and Authentication**			+	+	+	+	+	+				Insider Threat APT				√
IA-9(1)	***Information Exchange***	***Withdrawn***															
IA-9(2)	***Transmission of Decisions***	***Withdrawn***															
IA-10	**Adaptive Authentication**					+			+				Insider Threat APT			√	

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
IA-11	**Re-Authentication**			X	X	X	X	X	X								√
IA-12	**Identity Proofing**		√3	+	X	X	+	X	X				Insider Threat				√
IA-12(1)	Supervisor Authorization			+	+	+	+	+	+				Insider Threat				
IA-12(2)	Identity Evidence		√3	+	X	X	+	X	X				Insider Threat				
IA-12(3)	Identity Evidence Validation and Verification		√3	+	X	X	+	X	X				Insider Threat				
IA-12(4)	In-Person Validation and Verification		√3			X			X								
IA-12(5)	Address Confirmation		√3		--	--		--	--								
IA-12(6)	Accept Externally-Proofed Identities		√3														

Table D-8: Incident Response (IR) Family

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
IR-1	**Policy and Procedures**	X		X	X	X	X	X	X	X	X	X		c.1., c.2. 1st PV: at least annually	√		
IR-2	**Incident Response Training**	X		X	X	X	X	X	X	X	X	X		a.1: 30 working days a.3: at least annually b. 1st PV: at least annually	√		
IR-2(1)	Simulated Events					X			X			X			√		
IR-2(2)	Automated Training Environments								X			X			√		
IR-2(3)	Breach	X													√		
IR-3	**Incident Response Testing**	X		+	X	X	+	X	X	+	X	X	Consistent with IR-1	1st PV: at least annually	√		
IR-3(1)	Automated Testing														√		
IR-3(2)	Coordination with Related Plans				X	X		X	X		X	X			√		
IR-3(3)	Continuous Improvement														√		
IR-4	**Incident Handling**	X		X	X	X	X	X	X	X	X	X					

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
IR-4(1)	Automated Incident Handling Processes				X	X		X	X		X	X					
IR-4(2)	Dynamic Reconfiguration															√	
IR-4(3)	Continuity of Operations				+	+		+	+		+	+	EO 13587 APT Insider Threat			√	
IR-4(4)	Information Correlation		√[2]	+	+	X	+	+	X	+	+	X	EO 13587 NSM-8 APT Consistent with IR-5 and IR-6 Insider Threat			√	
IR-4(5)	Automatic Disabling of System		√[2]														
IR-4(6)	Insider Threats			+	+	+	+	+	+	+	+	+	EO 13587 Insider Threat CNSSD No. 504				

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
IR-4(7)	Insider Threats — Intra-Organization Coordination	+		+	+	+	+	+	+	+	+	+	Recognize broader privacy interests EO 13587 Insider Threat CNSSD No. 504	at a minimum, Senior Agency Official for Privacy or designee and key cybersecurity personnel			
IR-4(8)	Correlation with External Organizations		√2	+	+	+	+	+	+	+	+	+	EO 13587 NSM-8 Insider Threat Consistent with IR-4(4)	1st PV: the National Manager, through the appropriate Federal Cyber Center or other designated central department point of contact (such as US-CERT, DoD CERT, IC CERT) 2nd PV: at a minimum, a known or suspected compromise or unauthorized access			
IR-4(9)	Dynamic Response Capability															√	
IR-4(10)	Supply Chain Coordination					+			+			+	NSM-8			√	
IR-4(11)	Integrated Incident Response Team		√2			X			X			X				√	

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
IR-4(12)	Malicious Code and Forensic Analysis				+	+		+	+		+	+	APT			√	
IR-4(13)	Behavior Analysis		√2		+	+		+	+		+	+	APT			√	
IR-4(14)	Security Operations Center			+	+	+	+	+	+	+	+	+	NSM-8 APT				
IR-4(15)	Publication Relations and Reputation Repair																
IR-5	**Incident Monitoring**	X		X	X	X	X	X	X	X	X	X			√	√	
IR-5(1)	Automated Tracking, Data Collection, and Analysis		√3		+	X		+	X		+	X	Insider Threat		√		
IR-6	**Incident Reporting**	X		X	X	X	X	X	X	X	X	X		a. 2 hours b. the appropriate Federal Cyber Center or other designated central department point of contact (such as US-CERT, DoD CERT, IC CERT) (see IR-4(8))			
IR-6(1)	Automated Reporting				X	X		X	X		X	X					

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
IR-6(2)	Vulnerabilities Related to Incidents			+	+	+	+	+	+	+	+	+	APT Insider Threat Consistent with IR-4(4)				
IR-6(3)	Supply Chain Coordination			+	X	X	+	X	X	+	X	X	APT CNSSD No. 505				
IR-7	**Incident Response Assistance**	X		X	X	X	X	X	X	X	X	X					
IR-7(1)	Automation Support for Availability of Information and Support				X	X		X	X		X	X					
IR-7(2)	Coordination with External Providers		√3	+	+	+	+	+	+	+	+	+	APT Insider Threat Consistent with IR-4(4)				

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
IR-8	**Incident Response Plan**	X		X	X	X	X	X	X	X	X	X		a.9 1st PV: CISO/SAISO or equivalent. a.9 2nd PV: at least annually (incorporating lessons learned from past incidents). b. all personnel with a role or responsibility for implementing the incident response plan d. all personnel with a role or responsibility for implementing the incident response plan			
IR-8(1)	Breaches	X															
IR-9	**Information Spillage Response**			+	+	+							NSS Best Practice				
IR-9(1)	***Responsible Personnel***	***Withdrawn***															
IR-9(2)	Training			+	+	+							NSS Best Practice	consistent with IR-2			
IR-9(3)	Post-Spill Operations										+	+	NSS Best Practice				
IR-9(4)	Exposure to Unauthorized Personnel		√3	+	+	+							NSS Best Practice				

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
IR-10	*Integrated Information System Analysis Team*	*Withdrawn*															

Table D-9: Maintenance (MA) Family

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
MA-1	**Policy and Procedures**			X	X	X	X	X	X	X	X	X		c.1., c.2. 1st PV: at least annually	√		
MA-2	**Controlled Maintenance**			X	X	X	X	X	X	X	X	X					
MA-2(1)	*Record Content*	*Withdrawn*															
MA-2(2)	Automated Maintenance Activities					X			X			X					
MA-3	**Maintenance Tools**						+	X	X				APT Insider Threat	b. at least annually			
MA-3(1)	Inspect Tools							X	X								
MA-3(2)	Inspect Media						+	X	X				APT Insider Threat CNSSP No. 26				
MA-3(3)	Prevent Unauthorized Removal			+	X	X							NSS Best Practice				
MA-3(4)	Restricted Tool Use						+	+	+				NSS Best Practice				
MA-3(5)	Execution with Privilege			+	+	+	+	+	+				Insider Threat				

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
MA-3(6)	Software Updates and Patches			+	+	+	+	+	+				Insider Threat APT				
MA-4	**Nonlocal Maintenance**						X	X	X								
MA-4(1)	Logging and Review						+	+	+				Insider Threat	a. as defined in the organization's formal audit policy (AU-1)			
MA-4(2)	***Document Nonlocal Maintenance***	***Withdrawn***															
MA-4(3)	Comparable Security and Sanitization			+	+	X	+	+	X				APT				
MA-4(4)	Authentication and Separation of Maintenance Sessions							+	+				Insider Threat			√	
MA-4(5)	Approvals and Notifications																
MA-4(6)	Cryptographic Protection			+	+	+	+	+	+				CNSSP 15	approved algorithms listed in CNSSP 15 Annex B			
MA-4(7)	Disconnect Verification						+	+	+				NSS Best Practice				
MA-5	**Maintenance Personnel**		√2,3	X	X	X	X	X	X	X	X	X					
MA-5(1)	Individuals without Appropriate Access		√2,3			X			X			X					

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
MA-5(2)	Security Clearances for Classified Systems		√2,3														
MA-5(3)	Citizenship Requirements for Classified Systems		√2,3														
MA-5(4)	Foreign Nationals		√2,3														
MA-5(5)	Non-System Maintenance		√2,3														
MA-6	**Timely Maintenance**										X	X					
MA-6(1)	Preventive Maintenance										+	+	NSS Best Practice				
MA-6(2)	Predictive Maintenance																
MA-6(3)	Automated Support for Predictive Maintenance																
MA-7	**Field Maintenance**																

