Committee on National Security Systems

CNSS Instruction No. 1253
October 2009

SECURITY CATEGORIZATION AND CONTROL SELECTION FOR NATIONAL SECURITY SYSTEMS

Version 1

Committee on National Security Systems

CNSS Instruction No. 1253

National Manager

FOREWORD

1. The Committee on National Security Systems (CNSS) Instruction No. 1253, "Security Categorization and Control Selection for National Security Systems" (hereinafter referred to as this Instruction), provides all Federal Government departments, agencies, bureaus, and offices with a process for security categorization of National Security Systems (NSS) that collect, generate, process, store, display, transmit, or receive National Security Information. CNSS Instruction No. 1253 also references a comprehensive set of security controls and enhancements associated with the selection of the determined level of potential impact (or loss) to confidentiality, integrity, and availability that may be applied to any NSS developed and employed by the National Security Community[1]. Accordingly, CNSS Instruction No. 1253 also provides tailoring guidance, so that organizations may select a robust set of security controls to secure their NSS, based on assessed risk. This Instruction is not a prescriptive solution; rather, it should be used as a tool by Information Systems Security Engineers, Authorizing Officials, and Senior Agency Information Security Officers to select and agree upon appropriate protections for an NSS.

2. This Instruction derives its authority 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. Additionally, CNSS Policy No. 22, "Information Assurance Risk Management Policy for National Security Systems," requires this Instruction.

3. This Instruction is formatted to align with the numbering scheme used in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3, August 2009, "Recommended Security Controls for Federal Information Systems and Organizations," to ensure that CNSS Instruction No. 1253 serves as a companion document to NIST SP 800-53.

4. CNSS Instruction No. 1253 is effective upon receipt.

5. Copies of this Instruction may be obtained by contacting the Secretariat at 410.854.6805 or www.cnss.gov.

FOR THE NATIONAL MANAGER

RICHARD C. SCHAEFFER

[1] The term National Security Community is used within CNSSI 1253 to refer to all Federal Government departments, agencies, bureaus, and offices that employ NSS.

TABLE OF CONTENTS

CHAPTER ONE

1. The National Institute of Standards and Technology (NIST) created NIST Special Publication (SP) 800-53, "Recommended Security Controls for Federal Information Systems and Organizations," to establish a standardized set of information security controls for use within the United States (U.S.) Federal Government. NIST collaborated with the Intelligence Community (IC), Department of Defense (DoD), and the Committee on National Security Systems (CNSS) to ensure NIST SP 800-53 contains security controls to meet the requirements of National Security Systems (NSS).[2] As a result of these collaborative efforts, the Director of National Intelligence and the Secretary of Defense have directed that the processes described in NIST SP 800-53 (as amended by this Instruction) and the security and programmatic controls contained in Appendices F and G, respectively, shall apply to NSS within the National Security Community. This means NIST SP 800-53 now provides a common foundation for information security controls across the U.S. Federal Government.

1.1 SCOPE

2. This Instruction provides guidance on how to implement the processes described in NIST SP 800-53, the security and programmatic controls contained in Appendices F and G, respectively, and concepts from Federal Information Processing Standard (FIPS) 199, "Standards for Security Categorization of Federal Information and Information Systems," and FIPS 200, "Minimum Security Requirements for Federal Information and Information Systems," as adapted for use within the National Security Community and NSS. It also provides baseline sets of controls for NSS based on these categorizations. This Instruction applies to all components[3] of information systems that process, store, or transmit National Security Information (NSI).[4] For NSS, where differences between the NIST documentation and this Instruction occur, this Instruction is authoritative.

3. The controls contained within NIST SP 800-53, Appendices F and G, are directly applicable to the National Security Community. However, the special nature of the National Security Community results in some variance from the civil sector with respect to the process for information and information system categorization. This Instruction, therefore, provides the processes for categorizing NSI and NSS, and for selecting security controls to provide appropriate protections for NSS.

1.2 PURPOSE

[2] National Institute of Standards and Technology Special Publication 800-59, "Guidelines for Identifying an Information System as a National Security System," provides guidelines developed in conjunction with the Department of Defense, 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 Management Act of 2002 (Title III, Public Law 107-347, December 17, 2002), which provides government-wide requirements for information security.

[3] Information system components include, but are not limited to mainframes, servers, workstations, network components, operating systems, middleware, and applications. Network components may include, for example, devices such as firewalls, sensors (local or remote), switches, guards, routers, gateways, wireless access points, and network appliances. Servers may include, for example, database servers, authentication servers, electronic mail and web servers, proxy servers, domain name servers, and network time protocol servers. Information system components may be either commercial off-the-shelf or custom-developed. These components may be deployed within land-based, sea-based, airborne, and/or space-based information systems.

[4] NSI is defined in CNSSI 4009.

4. This Instruction serves as a companion document to NIST SP 800-53 for organizations within the National Security Community. It establishes the processes for categorizing NSI and NSS, and for appropriately selecting security and programmatic controls for NSS from NIST SP 800-53. To support reciprocity among National Security Community members, this document provides in Appendix J a set of organization-defined values for certain key parameters where NIST SP 800-53 leaves the determination of those values up to the implementing organizations. The resultant set of controls derived from these processes—when properly implemented, assessed, and monitored—mitigates risks to and from these NSS to a level that is acceptable to the authorizing official.

1.3 AUTHORITIES

5. This Instruction derives its authority 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, and from CNSS Policy No. 22, "Information Assurance Risk Management Policy for National Security Systems."

1.4 RESPONSIBILITIES

6. This Instruction is established by the CNSS, which retains the responsibility and authority for updates and maintenance.

1.5 TARGET AUDIENCE

7. This Instruction serves the National Security Community's information security and information assurance (IA) professionals, including those responsible for—

a. An information system, information security, or risk management and oversight (e.g., Chief Information Officers [CIO], Senior Agency Information Security Officers [SAISO], and Authorizing Officials [AO])

b. Information system development (e.g., program and project managers, mission/application owners, system designers, and system/application programmers)

c. Information security implementation and operation (e.g., information system owners, data stewards, information system security engineers, information system administrators, Information System Security Officers [ISSO])

d. Information system and information security assessment and monitoring (e.g., auditors, Inspectors General, evaluators, ISSOs, and assessors).

1.6 KEY DIFFERENCES BETWEEN CNSS INSTRUCTION NO. 1253 AND NIST PUBLICATIONS

8. There are four key differences between the information and system categorization steps and the control selection processes described in this Instruction, and those documented in

NIST publications. These differences are described below, along with the location within this Instruction of the process to be used within the National Security Community.

Aspects of the National Security Community differ from those of the non-National Security Community, particularly the nature of the information processed. The National Security Community is responsible for processing classified NSI. As a result, the National Security Community has a need to securely transfer classified information between security domains without compromising the security of the information or either domain. This scenario, while relatively common within the National Security Community, is extremely uncommon in the non-National Security Community, resulting in the National Security Community's need to develop and employ cross-domain systems and architectures. Due to this and other differences in the security environment between the national security and the non-national security communities, the processes of categorization, selection of control baselines, or control profiles will be conducted differently within each of these communities.

e. Both FIPS 200 and NIST 800-53 apply the concept of a high-water mark (HWM) when categorizing information systems according to the worst-case potential impact of a loss of confidentiality, integrity, or availability of information or an information system. That is, after the potential impact levels for the confidentiality, integrity, and availability security objectives are each determined, the highest of the three is selected as the potential impact level, or HWM, for the system. This Instruction does not adopt this HWM usage. In the National Security Community, the potential impact levels determined for confidentiality, integrity, and availability are retained, meaning there are 27 possible three-value combinations for NSI or NSS, as opposed to the three possible single-value categorizations obtained using the guidelines in FIPS 200. Retaining the discrete impact levels for each of the three security objectives is done to provide a better granularity in allocating security controls to baselines, and should thereby reduce the need for subsequent tailoring of controls. The definition for what constitutes a Low, Moderate, or High confidentiality, integrity, and availability potential impact level for NSI or NSS is included in Chapter 2, Section 2.1.

f. Potential impact-based security categorizations for NSS may be tailored through the use of a risk-based adjustment. This adjustment takes into consideration the physical and personnel security measures already employed throughout the National Security Community and factors such as aggregation of information. This means the security categorization of NSS may be reduced or increased to reflect the overall risk to the organization, the NSS, and the NSI that it stores, processes, or transmits. The risk-based adjustment process is described in Chapter 2, Section 2.1.3.

g. While NIST SP 800-53 and FIPS 199 employ potential impact-level determinations as a required component of the process of selecting controls and enhancements, CNSS Instruction No. 1253 supplements the use of impact-level determinations with control profiles. Control profiles are included as an option because of the recognition that there are certain situations, some common or key in the National Security Community (e.g., cross-domain systems), in which impact-level determination may not provide the most efficient and effective method of control selection. Both the potential impact level and control profile methods of categorization are described in Chapter 2, Section 2.2.

h. It is the policy of the National Security Community that member organizations practice reciprocity with respect to the certification of systems and system components to the greatest extent practicable. Reciprocity of certification reduces the cost and time to implement systems and system components. To facilitate reciprocity, this document provides explicit sets of controls that serve as common baselines for organizations to use in the control selection process described in Chapter 3 of this document. These baseline control sets are provided in Appendix D.

1.7 RELATIONSHIP TO OTHER DOCUMENTS

9. This Instruction is one of a family of documents that describe the information security/IA risk management and security control processes within the National Security Community. Related documents and their significance in this area are the following:

a. CNSS Policy No. 22, "Information Assurance Risk Management Policy for National Security Systems." Governs IA risk management activities within the National Security Community.

b. NIST SP 800-37 Rev 1 Initial Public Draft, "DRAFT Guide for Security Authorization of Federal Information Systems, A Security Life Cycle Approach" Provides guidance on the process for the certification and accreditation of information systems within the U.S. Federal Government.

c. NIST SP 800-39, "DRAFT Managing Risk from Information Systems: An Organizational Perspective." Provides guidance on organizational risk management.

d. NIST SP 800-53 Rev 3, August 2009, "Recommended Security Controls for Federal Information Systems and Organizations." Provides guidance on the process for selecting security controls, as well as providing the security controls applicable to all U.S. Federal Government information systems.

CHAPTER TWO

CATEGORIZING NSI AND NSS

10. All U.S. Federal Government departments, agencies, bureaus, and offices that operate, use, or manage NSS must establish and implement an IA Risk Management Program (IARMP), in accordance with CNSS Policy No. 22. The Risk Management Framework (RMF) defined in CNSS Policy No. 22 and described in NIST SP 800-39 provides National Security Community organizations a framework for risk management within their IARMP. Step one of the RMF requires these organizations to categorize their NSI and NSS as part of their system development life cycle (SDLC). Once categorization is successfully accomplished, the organization may then determine the appropriate security controls to apply to the system in order to properly manage their mission, business, and system risks.

11. The following sections establish the security categorization guidelines for NSI and NSS and provide direction for their use. These guidelines describe and specify the use of either a baseline or control profile security categorization methodology to complete Step 1 during the Categorization phase of the RMF. The head of an organization or that person's designee is responsible for determining how system categorization is conducted per NSS within the organization.

12. The results of Step 1 will subsequently be used in defining the set of controls applied to the system. The set of controls is determined through the Selection step of the RMF described in Chapter 3 of this Instruction. Determining the appropriate controls for their NSS helps organizations properly manage their NSS-related mission, business, and system risks.

2.1 BASELINE SECURITY CATEGORIZATION METHOD

13. The baseline method of security categorization builds on the foundation established in FIPS 199, which defines three levels of potential impact (Low, Moderate, or High) on organizations or individuals should a security breach occur (i.e., a loss of confidentiality, integrity, or availability). National Security Community organizations applying these definitions must do so within the context of their organization and the overall national interest.

14. The baseline method of security categorization is a three-step process:

Step 1. Security categorization of information types.

Step 2. Security categorization of NSS using the output from Step 1.

Step 3. Risk adjustment of the NSS categorization using the output from Step 2 as a starting point.

15. The security categorization of an NSS relies on common definitions for each of the potential impact levels. These potential impact levels are defined as follows:

a. The potential impact is **Low** if the loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational

assets, individuals,[5] other organizations, or the national security interests of the United States.

AMPLIFICATION: A limited adverse effect means that the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of those functions is noticeably reduced; (ii) result in minor damage to organizational, critical infrastructure, or national security assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

b. The potential impact is **Moderate** if the loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States.

AMPLIFICATION: A serious adverse effect means that the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of those functions is significantly reduced; (ii) result in significant damage to organizational, critical infrastructure, or national security assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals ***exceeding mission expectations***.

c. The potential impact is **High** if the loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States.

AMPLIFICATION: A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational, critical infrastructure, or national security assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals ***exceeding mission expectations***.

2.1.1 Security Categorization of Information Types

16. The security category of an information type[6] may be associated with user information or system information in either electronic or non-electronic form. Selecting the appropriate security category for an information type requires determining the potential impact for loss of confidentiality, integrity, or availability associated with it. Determination of the potential impact for an information type considers all factors that may affect an organization's mission, business objectives, and system risks related to it. The security category of an information type is

[5] Adverse effects on individuals may include, but are not limited to, loss of the privacy to which individuals are entitled under law.

[6] 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.

represented as a set of three values, reflecting the potential impact with respect to confidentiality, integrity, and availability.

17. National Security Community organizations using the baseline categorization method must determine the security category for all information types resident on the target information system, taking into account each of the three security objectives independently. This means the determination of the potential impact level for one security objective (e.g., confidentiality) is independent of the potential impact determination of the other two objectives (integrity and availability). In some instances, a system might contain various types of information that have different potential impact values. For example, a system might contain administrative data that is assessed to have a Low availability potential impact value. The same system may also contain mission data that is assessed to have a Moderate availability potential impact value. In such an instance, the availability potential impact value of the system's information would be designated as Moderate because this is the highest potential impact value of information processed by the system. An organization must make similar determinations for each information type concerning the integrity and confidentiality security objectives.

18. The generalized format for expressing the security category (SC) of an information type is—

> **SC** information type = {(**confidentiality**, *impact*), (**integrity** *impact*), (**availability** *impact*)}, where the acceptable values for potential impact are Low, Moderate, or High.

2.1.2 Security Categorization of NSS

19. Security categorization of an NSS must consider the security categories of all information types resident on it. For an NSS, the potential impact values assigned to the respective security objectives (confidentiality, integrity, availability) will be the highest values from among those security categories that have been determined for each type of information resident on the NSS. The set of three values comprises the security category of a system.

20. The generalized format for expressing the SC of an NSS is—

> **SC** NSS = {(**confidentiality**, *impact*), (**integrity**, *impact*), (**availability**, *impact*)}, where the acceptable values for potential impact are Low, Moderate, or High.

2.1.3 Risk Adjustment of the NSS Categorization

21. Impact-based security categorization requires a worst-case assessment of the potential impact with regard to potential loss of confidentiality, integrity, or availability for each information type independently. It does not reflect operational or environmental factors that might mitigate the potential impact or information aggregation that might increase the potential impact. Therefore, once the impact-based security of the system has been categorized, organizations should determine whether a risk adjustment of the system's categorization is warranted, based on the results of a risk assessment of the information types on the system and the system's environment. This risk adjustment can leverage security controls already in the system's environment or identify the need for additional security controls, resulting in a better

informed security controls baseline decision. If the original categorization is adjusted based on these factors, the reasons must be documented in categorization documentation and the relevant controls that are already in the system's environment must be included in the tailored baseline as common inherited controls. Additionally, controls excluded from the initial control baseline due to the risk adjustment should be reconsidered for inclusion during the supplementation step.