Table D-10: Media Protection (MP) Family

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
MP-1	**Policy and Procedures**	X		X	X	X	X	X	X					c.1., c.2. 1st PV: at least annually	√		
MP-2	**Media Access**			X	X	X	X	X	X					1st PV: all types of digital and/or non-digital media containing information not cleared for public release			
MP-2(1)	*Automated Restricted Access*	*Withdrawn*															
MP-2(2)	*Cryptographic Protection*	*Withdrawn*															
MP-3	**Media Marking**			+	X	X							Insider Threat CNSSP No. 26				
MP-4	**Media Storage**			+	X	X							Insider Threat				
MP-4(1)	*Cryptographic Protection*	*Withdrawn*															
MP-4(2)	Automated Restricted Access																
MP-5	**Media Transport**			+	X	X							Insider Threat CNSSP No. 26				

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
MP-5(1)	*Protection Outside of Controlled Areas*	*Withdrawn*															
MP-5(2)	*Documentation of Activities*	*Withdrawn*															
MP-5(3)	Custodians																
MP-5(4)	***Cryptographic Protection***	***Withdrawn***															
MP-6	**Media Sanitization**	--		X	X	X							Privacy implementation specific to systems that process PII				
MP-6(1)	Review, Approve, Track, Document, and Verify					X											
MP-6(2)	Equipment Testing					X								at least annually			
MP-6(3)	Nondestructive Techniques					X											
MP-6(4)	*Controlled Unclassified Information*	*Withdrawn*															
MP-6(5)	*Classified Information*	*Withdrawn*															
MP-6(6)	*Media Destruction*	*Withdrawn*															
MP-6(7)	Dual Authorization																

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
MP-6(8)	Remote Purging or Wiping of Information																
MP-7	**Media Use**			X	X	X	X	X	X								√
MP-7(1)	***Prohibit Use Without Owner***	***Withdrawn***															
MP-7(2)	Prohibit Use of Sanitization-Resistant Media																
MP-8	**Media Downgrading**																
MP-8(1)	Documentation of Process																
MP-8(2)	Equipment Testing																
MP-8(3)	Controlled Unclassified Information																
MP-8(4)	Classified Information																

Table D-11: Physical and Environmental Protection (PE) Family

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A							
				L	M	H	L	M	H	L	M	H			Assurance	Resiliency	ATT&CK
PE-1	**Policy and Procedures**	+		X	X	X	X	X	X	X	X	X	Ensure security and privacy collaboration	c.1., c.2. 1st PV: at least annually	√		
PE-2	**Physical Access Authorizations**	+		X	X	X	X	X	X	X	X	X	Recognize broader privacy interests	c. at least annually			
PE-2(1)	Access by Position and Role																
PE-2(2)	Two Forms of Identification		$\surd_{2,3}$														
PE-2(3)	Restrict Unescorted Access																
PE-3	**Physical Access Control**		$\surd_{2}$	X	X	X	X	X	X	X	X	X					
PE-3(1)	System Access			+	+	X	+	+	X				Insider Threat				
PE-3(2)	Facility and Systems																
PE-3(3)	Continuous Guards																
PE-3(4)	Lockable Casings																
PE-3(5)	Tamper Protection															√	

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
PE-3(6)	***Facility Penetration Testing***	***Withdrawn***															
PE-3(7)	Physical Barriers																
PE-3(8)	Access Control Vestibules																
PE-4	**Access Control for Transmission**				X	X		X	X								
PE-5	**Access Control for Output Devices**				X	X											
PE-5(1)	***Access to Output by Authorized Individuals***	***Withdrawn***															
PE-5(2)	Link to Individual Identity																
PE-5(3)	***Marking Output Devices***	***Withdrawn***															
PE-6	**Monitoring Physical Access**		√2,3	X	X	X	X	X	X	X	X	X		b. 1st PV: at least every 90 days	√	√	
PE-6(1)	Intrusion Alarms and Surveillance Equipment		√2,3		X	X		X	X		X	X			√		
PE-6(2)	Automated Intrusion Recognition and Responses														√	√	
PE-6(3)	Video Surveillance		√2,3												√		

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
PE-6(4)	Monitoring Physical Access to Systems		√2,3			X			X			X			√	√	
PE-7	*Visitor Control*	*Withdrawn*															
PE-8	**Visitor Access Records**	+		X	X	X	X	X	X	X	X	X	Recognize broader privacy interests	a. at least one year b. at least every 90 days	√		
PE-8(1)	Automated Records Maintenance and Review		√2			X			X			X					
PE-8(2)	*Physical Access Records*	*Withdrawn*															
PE-8(3)	Limit Personally Identifiable Information Elements	X		+	+	+							NSS Best Practice				
PE-9	**Power Equipment and Cabling**										X	X					
PE-9(1)	Redundant Cabling															√	
PE-9(2)	Automatic Voltage Controls																
PE-10	**Emergency Shutoff**										X	X					
PE-10(1)	*Accidental and Unauthorized Activation*	*Withdrawn*															
PE-11	**Emergency Power**										X	X					

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
PE-11(1)	Alternate Power Supply — Minimal Operational Capability											X				√	
PE-11(2)	Alternate Power Supply — Self-Contained															√	
PE-12	**Emergency Lighting**									X	X	X					
PE-12(1)	Essential Missions and Business Functions																
PE-13	**Fire Protection**									X	X	X					
PE-13(1)	Detection Systems — Automatic Activation and Notification										X	X					
PE-13(2)	Suppression Systems — Automatic Activation and Notification										+	X	NSS Best Practice				
PE-13(3)	***Automatic Fire Suppression***	***Withdrawn***															
PE-13(4)	Inspections											+	NSS Best Practice	1st PV: at least annually 2nd PV: 60 days			
PE-14	**Environmental Controls**									X	X	X		b. continuously			
PE-14(1)	Automatic Controls																

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
PE-14(2)	Monitoring with Alarms and Notifications																
PE-15	**Water Damage Protection**									X	X	X					
PE-15(1)	Automation Support											X					
PE-16	**Delivery and Removal**			X	X	X	X	X	X	X	X	X					
PE-17	**Alternate Work Site**		√1,3		X	X		X	X		X	X				√	
PE-18	**Location of System Components**											X					
PE-18(1)	***Facility Site***	***Withdrawn***															
PE-19	**Information Leakage**																
PE-19(1)	National Emissions Policies and Procedures																
PE-20	**Asset Monitoring and Tracking**		√2														
PE-21	**Electromagnetic Pulse Protection**																
PE-22	**Component Marking**			+	+	+							NSS Best Practice				
PE-23	**Facility Location**									+	+	+	NSS Best Practice				

Table D-12: Planning (PL) Family

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
PL-1	**Policy and Procedures**	X		X	X	X	X	X	X	X	X	X		c.1., c.2. 1st PV: at least annually	√		
PL-2	**System Security and Privacy Plans**	X		X	X	X	X	X	X	X	X	X		a.14. at a minimum, SAOP or designee and key cybersecurity personnel b. at a minimum, SAOP or designee and key cybersecurity personnel c. at least annually	√		
PL-2(1)	*Concept of Operations*	*Withdrawn*															
PL-2(2)	*Functional Architecture*	*Withdrawn*															
PL-2(3)	***Plan and Coordinate with Other Organizational Entities***	***Withdrawn***															
PL-3	*System Security Plan Update*	*Withdrawn*															

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A							
				L	M	H	L	M	H	L	M	H			Assurance	Resiliency	ATT&CK
PL-4	**Rules of Behavior**	X		X	X	X	X	X	X	X	X	X		c. at least annually d. at least annually or when the rules are revised or updated	√		
PL-4(1)	Social Media and External Site/Application Usage Restrictions	X		X	X	X									√		
PL-5	*Privacy Impact Assessment*	*Withdrawn*															
PL-6	*Security-Related Activity Planning*	*Withdrawn*															
PL-7	**Concept of Operations**		√2	+	+	+	+	+	+	+	+	+	NSS Best Practice				
PL-8	**Security and Privacy Architectures**	--		+	X	X	+	X	X	+	X	X	Privacy implementation specific to systems that process PII NSS Best Practice	b. at least annually	√		√
PL-8(1)	Defense-In-Depth			+	+	+	+	+	+	+	+	+	APT		√	√	
PL-8(2)	Supplier Diversity		√2	+	+	+	+	+	+	+	+	+	CNSSD No. 505		√	√	
PL-9	**Central Management**	X					+	+	+				APT Insider Threat	at a minimum, flaw remediation, malicious code protection, and spam protection	√		

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
PL-10	**Baseline Selection**	+		X	X	X	X	X	X	X	X	X	Ensure security and privacy collaboration				
PL-11	**Baseline Tailoring**	+		X	X	X	X	X	X	X	X	X	Ensure security and privacy collaboration				

Table D-13: Program Management (PM) Family

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
PM-1	**Information Security Program Plan**	+		**Deployed organization-wide.** **Supports information security program.** **Not associated with security control baselines.** **Independent of any system impact level.**									Ensure security and privacy collaboration	b. 1st PV: at least annually			
PM-2	**Information Security Program Leadership Role**																
PM-3	**Information Security and Privacy Resources**	X															
PM-4	**Plan of Action and Milestones Process**	X															
PM-5	**System Inventory**	+											Identify systems authorized to process PII	at least annually, or when systems are added or removed from the inventory			
PM-5(1)	Inventory of Personally Identifiable Information	X												continuously			
PM-6	**Measures of Performance**	X													√		
PM-7	**Enterprise Architecture**	X															
PM-7(1)	Offloading															√	
PM-8	**Critical Infrastructure Plan**	X															

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
PM-9	**Risk Management Strategy**	X												c. at least annually	√		
PM-10	**Authorization Process**	X													√		
PM-11	**Mission and Business Process Definition**	X												c. at least annually			
PM-12	**Insider Threat Program**		√2												√		
PM-13	**Security and Privacy Workforce**	X															
PM-14	**Testing, Training, and Monitoring**	X													√		
PM-15	**Security and Privacy Groups and Associations**																
PM-16	**Threat Awareness Program**		√2												√	√	
PM-16(1)	Automated Means for Sharing Threat Intelligence		√2,3												√	√	
PM-17	**Protecting Controlled Unclassified Information on External Systems**	X												b. at least annually	√		
PM-18	**Privacy Program Plan**	X															

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
PM-19	**Privacy Program Leadership Role**	X															
PM-20	**Dissemination of Privacy Program Information**	X															
PM-20(1)	Privacy Policies on Websites, Applications, and Digital Services	X													√		
PM-21	**Accounting of Disclosures**	--											Privacy implementation is specific to systems that process PII				
PM-22	**Personally Identifiable Information Quality Management**	X													√		
PM-23	**Data Governance Body**	+											Ensure security and privacy collaboration	1st PV: at a minimum, CISO/SAISO or designee and SAOP or designee	√		
PM-24	**Data Integrity Board**	X													√		
PM-25	**Minimization of Personally Identifiable Information Used in Testing, Training, and Research**	X												d. at least annually			
PM-26	**Complaint Management**	X															

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
PM-27	**Privacy Reporting**	X															
PM-28	**Risk Framing**	X												c. at least annually	√		
PM-29	**Risk Management Program Leadership Roles**	+											Ensure security and privacy collaboration				
PM-30	**Supply Chain Risk Management Strategy**	+											Ensure security and privacy collaboration	c. at least an annual basis	√		
PM-30(1)	Suppliers of Critical or Mission-Essential Items														√	√	
PM-31	**Continuous Monitoring Strategy**	X														√	
PM-32	**Purposing**														√	√	

Table D-14: Personnel Security (PS) Family

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
PS-1	**Policy and Procedures**	+		X	X	X	X	X	X	X	X	X	Ensure security and privacy collaboration	c.1., c.2. 1st PV: at least annually	√		
PS-2	**Position Risk Designation**		√1	X	X	X	X	X	X	X	X	X		c. at least annually or when the position description is updated or when the position is vacated			
PS-3	**Personnel Screening**		√1	X	X	X	X	X	X								
PS-3(1)	Classified Information																
PS-3(2)	Formal Indoctrination																
PS-3(3)	Information Requiring Special Protective Measures																
PS-3(4)	Citizenship Requirements		√1	+	+	+							NSS Best Practice				
PS-4	**Personnel Termination**		√1	X	X	X	X	X	X	X	X	X		a. if voluntary, as soon as possible, not to exceed 5 working days; if involuntary, within same day as termination			

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
PS-4(1)	Post-Employment Requirements			+	+	+							NSS Best Practice				
PS-4(2)	Automated Actions		√1			X			X			X					
PS-5	**Personnel Transfer**			X	X	X	X	X	X	X	X	X		b. 1st PV: reassignment actions to ensure all system accesses no longer required (e.g., need to know) are removed or disabled b. 2nd PV: 10 working days			
PS-6	**Access Agreements**	X		X	X	X	X	X	X					b. and c.2: at least annually	√		
PS-6(1)	*Information Requiring Special Protection*	*Withdrawn*															
PS-6(2)	Classified Information Requiring Special Protection														√		
PS-6(3)	Post-Employment Requirements			+	+	+							NSS Best Practice		√		
PS-7	**External Personnel Security**			X	X	X	X	X	X					d. 1st PV: organizational security manager d. 2nd PV: as soon as possible, not to exceed 1 working day	√		

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
PS-8	**Personnel Sanctions**	+		X	X	X	X	X	X	X	X	X	Privacy breach and risk management implications				
PS-9	**Position Descriptions**	+		X	X	X	X	X	X	X	X	X	Clarify roles, responsibilities, and authorities				

Table D-15: Personally Identifiable Information Processing and Transparency (PT) Family

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
PT-1	**Policy and Procedures**	X		**Personally Identifiable Information Processing and Transparency control are not allocated to the security control baselines.**										c.1, c.2 1st PV: at least annually	√		
PT-2	**Authority to Process Personally Identifiable Information**	--											Privacy implementation specific to systems that process PII		√		
PT-2(1)	Data Tagging														√		
PT-2(2)	Automation														√		
PT-3	**Personally Identifiable Information Processing Purposes**	--											Privacy implementation specific to systems that process PII				
PT-3(1)	Data Tagging														√		
PT-3(2)	Automation														√		
PT-4	**Consent**	--											Privacy implementation specific to systems that process PII				
PT-4(1)	Tailored Consent																
PT-4(2)	Just-In-Time Consent																

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
PT-4(3)	Revocation																
PT-5	**Privacy Notice**	--											Privacy implementation specific to systems that process PII				
PT-5(1)	Just-In-Time Notice																
PT-5(2)	Privacy Act Statements	--											Privacy implementation specific to systems that process PII				
PT-6	**System of Records Notice**	--											Privacy implementation specific to systems that process PII				
PT-6(1)	Routine Uses	--											Privacy implementation specific to systems that process PII				
PT-6(2)	Exemption Rules	--											Privacy implementation specific to systems that process PII				
PT-7	**Specific Categories of Personally Identifiable Information**	--											Privacy implementation specific to systems that process PII				
PT-7(1)	Social Security Numbers	--											Privacy implementation specific to systems that process PII				

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
PT-7(2)	First Amendment Information	--											Privacy implementation specific to systems that process PII				
PT-8	**Computer Matching Requirements**	--											Privacy implementation specific to systems that process PII				

Table D-16: Risk Assessment (RA) Family

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
RA-1	**Policy and Procedures**	X		X	X	X	X	X	X	X	X	X		c.1., c.2. 1st PV: at least annually	√		
RA-2	**Security Categorization**	+		X	X	X	X	X	X	X	X	X	Confirm if system processes PII				
RA-2(1)	Impact-Level Prioritization																
RA-3	**Risk Assessment**	X		X	X	X	X	X	X	X	X	X		d., f. at least annually	√		
RA-3(1)	Supply Chain Risk Assessment			X	X	X	X	X	X	X	X	X		b. at least annually	√		
RA-3(2)	Use of All-Source Intelligence			+	+	+	+	+	+	+	+	+	APT CNSSD No. 505		√	√	
RA-3(3)	Dynamic Threat Awareness			+	+	+	+	+	+	+	+	+	APT		√	√	
RA-3(4)	Predictive Cyber Analytics														√	√	
RA-4	*Risk Assessment Update*	*Withdrawn*															
RA-5	**Vulnerability Monitoring and Scanning**			X	X	X	X	X	X	X	X	X		a. at least every 30 days	√		√
RA-5(1)	***Update Tool Capability***	***Withdrawn***															

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
RA-5(2)	Update Vulnerabilities to be Scanned			X	X	X	X	X	X	X	X	X		within 24 hours prior to running scans	√		
RA-5(3)	Breadth and Depth of Coverage														√		
RA-5(4)	Discoverable Information			+	+	X	+	+	X	+	+	X	Insider Threat APT		√	√	
RA-5(5)	Privileged Access			+	X	X	+	X	X	+	X	X	Insider Threat APT		√	√	
RA-5(6)	Automated Trend Analyses														√	√	
RA-5(7)	*Automated Detection and Notification of Unauthorized Components*	*Withdrawn*															
RA-5(8)	Review Historic Audit Logs														√	√	
RA-5(9)	*Penetration Testing and Analyses*	*Withdrawn*															
RA-5(10)	Correlate Scanning Information					+			+			+	APT		√	√	
RA-5(11)	Public Disclosure Program			X	X	X	X	X	X	X	X	X			√		
RA-6	**Technical Surveillance Countermeasures Survey**		√3												√		