22. As a result of the risk adjustment, the appropriate organizational authority may select a control baseline that reflects a lower or higher potential impact than the one originally assessed for the system. Depending on the specific elements of the risk assessment, the adjustment may result in a lower or higher baseline for confidentiality, integrity, availability, or some combination of these three objectives.

23. Among other considerations, the risk adjustment should consider the security that is afforded by the larger system environment (e.g., physical, personnel, organizational) and its mitigating effect on external exposure. These environmental security measures are typically required to protect classified NSI as defined in Executive Order 12958, "Classified National Security Information," as amended. For example, a system that processes collateral Top Secret (TS) information may allow selecting the Low set of baselines when operating in an environment that already satisfies the security requirements for protecting TS information from external exposure. This is because any loss of information from the system would be contained within the protected environment and result in only limited adverse effects. On the other hand, an unclassified information system processing personally identifiable information (PII) may require selecting the Moderate set of baselines. In this instance, the loss of PII may have serious adverse effects on individuals, and the security controls limiting external exposure of information in an unclassified environment are much less stringent than those for a TS information environment.

24. The generalized format for expressing the post-risk assessment (post-RA) SC of an NSS is—

SC (post-RA) NSS = {(**confidentiality**, *impact*), (**integrity**, *impact*), (**availability**, *impact*)}, where the acceptable values for potential impact are Low, Moderate, or High.

2.2 CONTROL PROFILE SECURITY CATEGORIZATION METHOD

25. Control profiles provide a method by which organizations may designate sets of controls for NSS based on their enterprise-wide risk assessment and taking into account business objectives, system risks, and mission needs. Organizations may create security control profiles to establish and publish agreed-upon sets of security controls for specific information types or NSS within their organizations. These sets of controls, referred to as control profiles, are defined by organizations to meet specified purposes. Some organizations may choose to rigidly define some or all of their control profiles and allow little or no subsequent tailoring during control selection for specific systems. Other organizations may choose to loosely define some or all of their control profiles and permit or require subsequent tailoring during control selection for specific systems. The specific methodology for creation, selection, and implementation of a control profile is left to the organization establishing or employing it.

CHAPTER THREE

CONTROL SELECTION WITHIN THE RISK MANAGEMENT FRAMEWORK

26. Organizations can choose one of two methods to select applicable security controls. One is the baseline method, which is based on categorized potential impact levels; the other is the control profile security categorization method used when enterprise-level considerations involve the security management of multiple systems in the same or similar manner to meet mission needs. The head of an organization, or that person's designee, determines which method of security control selection should be used for their NSS. With either method, control selection is governed by risk management decisions made at the enterprise and individual system levels. Regardless of the categorization method used, controls are selected from the NIST SP 800-53 control catalog. Control selection is conducted as part of the organization's overall risk management program that identifies risks and associated threats, sets a risk threshold, and continually manages the selection and implementation of controls to mitigate the identified risks to an acceptable level.

3.1 SECURITY CONTROL SELECTION PROCESS

27. The security control selection process is based on the results of the system categorization process described above. Once the NSS has been categorized, the security controls for the system are selected using either the baseline or the control profile security categorization method. The process for selecting security controls for an NSS is a three-step process:

Step 1. Select the initial set of security controls.

Step 2. Tailor the initial set of security controls.

Step 3. Supplement the tailored set of security controls.

Note: If using the control profile method, refer to the applicable organizational guidance regarding the specific control profile to determine whether tailoring or supplementing it is permitted or required.

3.2 SELECTING THE INITIAL SET OF SECURITY CONTROLS

28. The initial set of security controls for a system is selected on the basis of either its baseline security categorization or its designated control profile.

29. If a baseline security categorization is used, the initial control set is the aggregation of the controls identified in the tables provided in Appendix D and corresponds to the value determined for each security objective (confidentiality, integrity, and availability) of the system.

30. If a control profile is used, the initial set of security controls is identified in the profile.

3.3 RISK-BASED MODIFICATIONS TO CONTROL SETS

31. Selecting and specifying controls for an NSS should be accomplished as part of an enterprise IARMP. The risk-based approach to control selection and specification considers effectiveness, efficiency, operational needs, and constraints resulting from applicable public laws, executive orders, directives, policies, and other official guidance. Risk must be considered throughout the system development life cycle. Risk-based selection of controls and their enhancements or parameters must be validated and verified through system requirements, design, test, and operations. Refer to NIST 800-30 for guidance on managing system risk and on developing a system risk model for an NSS.

32. NSS provide unique capabilities, operate in diverse environments, and are subject to advanced cyber threats. An enterprise-level risk approach must be taken when defining and implementing the final security controls for an NSS. A risk threshold needs to be established by the AO or Risk Executive Function (REF) early in the SDLC to provide guidance for control selection and follow-on security engineering activities. The established system risk model and acceptable risk threshold should be documented in accordance with NIST SP 800-37.

3.3.1 Tailoring Controls

33. Whether produced by the baseline or control profile selection process, AOs, the REF, and other decision-makers may find it necessary to tailor (modify) an initial control set because of operational considerations. NIST SP 800-53 groups this tailoring activity into three areas:

1. Scoping guidance.
2. Compensating security controls.
3. Specification of organization-defined parameters.

34. Refer to and use NIST SP 800-53, Section 3.3 for initial guidance on tailoring controls. Use Section 3.3.1 of this Instruction for supplemental guidance.

35. Such tailoring decisions must be aligned with operational considerations and the environment of the information system. For example, in command and control systems in which lives may be in the balance, adoption of security controls must be balanced against operational necessity. In the case of an air traffic control console, the need to access the console at all times may outweigh the security need for an AC-11 (Session Lock) capability.

36. Conversely, controls should not be removed for operational convenience, but have a specified, risk-based determination as established by the system's risk model. Tailoring decisions, including the specific rationale (i.e., mapping to risk thresholds) for those decisions, are documented in the security plan for the information system. Every control from the initial set of security controls must be accounted for either by the organization or the information system owner. If a control is not implemented or is tailored out, then the rationale for doing so should be documented.

3.3.1.1 Additional Scoping Guidance for NSS

37. There are a number of factors that may affect the security controls that should be applied to an NSS. Such factors recommend tailoring of the initial set of security controls by the addition or removal of controls. These factors include those described in NIST SP 800-53, Revision 3, Section 3.3, as well as the mobility of the physical hosting environment, the system's capabilities or technologies, and the processing and storage capabilities of an NSS.

Mobility

38. The mobility of the physical hosting environment can impact the set of security controls selected for the system. The initial sets of security controls identified in Appendix D assume operation of an NSS in a fixed, non-mobile location. If an NSS is to operate in a mobile or semi-mobile environment, the initial set of security controls should be tailored appropriately, adding or removing security controls as required, to account for the difference in the mobility and accessibility of the location housing an NSS.

39. A system's mobility may make some controls impractical or unnecessary. Conversely, greater mobility may require the use of controls not called for in the initial set. Vehicles such as ships, airplanes, or vans do not reside in a fixed environment, and some controls may not be applicable for such semi-mobile entities. The security controls most likely to be affected by such semi-mobile entities would be in the PE (physical environment) family. For example, controls such as Visitor Control may be met by the system's mobility, because they generally preclude casual visitors. Similarly, Alternate Work Site may not be applicable for systems on ships (at sea). These do not lend themselves to the definition of an alternate site because of their constant movement.

User-Based Collaboration and Information Sharing

40. The selection of some controls and enhancements should be based on the accessibility or exposure of the system to access by unauthorized parties—the greater the degree of access to a system, both logical and physical, the greater the risk of information exposure. The authorization boundary established during the security categorization process should be assessed for accessibility and exposure risks at points of interface. Factors that must be considered include the number of individuals granted access to a system or an area around the system. For example, an organization may require the use of Control Enhancements to Auditable Events, Audit Records, or Audit Monitoring in order to address the insider threat. Accessibility and exposure also need careful consideration in the following:

a. Cross-domain solutions (where the risk of data spillage or exposure is great)

b. Systems that simultaneously process and keep separated multiple classification levels of data, and whose authorized users have various clearance and/or access authorization levels

c. When determining the appropriateness of providing restricted information (e.g., compartmented, privileged medical, or PII in environments where not all system users are authorized to access all of the information).

System Capabilities/Technology

41. Security controls that refer to specific technologies (e.g., wireless, cryptography, Public Key Infrastructure) are applicable only when those technologies are employed or are required to be employed within an NSS. Security controls are applicable only to those NSS components that provide or support the security capability addressed by the control and are sources of potential risk being mitigated by the control. For example, when information system components are single user and not networked (or only locally networked), one or more of these characteristics may provide appropriate rationale for not applying selected controls to that component.

Processing and Storage Capability

42. What constitutes a *system* under the E-Government Act of 2002 is quite broad. Large collections of like entities, including fax machines, "beepers," cellular telephones, public branch exchanges, digital cameras, and telephone answering machines, could be categorized as systems. These types of systems usually lack the general processing and storage capabilities assumed for the categorized controls. This does not preclude organizations from selectively applying the suggested controls to this class of systems, but the application of the controls and enhancements should be done judiciously and always take into account the intended use of the systems, system capabilities, and the risk of compromise to the system. There may be instances in which selective application of controls to such systems would be practical (e.g., requiring the use of a password, personal identification number, or some other form of authentication on a cellular telephone before making an outgoing call).

3.3.1.2 Additional Compensating Guidance for NSS

43. Compensating security controls are needed because all possible circumstances cannot be anticipated when constructing an initial set of security controls, no matter how well-written and reviewed the list of possible circumstances may be. A variety of circumstances may require the use of compensating security controls:

a. The selected control in the catalog cannot be applied to a given NSS.

b. The selected control would impose excessive or unnecessary costs on the organization.

c. The selected control may have a significantly adverse effect on mission requirements (e.g., need to deploy the system rapidly in a mobile configuration).

44. The following is an example of using compensating security controls (physical or procedural controls to compensate for insufficient identification and authentication (I&A) controls). The use of more stringent physical or procedural security measures, requiring an individual to go through multiple physical security checks prior to being granted access to an information system, may compensate for a lack of stronger automated I&A measures than are called for in impact- or profile-derived sets of security controls (e.g., two-factor authentication).

45. The use of compensating security controls should be documented in the SSP for the information system and approved by the AO.[7]

Enterprise-Implemented Security Controls and Related Considerations

46. Security controls may be implemented and managed by an organizational entity at the enterprise level. Organizational decisions on which security controls are implemented and managed on behalf of the enterprise may greatly affect the responsibilities of individual information system owners with regard to the implementation of controls in a particular set. Every control must be fully addressed either by the organization or the NSS owner. Thus, a system owner might be directed not to implement an intrusion detection system at the system level, because intrusion detection systems are already implemented at the organizational level, and the NSS risk model indicates that such a level of implementation is sufficient.

System Capabilities/Technology

47. Refer to NIST SP800-53 Rev.3.

3.3.1.3 Organization-Defined Security Control Parameters for NSS

48. To support reciprocity among national security organizations, many parameters within the NIST SP 800-53 controls catalog require specific instantiation. The defined values for applicable controls can be found in Appendix J of this document. These values establish a standard for certifying that a control mitigates a threat. In differing risk thresholds or threat scenarios some AOs may require systems to diverge from this standard. In these situations, additional technology may be added, or architectural implementations may be modified to adequately mitigate the risk. By establishing a standard on key parameters, organizations have a known baseline when accepting certifications of technologies or systems from other National Security Community organizations and do not have to duplicate that level of certification. When reciprocity of certification is to be extended across AOs, or when one system provides security on behalf of another system, values for these parameters are negotiated between relevant authorizers and the results are documented in the SSPs of both systems.

3.3.2 Supplementing Controls

49. The tailored baseline is supplemented on the basis of the system's risk analysis. Supplementation addresses any residual risks not adequately mitigated by the tailored baseline. In many cases, additional security controls or control enhancements will be needed to address specific threats to or vulnerabilities in an NSS or to satisfy the requirements of public laws, executive orders, directives, policies, standards, or regulations. Risk assessment at this stage in the security control selection process provides important inputs for determining the sufficiency of the security controls. The inclusion of each control is based on the need to reduce risk to an established threshold. When the tailoring of controls is inadequate, supplemental controls need

[7] This Instruction encourages organizations to select compensating controls from the Security Controls Catalog (SCC). There are instances where organization-defined compensating controls should be employed, because the SCC does not contain suitable compensating controls.

to be added. Ultimately, this is not a process of managing controls, but of using controls to manage risk. Refer to NIST SP 800-53 for specific details of the supplementing process.

Control of the System

50. Some of the security controls and enhancements make certain assumptions regarding the ownership and management of the system. For example, the joint ownership of an NSS by coalition partners would require deeper review of control enhancements to controls in the MA family (e.g., maintenance personnel).

Advanced Cyber Threat

51. NSS, as well as many non-NSS, are subject to advanced cyber threats. Such threats are of a sufficient caliber that they cannot be entirely mitigated given the high-risk environments in which they operate. Stakeholders must be aware of this threat and ensure that control sets are supplemented in a way that provides defense-in-breadth, while maintaining operational flexibility at the enterprise level. Rather than operating independently, controls provide support for each other. In high-threat environments, control mechanisms themselves will be subject to attack. The risk-managed approach to control selection should ensure that protective, detective, and corrective controls are instantiated such that they restrict access to security mechanisms, detect when security mechanisms are modified, and take appropriate corrective action when such modifications are detected. Situations in which even the defense-in-depth approach for controlling implementation is insufficient, usage restrictions should be considered.

52. Organizational officials should determine the required use restrictions for the system. They have a vested interest in accomplishing organizational missions in accordance with risks identified for the system. These officials typically include the information system owner, mission owner, AO, SAISO, and CIO. Examples of use restrictions include—

a. Limiting either the information an information system can process, store, or transmit or the manner in which a mission is automated

b. Prohibiting external information system access to critical organizational information by removing selected system components from the network (i.e., “air gapping”)

c. Prohibiting moderate- or high-impact information on an information system component that the public can access, unless an explicit determination is made authorizing such access.

53. It is important for organizations to document the decisions made during the security control selection process, identifying the risk-based rationale for those decisions. This documentation is essential when assessing the overall security posture of information systems with respect to potential mission and/or business case impact. The implementation of any security control is intended to mitigate a risk, and the level of its implementation is set to the level of mitigation required to meet documented risk-tolerance thresholds. The resulting set of agreed-upon security controls, the supporting rationale for control selection decisions, and any NSS use restrictions must be documented in the SSP for the information system.

APPENDIX A: REFERENCES

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

Appendix A provides the references used within Committee on National Security Systems Instruction No. 1253. The references are consistent with the references contained in National Institute of Standards and Technology Special Publication 800-53, Revision 3, which are adopted in their entirety for this Instruction. References unique to this Instruction are provided below.

a. Executive Order 12958, "Classified National Security Information," as amended, March 2003.

b. National Security Directive 42, "National Policy for the Security of National Security Telecommunications and Information Systems," July 1990.

c. Committee on National Security Systems Policy No. 22, "Information Assurance Risk Management Policy for National Security Systems," February 2009.

d. National Institute of Standards and Technology Special Publication 800-53, Revision 3, August 2009.

e. NIST SP 800-37 Rev 1 Initial Public Draft, "DRAFT Guide for Security Authorization of Federal Information Systems, A Security Life Cycle Approach."

f. NIST SP 800-39, "DRAFT Managing Risk from Information Systems: An Organizational Perspective."

APPENDIX B: GLOSSARY

COMMON TERMS AND DEFINITIONS

The terms used in this publication are consistent with those contained in National Institute of Standards and Technology Special Publication 800-53, Revision 3, or Committee on National Security Systems Instruction No. 4009, “National Information Assurance Glossary,” which are adopted in their entirety for this Appendix.

APPENDIX C: ACRONYMS

COMMON ABBREVIATIONS

The acronyms and abbreviations used in this Instruction are consistent with those contained in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3, and are adopted in their entirety for this Instruction. The acronyms and abbreviations not specifically addressed in NIST SP 800-53, Revision 3, are included below.

IARMP	Information Assurance Risk Management Program
IC	Intelligence Community
NSI	National Security Information
NSS	National Security System
PII	Personally Identifiable Information
RMF	Risk Management Framework

APPENDIX D: SECURITY CONTROL BASELINES—SUMMARY

BASELINE CONTROLS BY IMPACT LEVEL PER SECURITY OBJECTIVE

1. Table D–1 identifies security control baselines for National Security Systems (NSS). This table lists the security controls from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3, Appendix F, and identifies their applicability by impact level (Low, Moderate, and High) per security objective (confidentiality, integrity, and availability).

2. Table D–2 lists the security controls from NIST SP 800-53, Revision 3, Appendices F and G, and identifies their relationships to security objectives (confidentiality, integrity, and availability), regardless of their identification as a component of a baseline in Table D-1. These relationships are a factor in the development of the baselines shown in Table D-1 and should also inform the tailoring and supplementing of controls.

3. Tables D–1 and D–2 are consistent with the assumptions and guidelines provided in this Appendix. The designation of applicability and relationships in these two tables is herein referred to as "binning."

Assumptions and Guidelines for Confidentiality, Integrity, and Availability Binning

4. Establishing the confidentiality, integrity, and availability binning was accomplished by employing a pre-determined set of guidelines. The definition of the confidentiality, integrity, and availability objectives from [44 United States Code (U.S.C.), Section 3542] are as follows:

CONFIDENTIALITY: "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" [44 U.S.C., Section 3542] A loss of *confidentiality* is the unauthorized disclosure of information.

INTEGRITY: "Guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity…" [44 U.S.C., Sec. 3542] A loss of *integrity* is the unauthorized modification or destruction of information.

AVAILABILITY: "Ensuring timely and reliable access to and use of information…" [44 U.S.C., Section 3542] A loss of *availability* is the disruption of access to or use of information or an information system.

5. Based on these definitions and a review of the controls and enhancements, the following rules were established:

a. **Primary Focus.** Each control/enhancement was binned based on whether the security objective(s) were the *primary* focus of the control/enhancement. If a security objective was only indirectly affected by a control/enhancement, it was not associated with that control/enhancement. In some cases, only one objective was the primary focus of a

control/enhancement; in other cases, two objectives were equally affected; and in still other cases, all three objectives were equally affected. This rule is probably the greatest distinction between this confidentiality, integrity, and availability approach and that employed in NIST SP 800-53. The NIST SP 800-53 Table D-1 control baselines do not characterize controls as having relationships with security objectives.

b. Focus of Confidentiality (C), Integrity (I), and Availability (A). The determination was made that—

- The C and I objectives are largely focused on reading and writing (disclosure and modification).
- The A objective is more concerned with survivability and ensuring that the resources were there when needed.
- The A objective is also concerned with consequence management and countering certain activities aimed at denial of service.
- The I objective is also concerned with the correctness of actions.

c. The application of these rules resulted in consequences to the binning of the various families. For example, the controls/enhancements of the AC family were largely binned as CI, the controls and enhancements for the CP family were largely binned as A, and the controls and enhancements for the SA family were largely binned as I.

d. **Accountability.** The controls and enhancements focusing on Accountability (largely the AU and IA families) were binned CI, unless explicitly indicated otherwise.

e. **Class of Family.** The families that were categorized as Management or Operational were largely binned as CIA; that is, they did not support any one or two objectives, but rather were equally applicable to all three objectives. This was not a firm rule. The CP family was largely binned as A, and the SA and SI families were largely binned as I.

f. **X-1.** The first entry in each family (AU-1, CA-1) was often hard to bin because it covers the policy and procedure for the entire family. The determination was made that the first control (X-1) of each family should be binned at the high-water mark (HWM) for that family; therefore it was binned as CIA in most instances.

g. **Cryptography.** Unless specified otherwise in the control, it was assumed that cryptographic methods provide the ability to address disclosure (by encrypting information) and integrity (through the use of hashes and encrypted hashes). Therefore, controls that address the use of cryptographic methods were binned as CI. If the control addressed using cryptography to protect the confidentiality of information, then it was binned only as C.

h. **PE Family.** The PE family was a dichotomy. Many of the controls/enhancements were focused on providing physical access control. Those were binned in a manner comparable to the majority of the AC family. Some of the controls/enhancements were focused on environmental issues (e.g., adequate a/c). Those controls/enhancements were largely binned as A.

Exceptions: There were always some exceptions to the rules. Thus, exceptions were found even in families that would appear to logically fall into a single objective (e.g., System Integrity).

Assumptions and Guidelines for Low Impact, Moderate Impact, and High Impact Binning

6. One development goal was for the baselines to approximate the needs for a majority of NSS, in order to minimize the efforts needed by organizations for tailoring the control selection. In producing the baselines, certain assumptions were employed with regard to either the systems or their environment. Among the key assumptions for these majority NSS were—

- The systems store, process, or transmit classified information.
- All users of the systems are cleared for access to the information stored, processed, or transmitted by the system and have formal access approval to all the information stored, processed, or transmitted by the system; some users may not have a need-to-know for all the information.
- The systems are multi-user (either serially or concurrently) in operation.
- The systems are housed in a physical complex.

7. Systems or environments that diverge from these assumptions may require tailoring of the selected controls and enhancements.

Table D-1 Legend

An X in the table signifies the control is allocated to a baseline. A blank signifies the control is not allocated to a baseline. Controls not allocated to a baseline can be allocated during the tailoring or supplementing steps of the selection process. A dash signifies the control was in an earlier revision of NIST SP 800-53, but has been withdrawn.

Table D–1: Security Control Baselines

			C	C	C	I	I	I	A	A	A
	ID	Title	L	M	H	L	M	H	L	M	H
1	AC-1	Access Control Policy And Procedures	X	X	X	X	X	X	X	X	X
2	AC-2	Account Management	X	X	X	X	X	X			
3	AC-2(1)	Account Management		X	X		X	X			
4	AC-2(2)	Account Management		X	X		X	X			
5	AC-2(3)	Account Management		X	X		X	X			
6	AC-2(4)	Account Management		X	X		X	X			
7	AC-2(5)	Account Management									
8	AC-2(6)	Account Management									
9	AC-2(7)	Account Management		X	X		X	X			
10	AC-3	Access Enforcement	X	X	X	X	X	X			
11	AC-3(1)	Access Enforcement	-	-	-	-	-	-	-	-	-
12	AC-3(2)	Access Enforcement									
13	AC-3(3)	Access Enforcement									
14	AC-3(4)	Access Enforcement	X	X	X	X	X	X			
15	AC-3(5)	Access Enforcement									
16	AC-3(6)	Access Enforcement									
17	AC-4	Information Flow Enforcement		X	X		X	X			
18	AC-4(1)	Information Flow Enforcement									

			C	C	C	I	I	I	A	A	A
	ID	Title	L	M	H	L	M	H	L	M	H
19	AC-4(2)	Information Flow Enforcement									
20	AC-4(3)	Information Flow Enforcement									
21	AC-4(4)	Information Flow Enforcement									
22	AC-4(5)	Information Flow Enforcement									
23	AC-4(6)	Information Flow Enforcement									
24	AC-4(7)	Information Flow Enforcement									
25	AC-4(8)	Information Flow Enforcement									
26	AC-4(9)	Information Flow Enforcement									
27	AC-4(10)	Information Flow Enforcement									
28	AC-4(11)	Information Flow Enforcement									
29	AC-4(12)	Information Flow Enforcement									
30	AC-4(13)	Information Flow Enforcement									
31	AC-4(15)	Information Flow Enforcement									
32	AC-4(15)	Information Flow Enforcement									
33	AC-4(16)	Information Flow Enforcement									
34	AC-4(17)	Information Flow Enforcement									
35	AC-5	Separation Of Duties		X	X		X	X			
36	AC-6	Least Privilege		X	X		X	X			
37	AC-6(1)	Least Privilege		X	X		X	X			
38	AC-6(2)	Least Privilege		X	X		X	X			
39	AC-6(3)	Least Privilege									
40	AC-6(4)	Least Privilege									
41	AC-6(5)	Least Privilege		X	X		X	X			
42	AC-6(6)	Least Privilege									
43	AC-7	Unsuccessful Login Attempts	X	X	X	X	X	X	X	X	X
44	AC-7(1)	Unsuccessful Login Attempts		X	X		X	X			
45	AC-7(2)	Unsuccessful Login Attempts									
46	AC-8	System Use Notification	X	X	X	X	X	X			
47	AC-9	Previous Logon (Access) Notification					X	X			
48	AC-9(1)	Previous Logon (Access) Notification									
49	AC-9(2)	Previous Logon (Access) Notification									
50	AC-9(3)	Previous Logon (Access) Notification									
51	AC-10	Concurrent Session Control					X	X			
52	AC-11	Session Lock	X	X	X	X	X	X			
53	AC-11(1)	Session Lock	X	X	X						
54	AC-12	Session Termination	-	-	-	-	-	-	-	-	-
55	AC-13	Supervision And Review — Access Control	-	-	-	-	-	-	-	-	-
56	AC-14	Permitted Actions Without Identification Or Authentication	X	X	X	X	X	X			
57	AC-14(1)	Permitted Actions Without Identification Or Authentication		X	X		X	X			
58	AC-15	Automated Marking	-	-	-	-	-	-	-	-	-
59	AC-16	Security Attributes	X	X	X	X	X	X			
60	AC-16(1)	Security Attributes									
61	AC-16(2)	Security Attributes									
62	AC-16(3)	Security Attributes									
63	AC-16(4)	Security Attributes	X	X	X	X	X	X			
64	AC-16(5)	Security Attributes									
65	AC-17	Remote Access	X	X	X	X	X	X			
66	AC-17(1)	Remote Access		X	X		X	X			
67	AC-17(2)	Remote Access	X	X	X	X	X	X			
68	AC-17(3)	Remote Access		X	X		X	X			
69	AC-17(4)	Remote Access		X	X		X	X			
70	AC-17(5)	Remote Access		X	X		X	X			
71	AC-17(6)	Remote Access		X	X						
72	AC-17(7)	Remote Access		X	X		X	X			
73	AC-17(8)	Remote Access		X	X		X	X			
74	AC-18	Wireless Access Restrictions	X	X	X	X	X	X			
75	AC-18(1)	Wireless Access Restrictions		X	X		X	X			
76	AC-18(2)	Wireless Access Restrictions		X	X		X	X			
77	AC-18(3)	Wireless Access Restrictions		X	X		X	X			

			C	C	C	I	I	I	A	A	A
	ID	Title	L	M	H	L	M	H	L	M	H
78	AC-18(4)	Wireless Access Restrictions		X	X		X	X			
79	AC-18(5)	Wireless Access Restrictions		X	X		X	X			
80	AC-19	Access Control For Mobile Devices	X	X	X	X	X	X			
81	AC-19(1)	Access Control For Mobile Devices		X	X						
82	AC-19(2)	Access Control For Mobile Devices		X	X		X	X			
83	AC-19(3)	Access Control For Mobile Devices		X	X		X	X			
84	AC-19(4)	Access Control For Mobile Devices	X	X	X						
85	AC-20	Use Of External Information Systems	X	X	X	X	X	X			
86	AC-20(1)	Use Of External Information Systems		X	X		X	X			
87	AC-20(2)	Use Of External Information Systems		X	X						
88	AC-21	User-Based Collaboration And Information Sharing									
89	AC-21(1)	User-Based Collaboration And Information Sharing									
90	AC-22	Publicly Accessible Content	X	X	X						
91	AT-1	Security Awareness And Training Policy And Procedures	X	X	X	X	X	X	X	X	X
92	AT-2	Security Awareness	X	X	X	X	X	X	X	X	X
93	AT-2(1)	Security Awareness									
94	AT-3	Security Training	X	X	X	X	X	X	X	X	X
95	AT-3(1)	Security Training									
96	AT-3(2)	Security Training		X	X		X	X		X	X
97	AT-4	Security Training Records	X	X	X	X	X	X	X	X	X
98	AT-5	Contacts With Security Groups And Associations									
99	AU-1	Audit And Accountability Policy And Procedures	X	X	X	X	X	X	X	X	X
100	AU-2	Auditable Events	X	X	X	X	X	X			
101	AU-2(1)	Auditable Events	-	-	-	-	-	-	-	-	-
102	AU-2(2)	Auditable Events	-	-	-	-	-	-	-	-	-
103	AU-2(3)	Auditable Events		X	X		X	X			
104	AU-2(4)	Auditable Events	X	X	X	X	X	X			
105	AU-3	Content Of Audit Records	X	X	X	X	X	X			
106	AU-3(1)	Content Of Audit Records		X	X		X	X			
107	AU-3(2)	Content Of Audit Records			X			X			
108	AU-4	Audit Storage Capacity							X	X	X
109	AU-5	Response To Audit Processing Failures							X	X	X
110	AU-5(1)	Response To Audit Processing Failures									X
111	AU-5(2)	Response To Audit Processing Failures									X
112	AU-5(3)	Response To Audit Processing Failures									
113	AU-5(4)	Response To Audit Processing Failures									
114	AU-6	Audit Review, Analysis, And Reporting	X	X	X	X	X	X			
115	AU-6(1)	Audit Review, Analysis, And Reporting			X			X			
116	AU-6(2)	Audit Review, Analysis, And Reporting	-	-	-	-	-	-	-	-	-
117	AU-6(3)	Audit Review, Analysis, And Reporting									
118	AU-6(4)	Audit Review, Analysis, And Reporting									
119	AU-6(5)	Audit Review, Analysis, And Reporting									
120	AU-6(6)	Audit Review, Analysis, And Reporting									
121	AU-6(7)	Audit Review, Analysis, And Reporting									
122	AU-6(8)	Audit Review, Analysis, And Reporting		X	X		X	X			
123	AU-6(9)	Audit Review, Analysis, And Reporting									
124	AU-7	Audit Reduction And Report Generation		X	X		X	X			
125	AU-7(1)	Audit Reduction And Report Generation		X	X		X	X			
126	AU-8	Time Stamps				X	X	X			
127	AU-8(1)	Time Stamps					X	X			
128	AU-9	Protection Of Audit Information	X	X	X	X	X	X			
129	AU-9(1)	Protection Of Audit Information									
130	AU-9(2)	Protection Of Audit Information									
131	AU-9(3)	Protection Of Audit Information									
132	AU-9(4)	Protection Of Audit Information									
133	AU-10	Non-Repudiation					X	X			
134	AU-10(1)	Non-Repudiation									
135	AU-10(2)	Non-Repudiation									
136	AU-10(3)	Non-Repudiation									