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
RA-7	**Risk Response**	X		X	X	X	X	X	X	X	X	X			√		
RA-8	**Privacy Impact Assessments**	--											Privacy implementation is specific to systems that process PII		√		
RA-9	**Criticality Analysis**				X	X		X	X		X	X				√	√
RA-10	**Threat Hunting**		√2	+	+	+	+	+	+	+	+	+	NSM-8 APT	continuously	√	√	√

Table D-17: System and Services Acquisition (SA) Family

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
SA-1	**Policy and Procedures**	X		X	X	X	X	X	X	X	X	X		c.1., c.2. 1st PV: at least annually	√		
SA-2	**Allocation of Resources**	--		X	X	X	X	X	X	X	X	X	Privacy implementation specific to systems that process PII		√		
SA-3	**System Development Life Cycle**	--		X	X	X	X	X	X	X	X	X	Privacy implementation specific to systems that process PII		√		√
SA-3(1)	Manage Preproduction Environment			+	+	+	+	+	+	+	+	+	APT		√		
SA-3(2)	Use of Live or Operational Data			+	+	+							NSS Best Practice		√	√	
SA-3(3)	Technology Refresh									+	+	+	NSS Best Practice		√		
SA-4	**Acquisition Process**	--		X	X	X	X	X	X	X	X	X	Privacy implementation specific to systems that process PII		√		√
SA-4(1)	Functional Properties of Controls				X	X		X	X		X	X			√		
SA-4(2)	Design and Implementation Information for Controls				X	X		X	X		X	X			√		

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
SA-4(3)	Development Methods, Techniques, and Practices								+				CNSSD No. 505		√		
SA-4(4)	*Assignment of Components to Systems*	*Withdrawn*															
SA-4(5)	System, Component, and Service Configurations								X						√		
SA-4(6)	Use of Information Assurance Products														√		
SA-4(7)	NIAP-Approved Protection Profiles			+	+	+	+	+	+				CNSSP No. 11		√		
SA-4(8)	Continuous Monitoring Plan for Controls														√		
SA-4(9)	Functions, Ports, Protocols, and Services in Use			+	X	X	+	X	X	+	X	X	NSS Best Practice		√		
SA-4(10)	Use of Approved PIV Products			X	X	X	X	X	X						√		
SA-4(11)	System of Records														√		
SA-4(12)	Data Ownership														√		
SA-5	**System Documentation**			X	X	X	X	X	X	X	X	X			√		
SA-5(1)	*Functional Properties of Security Controls*	*Withdrawn*															

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
SA-5(2)	*Security-Relevant External System Interfaces*	*Withdrawn*															
SA-5(3)	*High-Level Design*	*Withdrawn*															
SA-5(4)	*Low-Level Design*	*Withdrawn*															
SA-5(5)	*Source Code*	*Withdrawn*															
SA-6	*Software Usage Restrictions*	*Withdrawn*															
SA-7	*User-Installed Software*	*Withdrawn*															
SA-8	**Security and Privacy Engineering Principles**			X	X	X	X	X	X	X	X	X			√		√
SA-8(1)	Clear Abstractions					+			+			+	NSS Best Practice (SSE)		√		
SA-8(2)	Least Common Mechanism					+			+			+	NSS Best Practice (SSE)		√	√	
SA-8(3)	Modularity and Layering					+			+			+	NSS Best Practice (SSE)		√	√	
SA-8(4)	Partially Ordered Dependencies					+			+			+	NSS Best Practice (SSE)		√	√	
SA-8(5)	Efficiently Mediated Access					+			+			+	NSS Best Practice (SSE)		√		
SA-8(6)	Minimized Sharing					+			+			+	NSS Best Practice (SSE)		√	√	

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
SA-8(7)	Reduced Complexity					+			+			+	NSS Best Practice (SSE)		√	√	
SA-8(8)	Secure Evolvability					+			+			+	NSS Best Practice (SSE)		√	√	
SA-8(9)	Trusted Components					+			+			+	NSS Best Practice (SSE)		√		
SA-8(10)	Hierarchical Trust					+			+			+	NSS Best Practice (SSE)		√		
SA-8(11)	Inverse Modification Threshold					+			+			+	NSS Best Practice (SSE)		√		
SA-8(12)	Hierarchical Protection					+			+			+	NSS Best Practice (SSE)		√		
SA-8(13)	Minimized Security Elements					+			+			+	NSS Best Practice (SSE)		√	√	
SA-8(14)	Least Privilege					+			+			+	NSS Best Practice (SSE)		√		
SA-8(15)	Predicate Permission					+			+			+	NSS Best Practice (SSE)		√	√	
SA-8(16)	Self-Reliant Trustworthiness					+			+			+	NSS Best Practice (SSE)		√	√	
SA-8(17)	Secure Distributed Composition					+			+			+	NSS Best Practice (SSE)		√	√	
SA-8(18)	Trusted Communications Channels					+			+			+	NSS Best Practice (SSE)		√	√	
SA-8(19)	Continuous Protection					+			+			+	NSS Best Practice (SSE)		√	√	

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
SA-8(20)	Secure Metadata Management					+			+			+	NSS Best Practice (SSE)		√		
SA-8(21)	Self-Analysis					+			+			+	NSS Best Practice (SSE)		√		
SA-8(22)	Accountability and Traceability		√2			+			+			+	NSS Best Practice (SSE)		√		
SA-8(23)	Secure Defaults					+			+			+	NSS Best Practice (SSE)		√		
SA-8(24)	Secure Failure and Recovery					+			+			+	NSS Best Practice (SSE)		√		
SA-8(25)	Economic Security					+			+			+	NSS Best Practice (SSE)		√		
SA-8(26)	Performance Security					+			+			+	NSS Best Practice (SSE)		√		
SA-8(27)	Human Factored Security					+			+			+	NSS Best Practice (SSE)		√		
SA-8(28)	Acceptable Security					+			+			+	NSS Best Practice (SSE)		√		
SA-8(29)	Repeatable and Documented Procedures					+			+			+	NSS Best Practice (SSE)		√		
SA-8(30)	Procedural Rigor					+			+			+	NSS Best Practice (SSE)		√		
SA-8(31)	Secure System Modification		√2			+			+			+	NSS Best Practice (SSE)		√	√	
SA-8(32)	Sufficient Documentation					+			+			+	NSS Best Practice (SSE)		√		

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
SA-8(33)	Minimization	X													√		
SA-9	**External System Services**	X		X	X	X	X	X	X	X	X	X			√		
SA-9(1)	Risk Assessments and Organizational Approvals						+	+	+				NSS Best Practice		√		
SA-9(2)	Identification of Functions, Ports, Protocols, and Services			+	X	X	+	X	X	+	X	X	NSS Best Practice	all external information systems and services	√		
SA-9(3)	Establish and Maintain Trust Relationship with Providers				+	+		+	+		+	+	NSS Best Practice		√		
SA-9(4)	Consistent Interests of Consumers and Providers														√		
SA-9(5)	Processing, Storage, and Service Location														√		
SA-9(6)	Organization-Controlled Cryptographic Keys																
SA-9(7)	Organization-Controlled Integrity Checking																
SA-9(8)	Processing and Storage Location - U.S. Jurisdiction			+	+	+	+	+	+	+	+	+	CNSSP No. 32		√		
SA-10	**Developer Configuration Management**						+	X	X				APT		√		√

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
SA-10(1)	Software and Firmware Integrity Verification						+	+	+				APT		√		
SA-10(2)	Alternative Configuration Management Processes														√		
SA-10(3)	Hardware Integrity Verification						+	+	+				APT		√		
SA-10(4)	Trusted Generation														√		
SA-10(5)	Mapping Integrity for Version Control														√		
SA-10(6)	Trusted Distribution														√		
SA-10(7)	Security and Privacy Representatives						+	+	+				NSS Best Practice		√		
SA-11	**Developer Testing and Evaluation**	X			X	X		X	X		X	X			√		√
SA-11(1)	Static Code Analysis				+	+		+	+		+	+	NSS Best Practice		√		
SA-11(2)	Threat Modeling and Vulnerability Analyses					+			+			+	CNSSD No. 505		√	√	
SA-11(3)	Independent Verification of Assessment Plans and Evidence														√		
SA-11(4)	Manual Code Reviews														√		

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
SA-11(5)	Penetration Testing														√	√	
SA-11(6)	Attack Surface Reviews														√	√	
SA-11(7)	Verify Scope of Testing and Evaluation														√		
SA-11(8)	Dynamic Code Analysis														√		
SA-11(9)	Interactive Application Security Testing														√		
SA-12	***Supply Chain Protection***	***Withdrawn***															
SA-12(1)	***Acquisition Strategies, Tools, and Methods***	***Withdrawn***															
SA-12(2)	***Supplier Reviews***	***Withdrawn***															
SA-12(3)	*Trusted Shipping and Warehousing*	*Withdrawn*															
SA-12(4)	*Diversity of Suppliers*	*Withdrawn*															
SA-12(5)	***Limitation of Harm***	***Withdrawn***															
SA-12(6)	*Minimizing Procurement Time*	*Withdrawn*															

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
SA-12(7)	*Assessments Prior to Selection / Acceptance / Update*	*Withdrawn*															
SA-12(8)	*Use of All-Source Intelligence*	*Withdrawn*															
SA-12(9)	*Operations Security*	*Withdrawn*															
SA-12(10)	*Validate As Genuine and Not Altered*	*Withdrawn*															
SA-12(11)	*Penetration Testing / Analysis of Elements, Processes, and Actors*	*Withdrawn*															
SA-12(12)	*Inter-Organizational Agreements*	*Withdrawn*															
SA-12(13)	*Critical Information System Components*	*Withdrawn*															
SA-12(14)	*Identity and Traceability*	*Withdrawn*															
SA-12(15)	*Processes to Address Weaknesses or Deficiencies*	*Withdrawn*															
SA-13	*Trustworthiness*	*Withdrawn*															
SA-14	*Criticality Analysis*	*Withdrawn*															

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
SA-14(1)	*Critical Components with No Viable Alternative Sourcing*	*Withdrawn*															
SA-15	**Development Process, Standards, and Tools**			+	+	X	+	+	X	+	+	X	NSS Best Practice		√		√
SA-15(1)	Quality Metrics														√		
SA-15(2)	Security and Privacy Tracking Tools														√		
SA-15(3)	Criticality Analysis				X	X		X	X		X	X			√		
SA-15(4)	***Threat Modeling and Vulnerability Analysis***	***Withdrawn***															
SA-15(5)	Attack Surface Reduction														√	√	
SA-15(6)	Continuous Improvement														√		
SA-15(7)	Automated Vulnerability Analysis								+				CNSSD No. 505		√		
SA-15(8)	Reuse of Threat and Vulnerability Information														√		
SA-15(9)	***Use of Live Data***	***Withdrawn***															
SA-15(10)	Incident Response Plan														√		

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
SA-15(11)	Archive System or Component														√		
SA-15(12)	Minimize Personally Identifiable Information														√		
SA-16	**Developer-Provided Training**					X			X			X			√		√
SA-17	**Developer Security and Privacy Architecture and Design**					X			X			X			√		√
SA-17(1)	Formal Policy Model														√		
SA-17(2)	Security-Relevant Components														√		
SA-17(3)	Formal Correspondence														√		
SA-17(4)	Informal Correspondence														√		
SA-17(5)	Conceptually Simple Design														√		
SA-17(6)	Structure for Testing														√	√	
SA-17(7)	Structure for Least Privilege														√		
SA-17(8)	Orchestration														√	√	

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
SA-17(9)	Design Diversity														√	√	
SA-18	***Tamper Resistance and Detection***	***Withdrawn***															
SA-18(1)	***Multiple Phases of System Development Life Cycle***	***Withdrawn***															
SA-18(2)	***Inspection of Systems or Components***	***Withdrawn***															
SA-19	***Component Authenticity***	***Withdrawn***															
SA-19(1)	***Anti-Counterfeit Training***	***Withdrawn***															
SA-19(2)	***Configuration Control for Component Service and Repair***	***Withdrawn***															
SA-19(3)	***Component Disposal***	***Withdrawn***															
SA-19(4)	***Anti-Counterfeit Scanning***	***Withdrawn***															
SA-20	Customized Development of Critical Components														√	√	
SA-21	**Developer Screening**			+	+	X	+	+	X	+	+	X	Insider Threat		√		
SA-21(1)	***Validation of Screening***	***Withdrawn***															

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
SA-22	**Unsupported System Components**			X	X	X	X	X	X	X	X	X			√		√
SA-22(1)	***Alternative Sources for Continued Support***	***Withdrawn***															
SA-23	**Specialization**														√	√	

Table D-18: System and Communications Protection (SC) Family

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
SC-1	**Policy and Procedures**	+		X	X	X	X	X	X	X	X	X	Ensure security and privacy collaboration	c.1., c.2. 1st PV: at least annually	√		
SC-2	**Separation of System and User Functionality**				X	X		X	X						√	√	√
SC-2(1)	Interfaces for Non-Privileged Users														√	√	
SC-2(2)	Disassociability														√		
SC-3	**Security Function Isolation**					X			X						√	√	√
SC-3(1)	Hardware Separation														√	√	
SC-3(2)	Access and Flow Control Functions														√	√	
SC-3(3)	Minimize Non-Security Functionality														√	√	
SC-3(4)	Module Coupling and Cohesiveness														√		
SC-3(5)	Layered Structures														√	√	

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
SC-4	**Information in Shared System Resources**			+	X	X							Insider Threat				√
SC-4(1)	*Security Levels*	*Withdrawn*															
SC-4(2)	Multilevel or Periods Processing																
SC-5	**Denial of Service Protection**									X	X	X					
SC-5(1)	Restrict Ability to Attack Other Systems									+	+	+	Insider Threat				
SC-5(2)	Capacity, Bandwidth, and Redundancy										+	+	Insider Threat			√	
SC-5(3)	Detection and Monitoring										+	+	Consistent with SC-5 and its enhancements			√	
SC-6	**Resource Availability**														√		
SC-7	**Boundary Protection**		√4	X	X	X	X	X	X							√	√
SC-7(1)	*Physically Separated Subnetworks*	*Withdrawn*															
SC-7(2)	*Public Access*	*Withdrawn*															
SC-7(3)	Access Points			+	X	X	+	X	X				NSS Best Practice				

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
SC-7(4)	External Telecommunications Services			+	X	X	+	X	X				NSS Best Practice	at least every 180 days			
SC-7(5)	Deny by Default — Allow by Exception			+	X	X	+	X	X				NSS Best Practice				
SC-7(6)	*Response to Recognized Failures*	*Withdrawn*															
SC-7(7)	Split Tunneling for Remote Devices			+	X	X	+	X	X				NSS Best Practice				
SC-7(8)	Route Traffic to Authenticated Proxy Servers			+	+	X	+	+	X				NSS Best Practice	1st PV: all internal communications traffic that may be proxied, except traffic specifically exempted by the Authorizing Official or organizational policy 2nd PV: all untrusted networks outside the control of the organization			
SC-7(9)	Restrict Threatening Outgoing Communications Traffic						+	+	+				Insider Threat Consistent with SC-5(1)				
SC-7(10)	Prevent Exfiltration			+	+	+							Insider Threat APT			√	

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
SC-7(11)	Restrict Incoming Communications Traffic						+	+	+				NSS Best Practice			√	
SC-7(12)	Host-Based Protection			+	+	+	+	+	+	+	+	+	NSS Best Practice	2nd PV: all system components capable of supporting host-based boundary protection mechanisms, such as but not limited to servers, workstations, and those subject to operation outside of the organizational boundary (i.e., laptops and other mobile devices)			
SC-7(13)	Isolation of Security Tools, Mechanisms, and Support Components			+	+	+	+	+	+				APT			√	
SC-7(14)	Protect Against Unauthorized Physical Connections			+	+	+	+	+	+				NSS Best Practice	any managed interface that crosses security domains or connects to an external network, such as but not limited to cross domain solutions a network boundary with a WAN, a partner network, or the Internet			

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
SC-7(15)	Networked Privileged Accesses					+			+				Insider Threat			√	
SC-7(16)	Prevent Discovery of System Components															√	
SC-7(17)	Automated Enforcement of Protocol Formats																
SC-7(18)	Fail Secure					X			X			X			√		
SC-7(19)	Block Communication from Non-Organizationally Configured Hosts																
SC-7(20)	Dynamic Isolation and Segregation															√	
SC-7(21)	Isolation of System Components					X			X						√	√	
SC-7(22)	Separate Subnets for Connecting to Different Security Domains														√	√	
SC-7(23)	Disable Sender Feedback on Protocol Validation Failure																
SC-7(24)	Personally Identifiable Information	--											Privacy implementation is specific to systems that process PII				