			C	C	C	I	I	I	A	A	A
	ID	Title	L	M	H	L	M	H	L	M	H
137	AU-10(4)	Non-Repudiation									
138	AU-10(5)	Non-Repudiation					X	X			
139	AU-11	Audit Record Retention							X	X	X
140	AU-12	Audit Generation	X	X	X	X	X	X	X	X	X
141	AU-12(1)	Audit Generation						X			
142	AU-12(2)	Audit Generation									
143	AU-13	Monitoring For Information Disclosure									
144	AU-14	Session Audit									
145	AU-14(1)	Session Audit									
146	CA-1	Security Assessment And Authorization Policies And Procedures	X	X	X	X	X	X	X	X	X
147	CA-2	Security Assessments	X	X	X	X	X	X	X	X	X
148	CA-2(1)	Security Assessments		X	X		X	X		X	X
149	CA-2(2)	Security Assessments		X	X		X	X		X	X
150	CA-3	Information System Connections	X	X	X	X	X	X			
151	CA-3(1)	Information System Connections									
152	CA-3(2)	Information System Connections	X	X	X						
153	CA-4	Security Certification	-	-	-	-	-	-	-	-	-
154	CA-5	Plan Of Action And Milestones	X	X	X	X	X	X	X	X	X
155	CA-5(1)	Plan Of Action And Milestones									
156	CA-6	Security Authorization	X	X	X	X	X	X	X	X	X
157	CA-7	Continuous Monitoring	X	X	X	X	X	X	X	X	X
158	CA-7(1)	Continuous Monitoring		X	X		X	X		X	X
159	CA-7(2)	Continuous Monitoring		X	X		X	X		X	X
160	CM-1	Configuration Management Policy And Procedures	X	X	X	X	X	X			
161	CM-2	Baseline Configuration				X	X	X			
162	CM-2(1)	Baseline Configuration					X	X			
163	CM-2(2)	Baseline Configuration						X			
164	CM-2(3)	Baseline Configuration					X	X			
165	CM-2(4)	Baseline Configuration					X				
166	CM-2(5)	Baseline Configuration						X			
167	CM-2(6)	Baseline Configuration						X			
168	CM-3	Configuration Change Control					X	X			
169	CM-3(1)	Configuration Change Control						X			
170	CM-3(2)	Configuration Change Control					X	X			
171	CM-3(3)	Configuration Change Control									
172	CM-3(4)	Configuration Change Control					X	X			
173	CM-4	Security Impact Analysis					X	X			
174	CM-4(1)	Security Impact Analysis						X			
175	CM-4(2)	Security Impact Analysis									
176	CM-5	Access Restrictions For Change					X	X			
177	CM-5(1)	Access Restrictions For Change					X	X			
178	CM-5(2)	Access Restrictions For Change						X			
179	CM-5(3)	Access Restrictions For Change						X			
180	CM-5(4)	Access Restrictions For Change									
181	CM-5(5)	Access Restrictions For Change									
182	CM-5(6)	Access Restrictions For Change					X	X			
183	CM-5(7)	Access Restrictions For Change									
184	CM-6	Configuration Settings				X	X	X			
185	CM-6(1)	Configuration Settings						X			
186	CM-6(2)	Configuration Settings						X			
187	CM-6(3)	Configuration Settings					X	X			
188	CM-6(4)	Configuration Settings									
189	CM-7	Least Functionality	X	X	X	X	X	X			
190	CM-7(1)	Least Functionality		X	X		X	X			
191	CM-7(2)	Least Functionality			X			X			
192	CM-7(3)	Least Functionality		X	X		X	X			
193	CM-8	Information System Component Inventory				X	X	X			
194	CM-8(1)	Information System Component Inventory					X	X			
195	CM-8(2)	Information System Component Inventory						X			

			C	C	C	I	I	I	A	A	A
	ID	Title	L	M	H	L	M	H	L	M	H
196	CM-8(3)	Information System Component Inventory						X			
197	CM-8(4)	Information System Component Inventory						X			
198	CM-8(5)	Information System Component Inventory					X	X			
199	CM-8(6)	Information System Component Inventory									
200	CM-9	Configuration Management Plan					X	X			
201	CM-9(1)	Configuration Management Plan									
202	CP-1	Contingency Planning Policy And Procedures	X	X	X	X	X	X	X	X	X
203	CP-2	Contingency Plan							X	X	X
204	CP-2(1)	Contingency Plan								X	X
205	CP-2(2)	Contingency Plan									X
206	CP-2(3)	Contingency Plan									X
207	CP-2(4)	Contingency Plan									X
208	CP-2(5)	Contingency Plan									X
209	CP-2(6)	Contingency Plan									
210	CP-3	Contingency Training							X	X	X
211	CP-3(1)	Contingency Training									X
212	CP-3(2)	Contingency Training									
213	CP-4	Contingency Plan Testing And Exercises							X	X	X
214	CP-4(1)	Contingency Plan Testing And Exercises								X	X
215	CP-4(2)	Contingency Plan Testing And Exercises									X
216	CP-4(3)	Contingency Plan Testing And Exercises									
217	CP-4(4)	Contingency Plan Testing And Exercises								X	X
218	CP-5	Contingency Plan Update	-	-	-	-	-	-	-	-	-
219	CP-6	Alternate Storage Site								X	X
220	CP-6(1)	Alternate Storage Site								X	X
221	CP-6(2)	Alternate Storage Site									X
222	CP-6(3)	Alternate Storage Site								X	X
223	CP-7	Alternate Processing Site								X	X
224	CP-7(1)	Alternate Processing Site								X	X
225	CP-7(2)	Alternate Processing Site								X	X
226	CP-7(3)	Alternate Processing Site								X	X
227	CP-7(4)	Alternate Processing Site								X	X
228	CP-7(5)	Alternate Processing Site		X	X		X	X		X	X
229	CP-8	Telecommunications Services								X	X
230	CP-8(1)	Telecommunications Services								X	X
231	CP-8(2)	Telecommunications Services								X	X
232	CP-8(3)	Telecommunications Services									X
233	CP-8(4)	Telecommunications Services									X
234	CP-9	Information System Backup	X	X	X	X	X	X	X	X	X
235	CP-9(1)	Information System Backup					X	X		X	X
236	CP-9(2)	Information System Backup						X			X
237	CP-9(3)	Information System Backup									X
238	CP-9(4)	Information System Backup	-	-	-	-	-	-	-	-	-
239	CP-9(5)	Information System Backup									
240	CP-9(6)	Information System Backup									
241	CP-10	Information System Recovery And Reconstitution							X	X	X
242	CP-10(1)	Information System Recovery And Reconstitution	-	-	-	-	-	-	-	-	-
243	CP-10(2)	Information System Recovery And Reconstitution					X	X		X	X
244	CP-10(3)	Information System Recovery And Reconstitution								X	X
245	CP-10(4)	Information System Recovery And Reconstitution						X			X
246	CP-10(5)	Information System Recovery And Reconstitution									
247	CP-10(6)	Information System Recovery And Reconstitution								X	X
248	IA-1	Identification And Authentication Policy And Procedures	X	X	X	X	X	X			
249	IA-2	Identification And Authentication (Organizational Users)	X	X	X	X	X	X			
250	IA-2(1)	Identification And Authentication (Organizational Users)	X	X	X	X	X	X			
251	IA-2(2)	Identification And Authentication (Organizational Users)		X	X		X	X			
252	IA-2(3)	Identification And Authentication (Organizational Users)		X	X		X	X			
253	IA-2(4)	Identification And Authentication (Organizational Users)			X			X			
254	IA-2(5)	Identification And Authentication (Organizational Users)		X	X		X	X			

			C	C	C	I	I	I	A	A	A
	ID	Title	L	M	H	L	M	H	L	M	H
255	IA-2(6)	Identification And Authentication (Organizational Users)									
256	IA-2(7)	Identification And Authentication (Organizational Users)									
257	IA-2(8)	Identification And Authentication (Organizational Users)	X	X	X	X	X	X			
258	IA-2(9)	Identification And Authentication (Organizational Users)		X	X		X	X			
259	IA-3	Device Identification And Authentication		X	X		X	X			
260	IA-3(1)	Device Identification And Authentication									
261	IA-3(2)	Device Identification And Authentication									
262	IA-3(3)	Device Identification And Authentication									
263	IA-4	Identifier Management	X	X	X	X	X	X			
264	IA-4(1)	Identifier Management									
265	IA-4(2)	Identifier Management									
266	IA-4(3)	Identifier Management									
267	IA-4(4)	Identifier Management		X	X		X	X			
268	IA-4(5)	Identifier Management									
269	IA-5	Authenticator Management	X	X	X	X	X	X			
270	IA-5(1)	Authenticator Management		X	X		X	X			
271	IA-5(2)	Authenticator Management					X	X			
272	IA-5(3)	Authenticator Management					X	X			
273	IA-5(4)	Authenticator Management		X	X		X	X			
274	IA-5(5)	Authenticator Management									
275	IA-5(6)	Authenticator Management	X	X	X	X	X	X			
276	IA-5(7)	Authenticator Management		X	X						
277	IA-5(8)	Authenticator Management									
278	IA-6	Authenticator Feedback	X	X	X						
279	IA-7	Cryptographic Module Authentication	X	X	X	X	X	X			
280	IA-8	Identification And Authentication (Non-Organizational Users)	X	X	X	X	X	X			
281	IR-1	Incident Response Policy And Procedures	X	X	X	X	X	X	X	X	X
282	IR-2	Incident Response Training	X	X	X	X	X	X	X	X	X
283	IR-2(1)	Incident Response Training			X			X			X
284	IR-2(2)	Incident Response Training			X			X			X
285	IR-3	Incident Response Testing And Exercises		X	X		X	X		X	X
286	IR-3(1)	Incident Response Testing And Exercises			X			X			X
287	IR-4	Incident Handling	X	X	X	X	X	X	X	X	X
288	IR-4(1)	Incident Handling		X	X		X	X		X	X
289	IR-4(2)	Incident Handling									
290	IR-4(3)	Incident Handling									
291	IR-4(4)	Incident Handling									
292	IR-4(5)	Incident Handling									
293	IR-5	Incident Monitoring	X	X	X	X	X	X	X	X	X
294	IR-5(1)	Incident Monitoring			X			X			X
295	IR-6	Incident Reporting	X	X	X	X	X	X	X	X	X
296	IR-6(1)	Incident Reporting		X	X		X	X		X	X
297	IR-6(2)	Incident Reporting									
298	IR-7	Incident Response Assistance	X	X	X	X	X	X	X	X	X
299	IR-7(1)	Incident Response Assistance		X	X		X	X		X	X
300	IR-7(2)	Incident Response Assistance									
301	IR-8	Incident Response Plan	X	X	X	X	X	X	X	X	X
302	MA-1	System Maintenance Policy And Procedures	X	X	X	X	X	X	X	X	X
303	MA-2	Controlled Maintenance	X	X	X	X	X	X	X	X	X
304	MA-2(1)	Controlled Maintenance		X	X		X	X		X	X
305	MA-2(2)	Controlled Maintenance			X			X			X
306	MA-3	Maintenance Tools				X	X	X	X	X	X
307	MA-3(1)	Maintenance Tools					X	X		X	X
308	MA-3(2)	Maintenance Tools					X	X		X	X
309	MA-3(3)	Maintenance Tools	X	X	X						
310	MA-3(4)	Maintenance Tools									
311	MA-4	Non-Local Maintenance				X	X	X			
312	MA-4(1)	Non-Local Maintenance					X	X			
313	MA-4(2)	Non-Local Maintenance					X	X			

			C	C	C	I	I	I	A	A	A
	ID	Title	L	M	H	L	M	H	L	M	H
314	MA-4(3)	Non-Local Maintenance			X			X			X
315	MA-4(4)	Non-Local Maintenance									
316	MA-4(5)	Non-Local Maintenance									
317	MA-4(6)	Non-Local Maintenance									
318	MA-4(7)	Non-Local Maintenance									
319	MA-5	Maintenance Personnel	X	X	X	X	X	X	X	X	X
320	MA-5(1)	Maintenance Personnel	X	X	X	X	X	X	X	X	X
321	MA-5(2)	Maintenance Personnel	X	X	X	X	X	X	X	X	X
322	MA-5(3)	Maintenance Personnel									
323	MA-5(4)	Maintenance Personnel	X	X	X	X	X	X	X	X	X
324	MA-6	Timely Maintenance								X	X
325	MP-1	Media Protection Policy And Procedures	X	X	X	X	X	X	X	X	X
326	MP-2	Media Access	X	X	X						
327	MP-2(1)	Media Access		X	X		X	X			
328	MP-2(2)	Media Access									
329	MP-3	Media Marking	X	X	X						
330	MP-4	Media Storage	X	X	X						
331	MP-4(1)	Media Storage	X	X	X						
332	MP-5	Media Transport		X	X		X	X			
333	MP-5(1)	Media Transport	-	-	-	-	-	-	-	-	-
334	MP-5(2)	Media Transport		X	X		X	X			
335	MP-5(3)	Media Transport			X			X			
336	MP-5(4)	Media Transport		X	X		X	X			
337	MP-6	Media Sanitization	X	X	X						
338	MP-6(1)	Media Sanitization			X						
339	MP-6(2)	Media Sanitization			X						
340	MP-6(3)	Media Sanitization			X						
341	MP-6(4)	Media Sanitization									
342	MP-6(5)	Media Sanitization	X	X	X						
343	MP-6(6)	Media Sanitization	X	X	X						
344	PE-1	Physical And Environmental Protection Policy And Procedures	X	X	X	X	X	X	X	X	X
345	PE-2	Physical Access Authorizations	X	X	X	X	X	X	X	X	X
346	PE-2(1)	Physical Access Authorizations									
347	PE-2(2)	Physical Access Authorizations									
348	PE-2(3)	Physical Access Authorizations	X	X	X						
349	PE-3	Physical Access Control	X	X	X	X	X	X	X	X	X
350	PE-3(1)	Physical Access Control			X			X			
351	PE-3(2)	Physical Access Control	X	X	X						
352	PE-3(3)	Physical Access Control	X	X	X	X	X	X			
353	PE-3(4)	Physical Access Control									
354	PE-3(5)	Physical Access Control									
355	PE-3(6)	Physical Access Control						X			
356	PE-4	Access Control For Transmission Medium		X	X		X	X			
357	PE-5	Access Control For Output Devices		X	X						
358	PE-6	Monitoring Physical Access	X	X	X	X	X	X	X	X	X
359	PE-6(1)	Monitoring Physical Access								X	X
360	PE-6(2)	Monitoring Physical Access			X			X			X
361	PE-7	Visitor Control	X	X	X	X	X	X			
362	PE-7(1)	Visitor Control		X	X		X	X			
363	PE-7(2)	Visitor Control									
364	PE-8	Access Records	X	X	X	X	X	X			
365	PE-8(1)	Access Records									X
366	PE-8(2)	Access Records									X
367	PE-9	Power Equipment And Power Cabling								X	X
368	PE-9(1)	Power Equipment And Power Cabling									
369	PE-9(2)	Power Equipment And Power Cabling								X	X
370	PE-10	Emergency Shutoff								X	X
371	PE-10(1)	Emergency Shutoff	-	-	-	-	-	-	-	-	-
372	PE-11	Emergency Power								X	X

			C	C	C	I	I	I	A	A	A
	ID	Title	L	M	H	L	M	H	L	M	H
373	PE-11(1)	Emergency Power								X	
374	PE-11(2)	Emergency Power									X
375	PE-12	Emergency Lighting							X	X	X
376	PE-12(1)	Emergency Lighting								X	X
377	PE-13	Fire Protection							X	X	X
378	PE-13(1)	Fire Protection								X	X
379	PE-13(2)	Fire Protection								X	X
380	PE-13(3)	Fire Protection								X	X
381	PE-13(4)	Fire Protection								X	X
382	PE-14	Temperature And Humidity Controls							X	X	X
383	PE-14(1)	Temperature And Humidity Controls								X	X
384	PE-14(2)	Temperature And Humidity Controls								X	X
385	PE-15	Water Damage Protection							X	X	X
386	PE-15(1)	Water Damage Protection									X
387	PE-16	Delivery And Removal	X	X	X				X	X	X
388	PE-17	Alternate Work Site		X	X		X	X		X	X
389	PE-18	Location Of Information System Components								X	X
390	PE-18(1)	Location Of Information System Components									X
391	PE-19	Information Leakage		X	X		X	X			
392	PE-19(1)	Information Leakage		X	X		X	X			
393	PL-1	Security Planning Policy And Procedures	X	X	X	X	X	X	X	X	X
394	PL-2	System Security Plan	X	X	X	X	X	X	X	X	X
395	PL-2(1)	System Security Plan		X	X		X	X		X	X
396	PL-2(2)	System Security Plan		X	X		X	X		X	X
397	PL-3	System Security Plan Update	-	-	-	-	-	-	-	-	-
398	PL-4	Rules Of Behavior	X	X	X	X	X	X	X	X	X
399	PL-4(1)	Rules Of Behavior									
400	PL-5	Privacy Impact Assessment	X	X	X						
401	PL-6	Security-Related Activity Planning		X	X		X	X		X	X
402	PS-1	Personnel Security Policy And Procedures	X	X	X	X	X	X	X	X	X
403	PS-2	Position Categorization	X	X	X	X	X	X	X	X	X
404	PS-3	Personnel Screening	X	X	X	X	X	X			
405	PS-3(1)	Personnel Screening	X	X	X						
406	PS-3(2)	Personnel Screening	X	X	X						
407	PS-4	Personnel Termination	X	X	X	X	X	X	X	X	X
408	PS-5	Personnel Transfer	X	X	X	X	X	X	X	X	X
409	PS-6	Access Agreements	X	X	X	X	X	X			
410	PS-6(1)	Access Agreements		X	X		X	X			
411	PS-6(2)	Access Agreements	X	X	X						
412	PS-7	Third-Party Personnel Security	X	X	X	X	X	X			
413	PS-8	Personnel Sanctions	X	X	X	X	X	X	X	X	X
414	RA-1	Risk Assessment Policy And Procedures	X	X	X	X	X	X	X	X	X
415	RA-2	Security Categorization	X	X	X	X	X	X	X	X	X
416	RA-3	Risk Assessment	X	X	X	X	X	X	X	X	X
417	RA-4	Risk Assessment Update	-	-	-	-	-	-	-	-	-
418	RA-5	Vulnerability Scanning	X	X	X	X	X	X	X	X	X
419	RA-5(1)	Vulnerability Scanning		X	X		X	X		X	X
420	RA-5(2)	Vulnerability Scanning		X	X		X	X		X	X
421	RA-5(3)	Vulnerability Scanning			X			X			X
422	RA-5(4)	Vulnerability Scanning			X			X			X
423	RA-5(5)	Vulnerability Scanning			X			X			X
424	RA-5(6)	Vulnerability Scanning									
425	RA-5(7)	Vulnerability Scanning			X			X			X
426	RA-5(8)	Vulnerability Scanning									
427	RA-5(9)	Vulnerability Scanning									
428	SA-1	System And Services Acquisition Policy And Procedures	X	X	X	X	X	X			
429	SA-2	Allocation Of Resources				X	X	X			
430	SA-3	Life Cycle Support				X	X	X			
431	SA-4	Acquisitions				X	X	X			

			C	C	C	I	I	I	A	A	A
	ID	Title	L	M	H	L	M	H	L	M	H
432	SA-4(1)	Acquisitions					X	X			
433	SA-4(2)	Acquisitions						X			
434	SA-4(3)	Acquisitions					X	X			
435	SA-4(4)	Acquisitions									
436	SA-4(5)	Acquisitions									
437	SA-4(6)	Acquisitions					X	X			
438	SA-4(7)	Acquisitions					X	X			
439	SA-5	Information System Documentation				X	X	X			
440	SA-5(1)	Information System Documentation					X	X			
441	SA-5(2)	Information System Documentation						X			
442	SA-5(3)	Information System Documentation					X	X			
443	SA-5(4)	Information System Documentation									
444	SA-5(5)	Information System Documentation									
445	SA-6	Software Usage Restrictions	X	X	X	X	X	X			
446	SA-6(1)	Software Usage Restrictions		X	X		X	X			
447	SA-7	User Installed Software				X	X	X			
448	SA-8	Security Engineering Principles					X	X			
449	SA-9	External Information System Services				X	X	X			
450	SA-9(1)	External Information System Services					X	X			
451	SA-10	Developer Configuration Management					X	X			
452	SA-10(1)	Developer Configuration Management									
453	SA-10(2)	Developer Configuration Management									
454	SA-11	Developer Security Testing					X	X			
455	SA-11(1)	Developer Security Testing									
456	SA-11(2)	Developer Security Testing									
457	SA-11(3)	Developer Security Testing									
458	SA-12	Supply Chain Protection					X	X			
459	SA-12(1)	Supply Chain Protection									
460	SA-12(2)	Supply Chain Protection					X	X			
461	SA-12(3)	Supply Chain Protection									
462	SA-12(4)	Supply Chain Protection									
463	SA-12(5)	Supply Chain Protection									
464	SA-12(6)	Supply Chain Protection									
465	SA-12(7)	Supply Chain Protection									
466	SA-13	Trustworthiness						X			
467	SA-14	Critical Information System Components					X	X			
468	SA-14(1)	Critical Information System Components					X	X			
469	SC-1	System And Communications Protection Policy And Procedures	X	X	X	X	X	X	X	X	X
470	SC-2	Application Partitioning		X	X		X	X			
471	SC-2(1)	Application Partitioning									
472	SC-3	Security Function Isolation		X	X		X	X			
473	SC-3(1)	Security Function Isolation									
474	SC-3(2)	Security Function Isolation									
475	SC-3(3)	Security Function Isolation									
476	SC-3(4)	Security Function Isolation									
477	SC-3(5)	Security Function Isolation									
478	SC-4	Information In Shared Resources		X	X						
479	SC-4(1)	Information In Shared Resources									
480	SC-5	Denial Of Service Protection							X	X	X
481	SC-5(1)	Denial Of Service Protection									
482	SC-5(2)	Denial Of Service Protection									
483	SC-6	Resource Priority									X
484	SC-7	Boundary Protection	X	X	X	X	X	X			
485	SC-7(1)	Boundary Protection		X	X		X	X			
486	SC-7(2)	Boundary Protection		X	X		X	X			
487	SC-7(3)	Boundary Protection		X	X		X	X			
488	SC-7(4)	Boundary Protection		X	X		X	X			
489	SC-7(5)	Boundary Protection		X	X		X	X			
490	SC-7(6)	Boundary Protection			X						

			C	C	C	I	I	I	A	A	A
	ID	Title	L	M	H	L	M	H	L	M	H
491	SC-7(7)	Boundary Protection		X	X		X	X			
492	SC-7(8)	Boundary Protection			X			X			
493	SC-7(9)	Boundary Protection									
494	SC-7(10)	Boundary Protection									
495	SC-7(11)	Boundary Protection									
496	SC-7(12)	Boundary Protection		X	X		X	X		X	X
497	SC-7(13)	Boundary Protection									
498	SC-7(14)	Boundary Protection									
499	SC-7(15)	Boundary Protection									
500	SC-7(16)	Boundary Protection									
501	SC-7(17)	Boundary Protection									
502	SC-7(18)	Boundary Protection	X	X	X	X	X	X	X	X	X
503	SC-8	Transmission Integrity				X	X	X			
504	SC-8(1)	Transmission Integrity					X	X			
505	SC-8(2)	Transmission Integrity					X	X			
506	SC-9	Transmission Confidentiality	X	X	X						
507	SC-9(1)	Transmission Confidentiality	X	X	X						
508	SC-9(2)	Transmission Confidentiality									
509	SC-10	Network Disconnect		X	X		X	X			
510	SC-11	Trusted Path									
511	SC-12	Cryptographic Key Establishment And Management	X	X	X	X	X	X			
512	SC-12(1)	Cryptographic Key Establishment And Management									X
513	SC-12(2)	Cryptographic Key Establishment And Management									
514	SC-12(3)	Cryptographic Key Establishment And Management									
515	SC-12(4)	Cryptographic Key Establishment And Management									
516	SC-12(5)	Cryptographic Key Establishment And Management									
517	SC-13	Use Of Cryptography	X	X	X	X	X	X			
518	SC-13(1)	Use Of Cryptography									
519	SC-13(2)	Use Of Cryptography	X	X	X						
520	SC-13(3)	Use Of Cryptography									
521	SC-13(4)	Use Of Cryptography									
522	SC-14	Public Access Protections				X	X	X	X	X	X
523	SC-15	Collaborative Computing Devices	X	X	X						
524	SC-15(1)	Collaborative Computing Devices									
525	SC-15(2)	Collaborative Computing Devices		X	X		X	X			
526	SC-15(3)	Collaborative Computing Devices									
527	SC-16	Transmission Of Security Attributes		X	X		X	X			
528	SC-16(1)	Transmission Of Security Attributes									
529	SC-17	Public Key Infrastructure Certificates		X	X		X	X			
530	SC-18	Mobile Code				X	X	X			
531	SC-18(1)	Mobile Code									
532	SC-18(2)	Mobile Code									
533	SC-18(3)	Mobile Code					X	X			
534	SC-18(4)	Mobile Code					X	X			
535	SC-19	Voice Over Internet Protocol		X	X		X	X			
536	SC-20	Secure Name / Address Resolution Service (Authoritative Source)				X	X	X			
537	SC-20(1)	Secure Name / Address Resolution Service (Authoritative Source)				X	X	X			
538	SC-21	Secure Name / Address Resolution Service (Recursive Or Caching Resolver)						X			
539	SC-21(1)	Secure Name / Address Resolution Service (Recursive Or Caching Resolver)									
540	SC-22	Architecture And Provisioning For Name / Address Resolution Service		X	X		X	X		X	X
541	SC-23	Session Authenticity					X	X			
542	SC-23(1)	Session Authenticity									
543	SC-23(2)	Session Authenticity									
544	SC-23(3)	Session Authenticity									
545	SC-23(4)	Session Authenticity									
546	SC-24	Fail In Known State		X	X		X	X			
547	SC-25	Thin Nodes									
548	SC-26	Honeypots									
549	SC-26(1)	Honeypots									

			C	C	C	I	I	I	A	A	A
	ID	Title	L	M	H	L	M	H	L	M	H
550	SC-27	Operating System-Independent Applications									
551	SC-28	Protection Of Information At Rest		X	X		X	X			
552	SC-28(1)	Protection Of Information At Rest		X	X		X	X			
553	SC-29	Heterogeneity									
554	SC-30	Virtualization Techniques									
555	SC-30(1)	Virtualization Techniques									
556	SC-30(2)	Virtualization Techniques									
557	SC-31	Covert Channel Analysis									
558	SC-31(1)	Covert Channel Analysis									
559	SC-32	Information System Partitioning		X	X		X	X			
560	SC-33	Transmission Preparation Integrity									
561	SC-34	Non-modifiable executable programs									
562	SC-34(1)	Non-modifiable executable programs									
563	SC-34(2)	Non-modifiable executable programs									
564	SI-1	System And Information Integrity Policy And Procedures	X	X	X	X	X	X	X	X	X
565	SI-2	Flaw Remediation				X	X	X			
566	SI-2(1)	Flaw Remediation						X			
567	SI-2(2)	Flaw Remediation					X	X			
568	SI-2(3)	Flaw Remediation									
569	SI-2(4)	Flaw Remediation									
570	SI-3	Malicious Code Protection				X	X	X			
571	SI-3(1)	Malicious Code Protection					X	X			
572	SI-3(2)	Malicious Code Protection					X	X			
573	SI-3(3)	Malicious Code Protection					X	X			
574	SI-3(4)	Malicious Code Protection									
575	SI-3(5)	Malicious Code Protection									
576	SI-3(6)	Malicious Code Protection									
577	SI-4	Information System Monitoring					X	X			
578	SI-4(1)	Information System Monitoring									
579	SI-4(2)	Information System Monitoring					X	X			
580	SI-4(3)	Information System Monitoring									
581	SI-4(4)	Information System Monitoring			X		X	X			
582	SI-4(5)	Information System Monitoring					X	X			
583	SI-4(6)	Information System Monitoring					X	X			
584	SI-4(7)	Information System Monitoring									
585	SI-4(8)	Information System Monitoring									
586	SI-4(9)	Information System Monitoring									
587	SI-4(10)	Information System Monitoring		X	X		X	X			
588	SI-4(11)	Information System Monitoring									
589	SI-4(12)	Information System Monitoring									
590	SI-4(13)	Information System Monitoring									
591	SI-4(14)	Information System Monitoring									
592	SI-4(15)	Information System Monitoring									
593	SI-4(16)	Information System Monitoring									
594	SI-4(17)	Information System Monitoring									
595	SI-5	Security Alerts, Advisories, And Directives				X	X	X			
596	SI-5(1)	Security Alerts, Advisories, And Directives						X			
597	SI-6	Security Functionality Verification					X	X			
598	SI-6(1)	Security Functionality Verification									
599	SI-6(2)	Security Functionality Verification									
600	SI-6(3)	Security Functionality Verification									
601	SI-7	Software And Information Integrity					X	X			
602	SI-7(1)	Software And Information Integrity					X	X			
603	SI-7(2)	Software And Information Integrity						X			
604	SI-7(3)	Software And Information Integrity									
605	SI-7(4)	Software And Information Integrity									
606	SI-8	Spam Protection				X	X	X	X	X	X
607	SI-8(1)	Spam Protection						X			X
608	SI-8(2)	Spam Protection									

			C	C	C	I	I	I	A	A	A
	ID	Title	L	M	H	L	M	H	L	M	H
609	SI-9	Information Input Restrictions					X	X			
610	SI-10	Information Input Validation					X	X			
611	SI-11	Error Handling					X	X			
612	SI-12	Information Output Handling And Retention	X	X	X	X	X	X			
613	SI-13	Predictable Failure Prevention									
614	SI-13(1)	Predictable Failure Prevention									
615	SI-13(2)	Predictable Failure Prevention									
616	SI-13(3)	Predictable Failure Prevention									
617	SI-13(4)	Predictable Failure Prevention									