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
SC-7(25)	Unclassified National Security System Connections			+	+	+							NSS Best Practice	1st PV: all NSS			
SC-7(26)	Classified National Security System Connections																
SC-7(27)	Unclassified Non-National Security System Connections																
SC-7(28)	Connections to Public Networks			+	+	+							NSS Best Practice	all systems			
SC-7(29)	Separate Subnets to Isolate Functions				+	+							APT			√	
SC-8	**Transmission Confidentiality and Integrity**			+	X	X	+	X	X				NSS Best Practice				√
SC-8(1)	Cryptographic Protection			+	X	X	+	X	X				NSM-8 Consistent with SC-8	prevent unauthorized disclosure of, and detect changes to, information		√	
SC-8(2)	Pre- and Post-Transmission Handling				+	+		+	+				NSS Best Practice	confidentiality and integrity			
SC-8(3)	Cryptographic Protection for Message Externals																

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
SC-8(4)	Conceal or Randomize Communications															√	
SC-8(5)	Protected Distribution System															√	
SC-9	*Transmission Confidentiality*	*Withdrawn*															
SC-10	**Network Disconnect**			+	X	X	+	X	X				Insider Threat APT	no more than 15 minutes		√	√
SC-11	**Trusted Path**														√	√	
SC-11(1)	Irrefutable Communications Path														√		
SC-12	**Cryptographic Key Establishment and Management**		√[1]	X	X	X	X	X	X					for unclassified NSS, NIST FIPS-compliant processes/requirements for key generation, distribution, storage, access, and destruction consistent with NSA-approved protocols			√
SC-12(1)	Availability											X					
SC-12(2)	Symmetric Keys																
SC-12(3)	Asymmetric Keys																

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
SC-12(4)	*PKI Certificates*	*Withdrawn*															
SC-12(5)	*PKI Certificates / Hardware Tokens*	*Withdrawn*															
SC-12(6)	Physical Control of Keys																
SC-13	**Cryptographic Protection**			X	X	X	X	X	X								
SC-13(1)	*FIPS-Validated Cryptography*	*Withdrawn*															
SC-13(2)	*NSA-Approved Cryptography*	*Withdrawn*															
SC-13(3)	*Individuals Without Formal Access Approvals*	*Withdrawn*															
SC-13(4)	*Digital Signatures*	*Withdrawn*															
SC-14	*Public Access Protections*	*Withdrawn*															
SC-15	**Collaborative Computing Devices and Applications**			X	X	X								a. dedicated VTC suites located in approved VTC locations that are centrally managed			
SC-15(1)	Physical or Logical Disconnect															√	

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
SC-15(2)	*Blocking Inbound and Outbound Communications Traffic*	*Withdrawn*															
SC-15(3)	Disabling and Removal in Secure Work Areas																
SC-15(4)	Explicitly Indicate Current Participants																
SC-16	**Transmission of Security and Privacy Attributes**				+	+		+	+				NSS Best Practice				√
SC-16(1)	Integrity Verification							+	+				NSS Best Practice			√	
SC-16(2)	Anti-Spoofing Mechanisms							+	+				NSS Best Practice				
SC-16(3)	Cryptographic Binding								+				NSS Best Practice			√	
SC-17	**Public Key Infrastructure Certificates**			+	X	X	+	X	X				NSS Best Practice				√
SC-18	**Mobile Code**						+	X	X				NSS Best Practice				√
SC-18(1)	Identify Unacceptable Code and Take Corrective Actions						+	+	+				NSS Best Practice				

SC-18(2)	Acquisition, Development, and Use						+	+	+				NSS Best Practice	the following requirements: (a) Category 1A mobile code where technologies can differentiate between signed and unsigned mobile code and block execution of unsigned mobile code may be used. (b) Category 2 mobile code allowing mediated or controlled access to workstation, server, and remote system services and resources may be used with appropriate protections (e.g., executes in a constrained environment without access to system resources such as Windows registry, file system, system parameters, and network connections to other than the originating host; does not execute in a constrained environment unless obtained from a trusted source over an assured channel). (c) Category 3 mobile code having limited functionality, with no capability for unmediated access to workstation, server, and remote system services and resources may be used when executing in an approved browser.			
SC-18(3)	Prevent Downloading and Execution						+	+	+				NSS Best Practice	all unacceptable mobile code such as: (a) Emerging mobile code technologies that have not			

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
														undergone a risk assessment and been assigned to a Risk Category by the CIO. (b) Category 1X mobile code technologies and implementations that cannot differentiate between signed and unsigned mobile code. (c) Unsigned Category 1A mobile code. (d) Category 2 mobile code not obtained from a trusted source over an assured channel (e.g., SIPRNet, SSL connection, S/MIME, code is signed with an approved code signing certificate).			
SC-18(4)	Prevent Automatic Execution						+	+	+				NSS Best Practice	1st PV: software applications such as email, scriptable document/file editing applications that support documents with embedded code (e.g., MS Office applications/documents)			
SC-18(5)	Allow Execution Only in Confined Environments															√	

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
SC-19	*Voice Over Internet Protocol*	*Withdrawn*															
SC-20	**Secure Name/Address Resolution Service (Authoritative Source)**						X	X	X								√
SC-20(1)	*Child Subspaces*	*Withdrawn*															
SC-20(2)	Data Origin and Integrity																
SC-21	**Secure Name/Address Resolution Service (Recursive or Caching Resolver)**						X	X	X								√
SC-21(1)	*Data Origin and Integrity*	*Withdrawn*															
SC-22	**Architecture and Provisioning for Name/Address Resolution Service**			X	X	X	X	X	X	X	X	X				√	√
SC-23	**Session Authenticity**						+	X	X				APT				√
SC-23(1)	Invalidate Session Identifiers at Logout						+	+	+				APT				
SC-23(2)	*User-Initiated Logouts and Message Displays*	*Withdrawn*															

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
SC-23(3)	Unique System-Generated Session Identifiers						+	+	+				APT			√	
SC-23(4)	*Unique Session Identifiers with Randomization*	*Withdrawn*															
SC-23(5)	Allowed Certificate Authorities						+	+	+				APT				
SC-24	**Fail in Known State**					X			X					1st PV: known secure state 2nd PV: information necessary to determine cause of failure and to return to operations with least disruption to mission/business processes 3rd PV: all types of failures on all system components	√		
SC-25	**Thin Nodes**															√	
SC-26	**Decoys**															√	√
SC-26(1)	*Detection of Malicious Code*	*Withdrawn*															
SC-27	**Platform-Independent Applications**															√	

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
SC-28	**Protection of Information at Rest**			+	X	X	+	X	X				APT	1st PV: confidentiality and integrity 2nd PV: all information			√
SC-28(1)	Cryptographic Protection			+	X	X	+	X	X				NSM-8 APT	1st PV: all system components and media 2nd PV: all information		√	
SC-28(2)	Off-Line Storage																
SC-28(3)	Cryptographic Keys			+	+	+	+	+	+				NSS Best Practice				
SC-29	**Heterogeneity**														√	√	√
SC-29(1)	Virtualization Techniques														√	√	
SC-30	**Concealment and Misdirection**														√	√	√
SC-30(1)	*Virtualization Techniques*	*Withdrawn*															
SC-30(2)	Randomness														√	√	
SC-30(3)	Change Processing and Storage Locations														√	√	
SC-30(4)	Misleading Information														√	√	

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
SC-30(5)	Concealment of System Components														√	√	
SC-31	**Covert Channel Analysis**														√		√
SC-31(1)	Test Covert Channels for Exploitability														√		
SC-31(2)	Maximum Bandwidth														√		
SC-31(3)	Measure Bandwidth in Operational Environments														√		
SC-32	**System Partitioning**														√	√	
SC-32(1)	Separate Physical Domains for Privileged Functions														√	√	
SC-33	*Transmission Preparation Integrity*	*Withdrawn*															
SC-34	**Non-Modifiable Executable Programs**														√	√	√
SC-34(1)	No Writable Storage														√	√	
SC-34(2)	Integrity Protection and Read-Only Media														√	√	
SC-34(3)	***Hardware-Based Protection***	***Withdrawn***															

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
SC-35	**External Malicious Code Identification**															√	√
SC-36	**Distributed Processing and Storage**														√	√	√
SC-36(1)	Polling Techniques														√	√	
SC-36(2)	Synchronization														√	√	
SC-37	**Out-Of-Band Channels**														√	√	√
SC-37(1)	Ensure Delivery and Transmission														√		
SC-38	**Operations Security**		√3	+	+	+	+	+	+	+	+	+	Insider Threat APT		√		
SC-39	**Process Isolation**			X	X	X	X	X	X						√	√	√
SC-39(1)	Hardware Separation														√	√	
SC-39(2)	Separate Execution Domain Per Thread														√	√	
SC-40	**Wireless Link Protection**																
SC-40(1)	Electromagnetic Interference																