Table D–2: Control Relationships to Security Objectives

	ID	Title	C	I	A
1	AC-1	Access Control Policy And Procedures	X	X	X
2	AC-2	Account Management	X	X	
3	AC-2(1)	Account Management	X	X	
4	AC-2(2)	Account Management	X	X	
5	AC-2(3)	Account Management	X	X	
6	AC-2(4)	Account Management	X	X	
7	AC-2(5)	Account Management	X	X	
8	AC-2(6)	Account Management	X	X	
9	AC-2(7)	Account Management	X	X	
10	AC-3	Access Enforcement	X	X	
11	AC-3(1)	Access Enforcement	-	-	-
12	AC-3(2)	Access Enforcement	X	X	
13	AC-3(3)	Access Enforcement	X	X	
14	AC-3(4)	Access Enforcement	X	X	
15	AC-3(5)	Access Enforcement	X	X	
16	AC-3(6)	Access Enforcement	X	X	
17	AC-4	Information Flow Enforcement	X	X	
18	AC-4(1)	Information Flow Enforcement	X	X	
19	AC-4(2)	Information Flow Enforcement	X	X	
20	AC-4(3)	Information Flow Enforcement	X	X	
21	AC-4(4)	Information Flow Enforcement	X	X	
22	AC-4(5)	Information Flow Enforcement	X	X	
23	AC-4(6)	Information Flow Enforcement	X	X	
24	AC-4(7)	Information Flow Enforcement	X	X	
25	AC-4(8)	Information Flow Enforcement	X	X	
26	AC-4(9)	Information Flow Enforcement	X	X	
27	AC-4(10)	Information Flow Enforcement	X	X	
28	AC-4(11)	Information Flow Enforcement	X	X	
29	AC-4(12)	Information Flow Enforcement	X	X	
30	AC-4(13)	Information Flow Enforcement	X	X	
31	AC-4(15)	Information Flow Enforcement	X	X	
32	AC-4(15)	Information Flow Enforcement	X	X	
33	AC-4(16)	Information Flow Enforcement	X	X	
34	AC-4(17)	Information Flow Enforcement	X	X	
35	AC-5	Separation Of Duties	X	X	
36	AC-6	Least Privilege	X	X	
37	AC-6(1)	Least Privilege	X	X	
38	AC-6(2)	Least Privilege	X	X	
39	AC-6(3)	Least Privilege	X	X	
40	AC-6(4)	Least Privilege	X	X	
41	AC-6(5)	Least Privilege	X	X	
42	AC-6(6)	Least Privilege	X	X	

	ID	Title	C	I	A
43	AC-7	Unsuccessful Login Attempts	X	X	X
44	AC-7(1)	Unsuccessful Login Attempts	X	X	
45	AC-7(2)	Unsuccessful Login Attempts	X		
46	AC-8	System Use Notification	X	X	
47	AC-9	Previous Logon (Access) Notification		X	
48	AC-9(1)	Previous Logon (Access) Notification		X	
49	AC-9(2)	Previous Logon (Access) Notification		X	
50	AC-9(3)	Previous Logon (Access) Notification		X	
51	AC-10	Concurrent Session Control		X	
52	AC-11	Session Lock	X	X	
53	AC-11(1)	Session Lock	X		
54	AC-12	Session Termination	-	-	-
55	AC-13	Supervision And Review — Access Control	-	-	-
56	AC-14	Permitted Actions Without Identification Or Authentication	X	X	
57	AC-14(1)	Permitted Actions Without Identification Or Authentication	X	X	
58	AC-15	Automated Marking	-	-	-
59	AC-16	Security Attributes	X	X	
60	AC-16(1)	Security Attributes	X	X	
61	AC-16(2)	Security Attributes		X	
62	AC-16(3)	Security Attributes		X	
63	AC-16(4)	Security Attributes	X	X	
64	AC-16(5)	Security Attributes	X		
65	AC-17	Remote Access	X	X	
66	AC-17(1)	Remote Access	X	X	
67	AC-17(2)	Remote Access	X	X	
68	AC-17(3)	Remote Access	X	X	
69	AC-17(4)	Remote Access	X	X	
70	AC-17(5)	Remote Access	X	X	
71	AC-17(6)	Remote Access	X		
72	AC-17(7)	Remote Access	X	X	
73	AC-17(8)	Remote Access	X	X	
74	AC-18	Wireless Access Restrictions	X	X	
75	AC-18(1)	Wireless Access Restrictions	X	X	
76	AC-18(2)	Wireless Access Restrictions	X	X	
77	AC-18(3)	Wireless Access Restrictions	X	X	
78	AC-18(4)	Wireless Access Restrictions	X	X	
79	AC-18(5)	Wireless Access Restrictions	X	X	
80	AC-19	Access Control For Mobile Devices	X	X	
81	AC-19(1)	Access Control For Mobile Devices	X		
82	AC-19(2)	Access Control For Mobile Devices	X	X	
83	AC-19(3)	Access Control For Mobile Devices	X	X	
84	AC-19(4)	Access Control For Mobile Devices	X		
85	AC-20	Use Of External Information Systems	X	X	
86	AC-20(1)	Use Of External Information Systems	X	X	
87	AC-20(2)	Use Of External Information Systems	X		
88	AC-21	User-Based Collaboration And Information Sharing	X		
89	AC-21(1)	User-Based Collaboration And Information Sharing	X		
90	AC-22	Publicly Accessible Content	X		
91	AT-1	Security Awareness And Training Policy And Procedures	X	X	X
92	AT-2	Security Awareness	X	X	X
93	AT-2(1)	Security Awareness	X	X	X
94	AT-3	Security Training	X	X	X
95	AT-3(1)	Security Training			X
96	AT-3(2)	Security Training	X	X	X
97	AT-4	Security Training Records	X	X	X
98	AT-5	Contacts With Security Groups And Associations	X	X	X
99	AU-1	Audit And Accountability Policy And Procedures	X	X	X
100	AU-2	Auditable Events	X	X	
101	AU-2(1)	Auditable Events	-	-	-

	ID	Title	C	I	A
102	AU-2(2)	Auditable Events	-	-	-
103	AU-2(3)	Auditable Events	X	X	
104	AU-2(4)	Auditable Events	X	X	
105	AU-3	Content Of Audit Records	X	X	
106	AU-3(1)	Content Of Audit Records	X	X	
107	AU-3(2)	Content Of Audit Records	X	X	
108	AU-4	Audit Storage Capacity			X
109	AU-5	Response To Audit Processing Failures			X
110	AU-5(1)	Response To Audit Processing Failures			X
111	AU-5(2)	Response To Audit Processing Failures			X
112	AU-5(3)	Response To Audit Processing Failures			X
113	AU-5(4)	Response To Audit Processing Failures	X	X	
114	AU-6	Audit Review, Analysis, And Reporting	X	X	
115	AU-6(1)	Audit Review, Analysis, And Reporting	X	X	
116	AU-6(2)	Audit Review, Analysis, And Reporting	-	-	-
117	AU-6(3)	Audit Review, Analysis, And Reporting	X	X	
118	AU-6(4)	Audit Review, Analysis, And Reporting	X	X	
119	AU-6(5)	Audit Review, Analysis, And Reporting	X	X	
120	AU-6(6)	Audit Review, Analysis, And Reporting	X	X	
121	AU-6(7)	Audit Review, Analysis, And Reporting	X	X	
122	AU-6(8)	Audit Review, Analysis, And Reporting	X	X	
123	AU-6(9)	Audit Review, Analysis, And Reporting	X	X	
124	AU-7	Audit Reduction And Report Generation	X	X	
125	AU-7(1)	Audit Reduction And Report Generation	X	X	
126	AU-8	Time Stamps		X	
127	AU-8(1)	Time Stamps		X	
128	AU-9	Protection Of Audit Information	X	X	
129	AU-9(1)	Protection Of Audit Information		X	
130	AU-9(2)	Protection Of Audit Information			X
131	AU-9(3)	Protection Of Audit Information		X	
132	AU-9(4)	Protection Of Audit Information		X	
133	AU-10	Non-Repudiation		X	
134	AU-10(1)	Non-Repudiation		X	
135	AU-10(2)	Non-Repudiation		X	
136	AU-10(3)	Non-Repudiation		X	
137	AU-10(4)	Non-Repudiation		X	
138	AU-10(5)	Non-Repudiation		X	
139	AU-11	Audit Record Retention			X
140	AU-12	Audit Generation	X	X	X
141	AU-12(1)	Audit Generation		X	
142	AU-12(2)	Audit Generation		X	
143	AU-13	Monitoring For Information Disclosure	X		
144	AU-14	Session Audit			X
145	AU-14(1)	Session Audit			X
146	CA-1	Security Assessment And Authorization Policies And Procedures	X	X	X
147	CA-2	Security Assessments	X	X	X
148	CA-2(1)	Security Assessments	X	X	X
149	CA-2(2)	Security Assessments	X	X	X
150	CA-3	Information System Connections	X	X	
151	CA-3(1)	Information System Connections	X		
152	CA-3(2)	Information System Connections	X		
153	CA-4	Security Certification	-	-	-
154	CA-5	Plan Of Action And Milestones	X	X	X
155	CA-5(1)	Plan Of Action And Milestones	X	X	X
156	CA-6	Security Authorization	X	X	X
157	CA-7	Continuous Monitoring	X	X	X
158	CA-7(1)	Continuous Monitoring	X	X	X
159	CA-7(2)	Continuous Monitoring	X	X	X
160	CM-1	Configuration Management Policy And Procedures	X	X	

	ID	Title	C	I	A
161	CM-2	Baseline Configuration		X	
162	CM-2(1)	Baseline Configuration		X	
163	CM-2(2)	Baseline Configuration		X	
164	CM-2(3)	Baseline Configuration		X	
165	CM-2(4)	Baseline Configuration		X	
166	CM-2(5)	Baseline Configuration		X	
167	CM-2(6)	Baseline Configuration		X	
168	CM-3	Configuration Change Control		X	
169	CM-3(1)	Configuration Change Control		X	
170	CM-3(2)	Configuration Change Control		X	
171	CM-3(3)	Configuration Change Control		X	
172	CM-3(4)	Configuration Change Control		X	
173	CM-4	Security Impact Analysis		X	
174	CM-4(1)	Security Impact Analysis		X	
175	CM-4(2)	Security Impact Analysis		X	
176	CM-5	Access Restrictions For Change		X	
177	CM-5(1)	Access Restrictions For Change		X	
178	CM-5(2)	Access Restrictions For Change		X	
179	CM-5(3)	Access Restrictions For Change		X	
180	CM-5(4)	Access Restrictions For Change		X	
181	CM-5(5)	Access Restrictions For Change		X	
182	CM-5(6)	Access Restrictions For Change		X	
183	CM-5(7)	Access Restrictions For Change		X	
184	CM-6	Configuration Settings		X	
185	CM-6(1)	Configuration Settings		X	
186	CM-6(2)	Configuration Settings		X	
187	CM-6(3)	Configuration Settings		X	
188	CM-6(4)	Configuration Settings		X	
189	CM-7	Least Functionality	X	X	
190	CM-7(1)	Least Functionality	X	X	
191	CM-7(2)	Least Functionality	X	X	
192	CM-7(3)	Least Functionality	X	X	
193	CM-8	Information System Component Inventory		X	
194	CM-8(1)	Information System Component Inventory		X	
195	CM-8(2)	Information System Component Inventory		X	
196	CM-8(3)	Information System Component Inventory		X	
197	CM-8(4)	Information System Component Inventory		X	
198	CM-8(5)	Information System Component Inventory		X	
199	CM-8(6)	Information System Component Inventory		X	
200	CM-9	Configuration Management Plan		X	
201	CM-9(1)	Configuration Management Plan		X	
202	CP-1	Contingency Planning Policy And Procedures	X	X	X
203	CP-2	Contingency Plan			X
204	CP-2(1)	Contingency Plan			X
205	CP-2(2)	Contingency Plan			X
206	CP-2(3)	Contingency Plan			X
207	CP-2(4)	Contingency Plan			X
208	CP-2(5)	Contingency Plan			X
209	CP-2(6)	Contingency Plan			X
210	CP-3	Contingency Training			X
211	CP-3(1)	Contingency Training			X
212	CP-3(2)	Contingency Training			X
213	CP-4	Contingency Plan Testing And Exercises			X
214	CP-4(1)	Contingency Plan Testing And Exercises			X
215	CP-4(2)	Contingency Plan Testing And Exercises			X
216	CP-4(3)	Contingency Plan Testing And Exercises			X
217	CP-4(4)	Contingency Plan Testing And Exercises			X
218	CP-5	Contingency Plan Update	-	-	-
219	CP-6	Alternate Storage Site			X

	ID	Title	C	I	A
220	CP-6(1)	Alternate Storage Site			X
221	CP-6(2)	Alternate Storage Site			X
222	CP-6(3)	Alternate Storage Site			X
223	CP-7	Alternate Processing Site			X
224	CP-7(1)	Alternate Processing Site			X
225	CP-7(2)	Alternate Processing Site			X
226	CP-7(3)	Alternate Processing Site			X
227	CP-7(4)	Alternate Processing Site			X
228	CP-7(5)	Alternate Processing Site	X	X	X
229	CP-8	Telecommunications Services			X
230	CP-8(1)	Telecommunications Services			X
231	CP-8(2)	Telecommunications Services			X
232	CP-8(3)	Telecommunications Services			X
233	CP-8(4)	Telecommunications Services			X
234	CP-9	Information System Backup	X	X	X
235	CP-9(1)	Information System Backup		X	X
236	CP-9(2)	Information System Backup		X	X
237	CP-9(3)	Information System Backup			X
238	CP-9(4)	Information System Backup	-	-	-
239	CP-9(5)	Information System Backup			X
240	CP-9(6)	Information System Backup			X
241	CP-10	Information System Recovery And Reconstitution			X
242	CP-10(1)	Information System Recovery And Reconstitution	-	-	-
243	CP-10(2)	Information System Recovery And Reconstitution		X	X
244	CP-10(3)	Information System Recovery And Reconstitution			X
245	CP-10(4)	Information System Recovery And Reconstitution		X	X
246	CP-10(5)	Information System Recovery And Reconstitution			X
247	CP-10(6)	Information System Recovery And Reconstitution		X	X
248	IA-1	Identification And Authentication Policy And Procedures	X	X	
249	IA-2	Identification And Authentication (Organizational Users)	X	X	
250	IA-2(1)	Identification And Authentication (Organizational Users)	X	X	
251	IA-2(2)	Identification And Authentication (Organizational Users)	X	X	
252	IA-2(3)	Identification And Authentication (Organizational Users)	X	X	
253	IA-2(4)	Identification And Authentication (Organizational Users)	X	X	
254	IA-2(5)	Identification And Authentication (Organizational Users)	X	X	
255	IA-2(6)	Identification And Authentication (Organizational Users)			
256	IA-2(7)	Identification And Authentication (Organizational Users)	X	X	
257	IA-2(8)	Identification And Authentication (Organizational Users)	X	X	
258	IA-2(9)	Identification And Authentication (Organizational Users)	X	X	
259	IA-3	Device Identification And Authentication	X	X	
260	IA-3(1)	Device Identification And Authentication	X	X	
261	IA-3(2)	Device Identification And Authentication	X	X	
262	IA-3(3)	Device Identification And Authentication	X	X	
263	IA-4	Identifier Management	X	X	
264	IA-4(1)	Identifier Management	X	X	
265	IA-4(2)	Identifier Management		X	
266	IA-4(3)	Identifier Management		X	
267	IA-4(4)	Identifier Management	X	X	
268	IA-4(5)	Identifier Management	X	X	
269	IA-5	Authenticator Management	X	X	
270	IA-5(1)	Authenticator Management	X	X	
271	IA-5(2)	Authenticator Management		X	
272	IA-5(3)	Authenticator Management		X	
273	IA-5(4)	Authenticator Management	X	X	
274	IA-5(5)	Authenticator Management	X	X	
275	IA-5(6)	Authenticator Management	X	X	
276	IA-5(7)	Authenticator Management	X		
277	IA-5(8)	Authenticator Management	X	X	
278	IA-6	Authenticator Feedback	X		