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
SC-40(2)	Reduce Detection Potential															√	
SC-40(3)	Imitative or Manipulative Communications Deception															√	
SC-40(4)	Signal Parameter Identification																
SC-41	**Port and I/O Device Access**									+	+	+	Insider Threat				√
SC-42	**Sensor Capability and Data**		√3														
SC-42(1)	Reporting to Authorized Individuals or Roles		√3														
SC-42(2)	Authorized Use		√3														
SC-42(3)	***Prohibit Use of Devices***	***Withdrawn***															
SC-42(4)	Notice of Collection		√3														
SC-42(5)	Collection Minimization		√3														
SC-43	**Usage Restrictions**																√
SC-44	**Detonation Chambers**															√	√

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
SC-45	**System Time Synchronization**						+	+	+				NSS Best Practice				
SC-45(1)	Synchronization with Authoritative Time Source						+	+	+				NSS Best Practice				
SC-45(2)	Secondary Authoritative Time Source																
SC-46	**Cross Domain Policy Enforcement**		√3													√	√
SC-47	**Alternate Communications Paths**									+	+	+	APT			√	
SC-48	**Sensor Relocation**															√	
SC-48(1)	Dynamic Relocation of Sensors or Monitoring Capabilities															√	
SC-49	**Hardware-Enforced Separation and Policy Enforcement**														√	√	
SC-50	**Software-Enforced Separation and Policy Enforcement**														√	√	
SC-51	**Hardware-Based Protection**														√	√	

Table D-19: System and Information Integrity (SI) Family

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
SI-1	**Policy and Procedures**	X		X	X	X	X	X	X	X	X	X		c.1., c.2. 1st PV: at least annually	√		
SI-2	**Flaw Remediation**						X	X	X					30 days			√
SI-2(1)	***Central Management***	***Withdrawn***															
SI-2(2)	Automated Flaw Remediation Status						+	X	X				APT	2nd PV: at least quarterly			
SI-2(3)	Time to Remediate Flaws and Benchmarks for Corrective Actions						+	+	+				APT				
SI-2(4)	Automated Patch Management Tools						+	+	+				APT				
SI-2(5)	Automatic Software and Firmware Updates																
SI-2(6)	Removal of Previous Versions of Software and Firmware						+	+	+				APT	all upgraded/replaced software and firmware components that are no longer required for operation			

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
SI-3	**Malicious Code Protection**						X	X	X					c.1 1st PV: at least weekly c.1 2nd PV: endpoints and network entry/exit points c.2 1st PV: block and quarantine malicious code c.2 2nd PV: system administrator at a minimum			√
SI-3(1)	***Central Management***	***Withdrawn***															
SI-3(2)	***Automatic Updates***	***Withdrawn***															
SI-3(3)	*Non-Privileged Users*	*Withdrawn*															
SI-3(4)	Updates Only by Privileged Users																
SI-3(5)	*Portable Storage Devices*	*Withdrawn*															
SI-3(6)	Testing and Verification																
SI-3(7)	***Non-Signature-Based Detection***	***Withdrawn***															
SI-3(8)	Detect Unauthorized Commands																

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
SI-3(9)	***Authenticate Remote Commands***	***Withdrawn***															
SI-3(10)	Malicious Code Analysis						+	+	+				APT			√	
SI-4	**System Monitoring**		$\sqrt{}_{2,3}$	X	X	X	X	X	X	X	X	X			√		√
SI-4(1)	System-Wide Intrusion Detection System			+	+	+	+	+	+	+	+	+	APT		√	√	
SI-4(2)	Automated Tools and Mechanisms for Real-Time Analysis				X	X		X	X		X	X			√	√	
SI-4(3)	Automated Tool and Mechanism Integration														√	√	
SI-4(4)	Inbound and Outbound Communications Traffic			+	X	X	+	X	X	+	X	X	APT Insider Threat Consistent with SI-4(11) CNSSD No. 504	b. 1st PV: continuously	√	√	
SI-4(5)	System-Generated Alerts			+	X	X	+	X	X	+	X	X	APT Insider Threat CNSSD No. 504		√		
SI-4(6)	*Restrict Non-Privileged Users*	*Withdrawn*															

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
SI-4(7)	Automated Response to Suspicious Events														√	√	
SI-4(8)	*Protection of Monitoring Information*	*Withdrawn*															
SI-4(9)	Testing of Monitoring Tools and Mechanisms														√		
SI-4(10)	Visibility of Encrypted Communications		$\sqrt{}_{2,3}$		+	X		+	X		+	X	APT Insider Threat		√	√	
SI-4(11)	Analyze Communications Traffic Anomalies			+	+	+	+	+	+	+	+	+	APT Insider Threat Consistent with SI-4(4) CNSSD No. 504		√	√	
SI-4(12)	Automated Organization-Generated Alerts			+	+	X	+	+	X	+	+	X	Insider Threat CNSSD No. 504		√		
SI-4(13)	Analyze Traffic and Event Patterns														√	√	
SI-4(14)	Wireless Intrusion Detection		$\sqrt{}_{2,3}$	+	+	X	+	+	X	+	+	X	Insider Threat		√		
SI-4(15)	Wireless to Wireline Communications			+	+	+	+	+	+	+	+	+	NSS Best Practice		√		

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
SI-4(16)	Correlate Monitoring Information			+	+	+	+	+	+	+	+	+	Insider Threat CNSSI No. 1015 Consistent with SI-4(1)		√	√	
SI-4(17)	Integrated Situational Awareness														√	√	
SI-4(18)	Analyze Traffic and Covert Exfiltration														√	√	
SI-4(19)	Risk for Individuals		√2,3	+	+	+	+	+	+	+	+	+	Insider Threat		√		
SI-4(20)	Privileged Users		√2,3	+	+	X	+	+	X	+	+	X	Insider Threat		√		
SI-4(21)	Probationary Periods		√2,3												√		
SI-4(22)	Unauthorized Network Services			+	+	+	+	+	+	+	+	+	CNSSD No. 504		√		
SI-4(23)	Host-Based Devices			+	+	+	+	+	+	+	+	+	Insider Threat APT		√		
SI-4(24)	Indicators of Compromise			+	+	+	+	+	+	+	+	+	NSM-8		√	√	
SI-4(25)	Optimize Network Traffic Analysis		√2,3			+			+			+	APT		√	√	
SI-5	**Security Alerts, Advisories, and Directives**						X	X	X					a. minimally the US-CERT	√		√

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
SI-5(1)	Automated Alerts and Advisories								X						√		
SI-6	**Security and Privacy Function Verification**		√1						X					c. the system/security administrator at a minimum	√	√	
SI-6(1)	*Notification of Failed Security Tests*	*Withdrawn*															
SI-6(2)	Automation Support for Distributed Testing																
SI-6(3)	Report Verification Results								+				Consistent with SI-6	responsible security personnel (e.g., AO, CISO/SAISO or equivalent, ISSO, ISSM)			
SI-7	**Software, Firmware, and Information Integrity**							X	X						√	√	√
SI-7(1)	Integrity Checks							X	X						√	√	
SI-7(2)	Automated Notifications of Integrity Violations								X						√		
SI-7(3)	Centrally Managed Integrity Tools														√		
SI-7(4)	*Tamper-Evident Packaging*	*Withdrawn*															
SI-7(5)	Automated Response to Integrity Violations								X						√	√	

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
SI-7(6)	Cryptographic Protection														√	√	
SI-7(7)	Integration of Detection and Response							X	X						√	√	
SI-7(8)	Auditing Capability for Significant Events							+	+				Insider Threat		√		
SI-7(9)	Verify Boot Process						+	+	+				APT	all devices capable of verification of the boot process	√	√	
SI-7(10)	Protection of Boot Firmware						+	+	+				APT	1st PV: all capable devices	√	√	
SI-7(11)	***Confined Environments with Limited Privileges***	***Withdrawn***															
SI-7(12)	Integrity Verification														√	√	
SI-7(13)	***Code Execution in Protected Environments***	***Withdrawn***															
SI-7(14)	***Binary or Machine Executable Code***	***Withdrawn***															