	ID	**Title**	**C**	**I**	**A**
279	IA-7	Cryptographic Module Authentication	X	X	
280	IA-8	Identification And Authentication (Non-Organizational Users)	X	X	
281	IR-1	Incident Response Policy And Procedures	X	X	X
282	IR-2	Incident Response Training	X	X	X
283	IR-2(1)	Incident Response Training	X	X	X
284	IR-2(2)	Incident Response Training	X	X	X
285	IR-3	Incident Response Testing And Exercises	X	X	X
286	IR-3(1)	Incident Response Testing And Exercises	X	X	X
287	IR-4	Incident Handling	X	X	X
288	IR-4(1)	Incident Handling	X	X	X
289	IR-4(2)	Incident Handling	X	X	X
290	IR-4(3)	Incident Handling	X	X	X
291	IR-4(4)	Incident Handling	X	X	X
292	IR-4(5)	Incident Handling	X	X	
293	IR-5	Incident Monitoring	X	X	X
294	IR-5(1)	Incident Monitoring	X	X	X
295	IR-6	Incident Reporting	X	X	X
296	IR-6(1)	Incident Reporting	X	X	X
297	IR-6(2)	Incident Reporting	X	X	X
298	IR-7	Incident Response Assistance	X	X	X
299	IR-7(1)	Incident Response Assistance	X	X	X
300	IR-7(2)	Incident Response Assistance	X	X	X
301	IR-8	Incident Response Plan	X	X	X
302	MA-1	System Maintenance Policy And Procedures	X	X	X
303	MA-2	Controlled Maintenance	X	X	X
304	MA-2(1)	Controlled Maintenance	X	X	X
305	MA-2(2)	Controlled Maintenance	X	X	X
306	MA-3	Maintenance Tools		X	X
307	MA-3(1)	Maintenance Tools		X	X
308	MA-3(2)	Maintenance Tools		X	X
309	MA-3(3)	Maintenance Tools	X		
310	MA-3(4)	Maintenance Tools		X	
311	MA-4	Non-Local Maintenance		X	
312	MA-4(1)	Non-Local Maintenance		X	
313	MA-4(2)	Non-Local Maintenance		X	
314	MA-4(3)	Non-Local Maintenance	X	X	X
315	MA-4(4)	Non-Local Maintenance	X	X	
316	MA-4(5)	Non-Local Maintenance		X	
317	MA-4(6)	Non-Local Maintenance	X	X	
318	MA-4(7)	Non-Local Maintenance		X	
319	MA-5	Maintenance Personnel	X	X	X
320	MA-5(1)	Maintenance Personnel	X	X	X
321	MA-5(2)	Maintenance Personnel	X	X	X
322	MA-5(3)	Maintenance Personnel	X	X	X
323	MA-5(4)	Maintenance Personnel	X	X	X
324	MA-6	Timely Maintenance			X
325	MP-1	Media Protection Policy And Procedures	X	X	X
326	MP-2	Media Access	X		
327	MP-2(1)	Media Access	X	X	
328	MP-2(2)	Media Access	X	X	
329	MP-3	Media Marking	X		
330	MP-4	Media Storage	X		
331	MP-4(1)	Media Storage	X		
332	MP-5	Media Transport	X	X	
333	MP-5(1)	Media Transport	-	-	-
334	MP-5(2)	Media Transport	X	X	
335	MP-5(3)	Media Transport	X	X	
336	MP-5(4)	Media Transport	X	X	
337	MP-6	Media Sanitization	X		

	ID	Title	C	I	A
338	MP-6(1)	Media Sanitization	X		
339	MP-6(2)	Media Sanitization	X		
340	MP-6(3)	Media Sanitization	X		
341	MP-6(4)	Media Sanitization	X		
342	MP-6(5)	Media Sanitization	X		
343	MP-6(6)	Media Sanitization	X		
344	PE-1	Physical And Environmental Protection Policy And Procedures	X	X	X
345	PE-2	Physical Access Authorizations	X	X	X
346	PE-2(1)	Physical Access Authorizations	X	X	X
347	PE-2(2)	Physical Access Authorizations	X	X	
348	PE-2(3)	Physical Access Authorizations	X		
349	PE-3	Physical Access Control	X	X	X
350	PE-3(1)	Physical Access Control	X	X	
351	PE-3(2)	Physical Access Control	X		
352	PE-3(3)	Physical Access Control	X	X	
353	PE-3(4)	Physical Access Control	X	X	
354	PE-3(5)	Physical Access Control		X	
355	PE-3(6)	Physical Access Control		X	
356	PE-4	Access Control For Transmission Medium	X	X	
357	PE-5	Access Control For Output Devices	X		
358	PE-6	Monitoring Physical Access	X	X	X
359	PE-6(1)	Monitoring Physical Access			X
360	PE-6(2)	Monitoring Physical Access	X	X	X
361	PE-7	Visitor Control	X	X	
362	PE-7(1)	Visitor Control	X	X	
363	PE-7(2)	Visitor Control	X	X	
364	PE-8	Access Records	X	X	
365	PE-8(1)	Access Records			X
366	PE-8(2)	Access Records			X
367	PE-9	Power Equipment And Power Cabling			X
368	PE-9(1)	Power Equipment And Power Cabling			X
369	PE-9(2)	Power Equipment And Power Cabling			X
370	PE-10	Emergency Shutoff			X
371	PE-10(1)	Emergency Shutoff	-	-	-
372	PE-11	Emergency Power			X
373	PE-11(1)	Emergency Power			X
374	PE-11(2)	Emergency Power			X
375	PE-12	Emergency Lighting			X
376	PE-12(1)	Emergency Lighting			X
377	PE-13	Fire Protection			X
378	PE-13(1)	Fire Protection			X
379	PE-13(2)	Fire Protection			X
380	PE-13(3)	Fire Protection			X
381	PE-13(4)	Fire Protection			X
382	PE-14	Temperature And Humidity Controls			X
383	PE-14(1)	Temperature And Humidity Controls			X
384	PE-14(2)	Temperature And Humidity Controls			X
385	PE-15	Water Damage Protection			X
386	PE-15(1)	Water Damage Protection			X
387	PE-16	Delivery And Removal	X		X
388	PE-17	Alternate Work Site	X	X	X
389	PE-18	Location Of Information System Components			X
390	PE-18(1)	Location Of Information System Components			X
391	PE-19	Information Leakage	X		
392	PE-19(1)	Information Leakage	X		
393	PL-1	Security Planning Policy And Procedures	X	X	X
394	PL-2	System Security Plan	X	X	X
395	PL-2(1)	System Security Plan	X	X	X
396	PL-2(2)	System Security Plan	X	X	X

	ID	Title	C	I	A
397	PL-3	System Security Plan Update	-	-	-
398	PL-4	Rules Of Behavior	X	X	X
399	PL-4(1)	Rules Of Behavior	X		
400	PL-5	Privacy Impact Assessment	X		
401	PL-6	Security-Related Activity Planning	X	X	X
402	PS-1	Personnel Security Policy And Procedures	X	X	X
403	PS-2	Position Categorization	X	X	X
404	PS-3	Personnel Screening	X	X	
405	PS-3(1)	Personnel Screening	X		
406	PS-3(2)	Personnel Screening	X		
407	PS-4	Personnel Termination	X	X	X
408	PS-5	Personnel Transfer	X	X	X
409	PS-6	Access Agreements	X	X	
410	PS-6(1)	Access Agreements	X	X	
411	PS-6(2)	Access Agreements	X		
412	PS-7	Third-Party Personnel Security	X	X	
413	PS-8	Personnel Sanctions	X	X	X
414	RA-1	Risk Assessment Policy And Procedures	X	X	X
415	RA-2	Security Categorization	X	X	X
416	RA-3	Risk Assessment	X	X	X
417	RA-4	Risk Assessment Update	-	-	-
418	RA-5	Vulnerability Scanning	X	X	X
419	RA-5(1)	Vulnerability Scanning	X	X	X
420	RA-5(2)	Vulnerability Scanning	X	X	X
421	RA-5(3)	Vulnerability Scanning	X	X	X
422	RA-5(4)	Vulnerability Scanning	X	X	X
423	RA-5(5)	Vulnerability Scanning	X	X	X
424	RA-5(6)	Vulnerability Scanning	X	X	X
425	RA-5(7)	Vulnerability Scanning	X	X	X
426	RA-5(8)	Vulnerability Scanning	X	X	X
427	RA-5(9)	Vulnerability Scanning	X	X	X
428	SA-1	System And Services Acquisition Policy And Procedures	X	X	
429	SA-2	Allocation Of Resources		X	
430	SA-3	Life Cycle Support		X	
431	SA-4	Acquisitions		X	
432	SA-4(1)	Acquisitions		X	
433	SA-4(2)	Acquisitions		X	
434	SA-4(3)	Acquisitions		X	
435	SA-4(4)	Acquisitions		X	
436	SA-4(5)	Acquisitions		X	
437	SA-4(6)	Acquisitions		X	
438	SA-4(7)	Acquisitions		X	
439	SA-5	Information System Documentation		X	
440	SA-5(1)	Information System Documentation		X	
441	SA-5(2)	Information System Documentation		X	
442	SA-5(3)	Information System Documentation		X	
443	SA-5(4)	Information System Documentation		X	
444	SA-5(5)	Information System Documentation		X	
445	SA-6	Software Usage Restrictions	X	X	
446	SA-6(1)	Software Usage Restrictions	X	X	
447	SA-7	User Installed Software		X	
448	SA-8	Security Engineering Principles		X	
449	SA-9	External Information System Services		X	
450	SA-9(1)	External Information System Services		X	
451	SA-10	Developer Configuration Management		X	
452	SA-10(1)	Developer Configuration Management		X	
453	SA-10(2)	Developer Configuration Management		X	
454	SA-11	Developer Security Testing		X	
455	SA-11(1)	Developer Security Testing		X	

	ID	Title	C	I	A
456	SA-11(2)	Developer Security Testing		X	
457	SA-11(3)	Developer Security Testing		X	
458	SA-12	Supply Chain Protection		X	
459	SA-12(1)	Supply Chain Protection		X	
460	SA-12(2)	Supply Chain Protection		X	
461	SA-12(3)	Supply Chain Protection		X	
462	SA-12(4)	Supply Chain Protection		X	
463	SA-12(5)	Supply Chain Protection		X	
464	SA-12(6)	Supply Chain Protection		X	
465	SA-12(7)	Supply Chain Protection		X	
466	SA-13	Trustworthiness		X	
467	SA-14	Critical Information System Components		X	
468	SA-14(1)	Critical Information System Components		X	
469	SC-1	System And Communications Protection Policy And Procedures	X	X	X
470	SC-2	Application Partitioning	X	X	
471	SC-2(1)	Application Partitioning	X	X	
472	SC-3	Security Function Isolation	X	X	
473	SC-3(1)	Security Function Isolation	X	X	
474	SC-3(2)	Security Function Isolation	X	X	
475	SC-3(3)	Security Function Isolation	X	X	
476	SC-3(4)	Security Function Isolation	X	X	
477	SC-3(5)	Security Function Isolation	X	X	
478	SC-4	Information In Shared Resources	X		
479	SC-4(1)	Information In Shared Resources	X		
480	SC-5	Denial Of Service Protection			X
481	SC-5(1)	Denial Of Service Protection			X
482	SC-5(2)	Denial Of Service Protection			X
483	SC-6	Resource Priority			X
484	SC-7	Boundary Protection	X	X	
485	SC-7(1)	Boundary Protection	X	X	
486	SC-7(2)	Boundary Protection	X	X	
487	SC-7(3)	Boundary Protection	X	X	
488	SC-7(4)	Boundary Protection	X	X	
489	SC-7(5)	Boundary Protection	X	X	
490	SC-7(6)	Boundary Protection	X		
491	SC-7(7)	Boundary Protection	X	X	
492	SC-7(8)	Boundary Protection	X	X	
493	SC-7(9)	Boundary Protection	X	X	
494	SC-7(10)	Boundary Protection	X		
495	SC-7(11)	Boundary Protection		X	
496	SC-7(12)	Boundary Protection	X	X	
497	SC-7(13)	Boundary Protection	X	X	
498	SC-7(14)	Boundary Protection	X	X	
499	SC-7(15)	Boundary Protection	X	X	
500	SC-7(16)	Boundary Protection	X		
501	SC-7(17)	Boundary Protection		X	
502	SC-7(18)	Boundary Protection	X	X	X
503	SC-8	Transmission Integrity		X	
504	SC-8(1)	Transmission Integrity		X	
505	SC-8(2)	Transmission Integrity		X	
506	SC-9	Transmission Confidentiality	X		
507	SC-9(1)	Transmission Confidentiality	X		
508	SC-9(2)	Transmission Confidentiality	X		
509	SC-10	Network Disconnect	X	X	
510	SC-11	Trusted Path		X	
511	SC-12	Cryptographic Key Establishment And Management	X	X	
512	SC-12(1)	Cryptographic Key Establishment And Management			X
513	SC-12(2)	Cryptographic Key Establishment And Management	X	X	
514	SC-12(3)	Cryptographic Key Establishment And Management	X	X	