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
SI-7(15)	Code Authentication								X					all software and firmware from vendors/sources that provide cryptographic mechanisms to enable the validation of code authenticity and integrity	√	√	
SI-7(16)	Time Limit on Process Execution Without Supervision														√		
SI-7(17)	Runtime Application Self-Protection								+				APT		√		
SI-8	**Spam Protection**							X	X		X	X					√
SI-8(1)	***Central Management***	***Withdrawn***															
SI-8(2)	Automatic Updates							X	X		X	X		at least weekly			
SI-8(3)	Continuous Learning Capability																
SI-9	*Information Input Restrictions*	*Withdrawn*															

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
SI-10	**Information Input Validation**						+	X	X				APT	all inputs to web/application servers, database servers, and any system or application input that might receive a crafted exploit toward executing some code or buffer overflow	√		√
SI-10(1)	Manual Override Capability														√		
SI-10(2)	Review and Resolve Errors														√		
SI-10(3)	Predictable Behavior						+	+	+				APT		√	√	
SI-10(4)	Timing Interactions														√		
SI-10(5)	Restrict Inputs to Trusted Sources and Approved Formats								+				NSS Best Practice		√	√	
SI-10(6)	Injection Prevention						+	+	+				NSS Best Practice		√		
SI-11	**Error Handling**						+	X	X				APT				
SI-12	**Information Management and Retention**	X		X	X	X	X	X	X								√

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
SI-12(1)	Limit Personally Identifiable Information Elements	--											Privacy implementation specific to systems that process PII				
SI-12(2)	Minimize Personally Identifiable Information in Testing, Training, and Research	--											Privacy implementation specific to systems that process PII				
SI-12(3)	Information Disposal	--		+	+	+	+	+	+				Privacy implementation specific to systems that process PII NSS Best Practice				
SI-13	**Predictable Failure Prevention**														√		
SI-13(1)	Transferring Component Responsibilities														√		
SI-13(2)	*Time Limit on Process Execution Without Supervision*	*Withdrawn*															
SI-13(3)	Manual Transfer Between Components														√		
SI-13(4)	Standby Component Installation and Notification														√		

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
SI-13(5)	Failover Capability														√		
SI-14	**Non-Persistence**														√	√	
SI-14(1)	Refresh from Trusted Sources														√	√	
SI-14(2)	Non-Persistent Information														√	√	
SI-14(3)	Non-Persistent Connectivity														√	√	
SI-15	**Information Output Filtering**							+	+				APT		√	√	√
SI-16	**Memory Protection**							X	X						√	√	√
SI-17	**Fail-Safe Procedures**														√		
SI-18	**Personally Identifiable Information Quality Operations**	--											Privacy implementation specific to systems that process PII				
SI-18(1)	Automation Support																
SI-18(2)	Data Tags																
SI-18(3)	Collection																

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
SI-18(4)	Individual Requests	--											Privacy implementation specific to systems that process PII				
SI-18(5)	Notice of Correction or Deletion																
SI-19	**De-Identification**	--											Privacy implementation specific to systems that process PII				
SI-19(1)	Collection																
SI-19(2)	Archiving																
SI-19(3)	Release																
SI-19(4)	Removal, Masking, Encryption, Hashing, or Replacement of Direct Identifiers															√	
SI-19(5)	Statistical Disclosure Control																
SI-19(6)	Differential Privacy															√	
SI-19(7)	Validated Algorithms and Software																
SI-19(8)	Motivated Intruder															√	

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A							
				L	M	H	L	M	H	L	M	H			Assurance	Resiliency	ATT&CK
SI-20	**Tainting**														√	√	
SI-21	**Information Refresh**					+			+				APT		√	√	
SI-22	**Information Diversity**														√	√	
SI-23	**Information Fragmentation**														√	√	√

Table D-20: Supply Chain Risk Management (SR) Family

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
SR-1	**Policy and Procedures**	+		X	X	X	X	X	X	X	X	X	Ensure security and privacy collaboration	a. at a minimum, key cybersecurity and privacy personnel including SAOP or designee c.1., c.2. 1st PV: at least annually	√		
SR-2	**Supply Chain Risk Management Plan**			X	X	X	X	X	X	X	X	X		b. at least annually	√		
SR-2(1)	Establish SCRM Team			X	X	X	X	X	X	X	X	X			√		
SR-3	**Supply Chain Controls and Processes**			X	X	X	X	X	X	X	X	X			√		
SR-3(1)	Diverse Supply Base					+			+			+	APT		√	√	
SR-3(2)	Limitation of Harm					+			+			+	APT CNSSD No. 505		√	√	
SR-3(3)	Sub-tier Flow Down			+	+	+	+	+	+	+	+	+	APT CNSSD No. 505		√		

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
SR-4	**Provenance**			+	+	+	+	+	+	+	+	+	APT CNSSD No. 505		√	√	√
SR-4(1)	Identity														√	√	
SR-4(2)	Track and Trace														√	√	
SR-4(3)	Validate as Genuine and Not Altered														√	√	
SR-4(4)	Supply Chain Integrity — Pedigree														√	√	
SR-5	**Acquisition Strategies, Tools, and Methods**			X	X	X	X	X	X	X	X	X			√	√	√
SR-5(1)	Adequate Supply					+			+			+	APT CNSSD No. 505		√	√	
SR-5(2)	Assessments Prior to Selection, Acceptance, Modification, or Update				+	+		+	+		+	+	APT CNSSD No. 505		√		
SR-6	**Supplier Assessments and Reviews**			+	X	X	+	X	X	+	X	X	APT CNSSD No. 505	at least annually or as necessitated by events	√		√
SR-6(1)	Testing and Analysis					+			+			+	CNSSD No. 505		√	√	
SR-7	**Supply Chain Operations Security**					+			+			+	CNSSD No. 505		√	√	

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS	Parameter Value	Tailoring Considerations		
				C			I			A					Assurance	Resiliency	ATT&CK
				L	M	H	L	M	H	L	M	H					
SR-8	**Notification Agreements**			X	X	X	X	X	X	X	X	X			√		
SR-9	**Tamper Resistance and Detection**					X			X			X			√	√	
SR-9(1)	Multiple Stages of System Development Life Cycle					X			X			X			√	√	
SR-10	**Inspection of Systems or Components**			X	X	X	X	X	X	X	X	X			√	√	
SR-11	**Component Authenticity**			X	X	X	X	X	X	X	X	X			√	√	√
SR-11(1)	Anti-Counterfeit Training			X	X	X	X	X	X	X	X	X			√		
SR-11(2)	Configuration Control for Component Service and Repair			X	X	X	X	X	X	X	X	X		all system components	√		
SR-11(3)	Anti-Counterfeit Scanning														√	√	
SR-12	**Component Disposal**			X	X	X	X	X	X	X	X	X			√		

Appendix E Overlays

GUIDANCE FOR SPECIAL CONDITIONS AND COMMUNITY-WIDE USE

Overlays are a specification of security or privacy controls, control enhancements, guidance, and other supporting information employed during the tailoring process, that are intended to complement (and further refine) control baselines.[31] An overlay specification may be more stringent or less stringent than the original control baseline specification and can be applied to multiple systems. Overlays can be used to build consensus across communities of interest and identify relevant controls that have broad-based support for very specific circumstances, situations, and/or conditions that differ from the assumptions in Section 2.4. Each overlay provides guidance to determine when it is applicable.

An overlay provides control specifications and supporting risk-based justifications that are directly applicable to its subject matter for the tailoring process. Overlays may or may not be baseline independent and can be applied to any NSS baseline. As a result, there may be overlap of controls between an NSS baseline and controls identified in an overlay(s).[32]

Governance and Publication of CNSS Overlays

The CNSS Safeguarding Working Group (SWG) manages the CNSS overlay initiation, development, approval, publication, and maintenance processes. CNSS provides downloadable copies of the approved and published CNSS overlays, as well as the template to be used in overlay development and overlay development guidance[33]. Overlays marked "Unclassified//For Official Use Only" (UNCLASSIFIED//FOUO) are available on the restricted CNSS website.

Community or Organization Overlays

Independent of the CNSS, communities and organizations may develop, publish, and manage overlays for topics not applicable to all CNSS members or organizations. Any overlay developed by communities other than CNSS are not managed or published by the CNSS but may be available on the CNSS website. To support consistency in the look and feel of all overlays, the CNSS overlay template is published and available for use. Consult the owning organizations for a copy of overlays not available through the CNSS.

[31] NIST SP 800-53B Appendix C provides more guidance on overlays.

[32] If the use of multiple overlays results in conflicts between the application and removal of controls, see Section 3.2.2 for guidance.

[33] Overlays and the overlay template are published on the CNSS website with the CNSS Instructions at: https://www.cnss.gov.