	ID	Title	C	I	A
515	SC-12(4)	Cryptographic Key Establishment And Management	X	X	
516	SC-12(5)	Cryptographic Key Establishment And Management	X	X	
517	SC-13	Use Of Cryptography	X	X	
518	SC-13(1)	Use Of Cryptography	X		
519	SC-13(2)	Use Of Cryptography	X		
520	SC-13(3)	Use Of Cryptography	X		
521	SC-13(4)	Use Of Cryptography		X	
522	SC-14	Public Access Protections		X	X
523	SC-15	Collaborative Computing Devices	X		
524	SC-15(1)	Collaborative Computing Devices	X		
525	SC-15(2)	Collaborative Computing Devices	X	X	
526	SC-15(3)	Collaborative Computing Devices	X	X	
527	SC-16	Transmission Of Security Attributes	X	X	
528	SC-16(1)	Transmission Of Security Attributes		X	
529	SC-17	Public Key Infrastructure Certificates	X	X	
530	SC-18	Mobile Code		X	
531	SC-18(1)	Mobile Code		X	
532	SC-18(2)	Mobile Code		X	
533	SC-18(3)	Mobile Code		X	
534	SC-18(4)	Mobile Code		X	
535	SC-19	Voice Over Internet Protocol	X	X	
536	SC-20	Secure Name / Address Resolution Service (Authoritative Source)		X	
537	SC-20(1)	Secure Name / Address Resolution Service (Authoritative Source)		X	
538	SC-21	Secure Name / Address Resolution Service (Recursive Or Caching Resolver)		X	
539	SC-21(1)	Secure Name / Address Resolution Service (Recursive Or Caching Resolver)		X	
540	SC-22	Architecture And Provisioning For Name / Address Resolution Service	X	X	X
541	SC-23	Session Authenticity		X	
542	SC-23(1)	Session Authenticity		X	
543	SC-23(2)	Session Authenticity		X	
544	SC-23(3)	Session Authenticity		X	
545	SC-23(4)	Session Authenticity		X	
546	SC-24	Fail In Known State	X	X	
547	SC-25	Thin Nodes		X	
548	SC-26	Honeypots		X	
549	SC-26(1)	Honeypots		X	
550	SC-27	Operating System-Independent Applications		X	
551	SC-28	Protection Of Information At Rest	X	X	
552	SC-28(1)	Protection Of Information At Rest	X	X	
553	SC-29	Heterogeneity		X	
554	SC-30	Virtualization Techniques		X	
555	SC-30(1)	Virtualization Techniques		X	
556	SC-30(2)	Virtualization Techniques		X	
557	SC-31	Covert Channel Analysis	X		
558	SC-31(1)	Covert Channel Analysis	X		
559	SC-32	Information System Partitioning	X	X	
560	SC-33	Transmission Preparation Integrity		X	
561	SC-34	Non-modifiable executable programs		X	
562	SC-34(1)	Non-modifiable executable programs		X	
563	SC-34(2)	Non-modifiable executable programs		X	
564	SI-1	System And Information Integrity Policy And Procedures	X	X	X
565	SI-2	Flaw Remediation		X	
566	SI-2(1)	Flaw Remediation		X	
567	SI-2(2)	Flaw Remediation		X	
568	SI-2(3)	Flaw Remediation		X	
569	SI-2(4)	Flaw Remediation		X	
570	SI-3	Malicious Code Protection		X	
571	SI-3(1)	Malicious Code Protection		X	
572	SI-3(2)	Malicious Code Protection		X	
573	SI-3(3)	Malicious Code Protection		X	

	ID	Title	C	I	A
574	SI-3(4)	Malicious Code Protection		X	
575	SI-3(5)	Malicious Code Protection		X	
576	SI-3(6)	Malicious Code Protection		X	
577	SI-4	Information System Monitoring		X	
578	SI-4(1)	Information System Monitoring		X	
579	SI-4(2)	Information System Monitoring		X	
580	SI-4(3)	Information System Monitoring		X	
581	SI-4(4)	Information System Monitoring	X	X	
582	SI-4(5)	Information System Monitoring		X	
583	SI-4(6)	Information System Monitoring		X	
584	SI-4(7)	Information System Monitoring		X	X
585	SI-4(8)	Information System Monitoring	X	X	X
586	SI-4(9)	Information System Monitoring		X	
587	SI-4(10)	Information System Monitoring	X	X	
588	SI-4(11)	Information System Monitoring	X		
589	SI-4(12)	Information System Monitoring	X	X	
590	SI-4(13)	Information System Monitoring	X	X	X
591	SI-4(14)	Information System Monitoring	X	X	
592	SI-4(15)	Information System Monitoring	X	X	
593	SI-4(16)	Information System Monitoring		X	
594	SI-4(17)	Information System Monitoring	X	X	
595	SI-5	Security Alerts, Advisories, And Directives		X	
596	SI-5(1)	Security Alerts, Advisories, And Directives		X	
597	SI-6	Security Functionality Verification		X	
598	SI-6(1)	Security Functionality Verification		X	
599	SI-6(2)	Security Functionality Verification		X	
600	SI-6(3)	Security Functionality Verification		X	
601	SI-7	Software And Information Integrity		X	
602	SI-7(1)	Software And Information Integrity		X	
603	SI-7(2)	Software And Information Integrity		X	
604	SI-7(3)	Software And Information Integrity		X	
605	SI-7(4)	Software And Information Integrity		X	
606	SI-8	Spam Protection		X	X
607	SI-8(1)	Spam Protection		X	X
608	SI-8(2)	Spam Protection		X	X
609	SI-9	Information Input Restrictions		X	
610	SI-10	Information Input Validation		X	
611	SI-11	Error Handling		X	
612	SI-12	Information Output Handling And Retention	X	X	
613	SI-13	Predictable Failure Prevention			X
614	SI-13(1)	Predictable Failure Prevention			X
615	SI-13(2)	Predictable Failure Prevention			X
616	SI-13(3)	Predictable Failure Prevention			X
617	SI-13(4)	Predictable Failure Prevention			X
618	PM-1	Information Security Program Plan	X	X	X
619	PM-2	Senior Information Security Officer	X	X	X
620	PM-3	Information Security Resources	X	X	X
621	PM-4	Plan of Action and Milestones Process	X	X	X
622	PM-5	Information System Inventory	X	X	X
623	PM-6	Information Security Measures of Performance	X	X	X
624	PM-7	Enterprise Architecture	X	X	X
625	PM-8	Critical Infrastructure Plan	X	X	X
626	PM-9	Risk Management Strategy	X	X	X
627	PM-10	Security Authorization Process	X	X	X
628	PM-11	Mission/Business Process Definition	X	X	X

APPENDIX E: MINIMUM ASSURANCE REQUIREMENTS

LOW-IMPACT, MODERATE-IMPACT, AND HIGH-IMPACT INFORMATION SYSTEMS

Adoption of National Institute of Standards and Technology Special Publication 800-53, Appendix E, has been deferred at this time from this release of Committee on National Security Systems Instruction No. 1253 pending further review/discussions by the National Security Community.

APPENDIX F: SECURITY CONTROL CATALOG

SECURITY CONTROLS, ENHANCEMENTS, AND SUPPLEMENTAL GUIDANCE

Committee on National Security Systems Instruction No. 1253, Appendix F, adopts the security control catalog specified and defined in National Institute of Standards and Technology Special Publication 800-53, Revision 3, Appendix F, with the following exceptions and caveats.

The priority and baseline allocation specifications which are provided at the end of each security control in NIST SP 800-53 do not apply. The baseline allocation specifications which apply are provided in Appendix D, Table D-1 of CNSSI 1253. No prioritization of security controls is specified by CNSSI 1253.

Organization-defined parameters for security controls implemented in National Security Systems are implemented with the values for those parameters specified in Appendix J of this Instruction.

APPENDIX G: INFORMATION SECURITY PROGRAMS

ORGANIZATION-WIDE INFORMATION SECURITY PROGRAM MANAGEMENT CONTROLS

National Institute of Standards and Technology Special Publication 800-53, Revision 3, Appendix G, is adopted for optional use, at the discretion of National Security Community departments and agencies.

APPENDIX H: INTERNATIONAL INFORMATION SECURITY STANDARDS

SECURITY CONTROL MAPPINGS FOR INTERNATIONAL ORGANIZATION FOR STANDARDIZATION/ INTERNATIONAL ELECTROTECHNICAL COMMISSION 27001

National Institute of Standards and Technology Special Publication 800-53, Revision 3, Appendix H, is adopted for optional use, at the discretion of National Security Community departments and agencies.

APPENDIX I: INDUSTRIAL CONTROL SYSTEMS

SECURITY CONTROLS, ENHANCEMENTS AND SUPPLEMENTAL GUIDANCE

Adoption of National Institute of Standards and Technology Special Publication 800-53, Appendix I, is not mandatory and is solely at the discretion of National Security Community departments and agencies, at this time, pending further applicability by the National Security Community.

APPENDIX J: ORGANIZATION-DEFINED PARAMETER VALUES

VALUES FOR ORGANIZATION-DEFINED PARAMETERS IN NATIONAL SECURITY SYSTEMS

Table J–1 establishes common values for organization-defined parameters in National Security Systems (NSS). This table lists the security controls (or control enhancements) from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 that have organization-defined parameters. The CNSS has identified some parameters as requiring common ranges of values to facilitate reciprocity within the National Security Community. For those parameters Table J-1 lists specific values.

Some of the Table J-1 entries are blank in the column titled "**DEFINED VALUE FOR NSS**". For these parameters, common ranges of values are not required across all NSS. Organizations should define these appropriately for organization internal use, and in coordination with other organizations when they affect reciprocity.

Table J–1: Values for Organization-Defined Parameters in NSS

CNTL NO. (Enhancement)	CONTROL NAME	800-53 VARIABLE TEXT	DEFINED VALUE FOR NSS
Access Control			
AC-1	Access Control Policy and Procedures	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: …	
AC-2	Account Management	The organization manages information system accounts, including: … j. Reviewing accounts [*Assignment: organization-defined frequency*].	j. …or at least annually
AC-2 (2)	Account Management	The information system automatically terminates temporary and emergency accounts after [*Assignment: organization-defined time period for each type of account*].	…not to exceed 72 hours.
AC-2 (3)	Account Management	The information system automatically disables inactive accounts after [*Assignment: organization-defined time period*].	…not to exceed 30 days.
AC-2 (5)	Account Management	The organization: (a.) Requires that users logout when [*Assignment: organization defined time-period of expected inactivity and/or description of when to log out*]; …	a.
AC-3 (2)	Access Enforcement	The information system enforces dual authorization, based on organizational policies and procedures for [*Assignment: organization-defined privileged commands*].	

CNTL NO. (Enhancement)	CONTROL NAME	800-53 VARIABLE TEXT	DEFINED VALUE FOR NSS
AC-3 (3)	Access Enforcement	The information system enforces [*Assignment: organization-defined nondiscretionary access control policies*] over [*Assignment: organization-defined set of users and resources*] where the policy rule set for each policy specifies: (a)Access control information (i.e., attributes) employed by the policy rule set (e.g., position, nationality, age, project, time of day); and (b)Required relationships among the access control information to permit access.	
AC-3 (5)	Access Enforcement	The information system prevents access to [*Assignment: organization-defined security-relevant information*] except during secure, non-operable system states.	
AC-3 (6)	Access Enforcement	The organization encrypts or stores off line in a secure location [*Assignment: organization-defined user and/or system information*].	
AC-4 (5)	Information Flow Enforcement	The information system enforces [*Assignment: organization-defined limitations on the embedding of data types within other data types*].	
AC-4 (7)	Information Flow Enforcement	The information system enforces [*Assignment: organization-defined one-way flows*] using hardware mechanisms.	
AC-4 (8)	Information Flow Enforcement	The information system enforces information flow control using [*Assignment: organization-defined security policy filters*] as a basis for flow control decisions.	
AC-4 (9)	Information Flow Enforcement	The information system enforces the use of human review for [*Assignment: organization-defined security policy filters*] when the system is not capable of making an information flow control decision.	
AC-4 (10)	Information Flow Enforcement	The information system provides the capability for a privileged administrator to enable/disable [*Assignment: organization-defined security policy filters*].	
AC-4 (11)	Information Flow Enforcement	The information system provides the capability for a privileged administrator to configure the [*Assignment: organization-defined security policy filters*] to support different security policies.	
AC-4 (14)	Information Flow Enforcement	The information system, when transferring information between different security domains, implements policy filters that constrain data structure and content to [*Assignment: organization-defined information security policy requirements*].	
AC-6 (1)	Least Privilege	The organization explicitly authorizes access to [*Assignment: organization-defined list of security functions (deployed in hardware, software, and firmware) and security-relevant information*].	

CNTL NO. (Enhancement)	CONTROL NAME	800-53 VARIABLE TEXT	DEFINED VALUE FOR NSS
AC-6 (2)	Least Privilege	The organization requires that users of information system accounts, or roles, with access to [*Assignment: organization-defined list of security functions or security-relevant information*], use non-privileged accounts, or roles, when accessing other system functions, and if feasible, audits any use of privileged accounts, or roles, for such functions.	
AC-6 (3)	Least Privilege	The organization authorizes network access to [*Assignment: organization-defined privileged commands*] only for compelling operational needs and documents the rationale for such access in the security plan for the information system.	
AC-7	Unsuccessful Login Attempts	The information system: a.Enforces a limit of [*Assignment: organization-defined number*] consecutive invalid access attempts by a user during a [*Assignment: organization-defined time period*] time period; and b.Automatically [*Selection: locks the account/node for an* [*Assignment: organization-defined time period*]; *locks the account/node until released by an administrator;* *delays next login prompt according to* [*Assignment: organization-defined delay algorithm*]] when the maximum number of unsuccessful attempts is exceeded. The control applies regardless of whether the login is done via a local, network, or remote connection.	a.…or a maximum of 3 …or at least 15 minutes b.…locks the account/node for at least 10 minutes
AC-7 (2)	Unsuccessful Login Attempts	The information system provides additional protection for mobile devices accessed via login by purging information from the device after [*Assignment: organization-defined number*] *consecutive, unsuccessful login attempts* to the device.	
AC-9 (2)	Previous Logon (Access) Notification	The information system notifies the user of the number of [*Selection: successful logins/accesses; unsuccessful login/access attempts; both*] during [*Assignment: organization-defined time period*].	
AC-9 (3)	Previous Logon (Access) Notification	The information system notifies the user of [*Assignment: organization-defined set of security-related changes to the user's account*] during [*Assignment: organization-defined time period*].	
AC-10	Concurrent Session Control	The information system limits the number of concurrent sessions for each system account to [*Assignment: organization-defined number*].	…or a maximum of three (3) sessions
AC-11	Session Lock	The information system: a. Prevents further access to the system by initiating a session lock after [*Assignment: organization-defined time period*] of inactivity or upon receiving a request from a user; and …	a.…not to exceed 30 minutes
AC-16	Security Attributes	The information system supports and maintains the binding of [*Assignment: organization-defined security attributes*] to information in storage, in process, and in transmission.	

CNTL NO. (Enhancement)	CONTROL NAME	800-53 VARIABLE TEXT	DEFINED VALUE FOR NSS
AC-16 (5)	Security Attributes	The information system displays security attributes in human-readable form on each object output from the system to system output devices to identify [*Assignment: organization-identified set of special dissemination, handling, or distribution instructions*] using [*Assignment: organization-identified human readable, standard naming conventions*].	
AC-17 (5)	Remote Access	The organization monitors for unauthorized remote connections to the information system [*Assignment: organization-defined frequency*], and takes appropriate action if an unauthorized connection is discovered.	
AC-17 (7)	Remote Access	The organization ensures that remote sessions for accessing [*Assignment: organization-defined list of security functions and security-relevant information*] employ [*Assignment: organization-defined additional security measures*] and are audited.	
AC-17 (8)	Remote Access	The organization disables [*Assignment: organization-defined networking protocols within the information system deemed to be nonsecure*] except for explicitly identified components in support of specific operational requirements.	
AC-18 (2)	Wireless Access	The organization monitors for unauthorized wireless connections to the information system, including scanning for unauthorized wireless access points [*Assignment: organization-defined frequency*], and takes appropriate action if an unauthorized connection is discovered.	at least every 30 days
AC-19	Access Control for Mobile Devices	The organization: … g. Applies [*Assignment: organization-defined inspection and preventative measures*] to mobile devices returning from locations that the organization deems to be of significant risk in accordance with organizational policies and procedures.	g
AC-19 (4)	Access Control for Mobile Devices	The organization: … (b)Enforces the following restrictions on individuals permitted to use mobile devices in facilities containing information systems processing, storing, or transmitting classified information: **…** -Mobile devices and the information stored on those devices are subject to random reviews/inspections by [*Assignment: organization-defined security officials*], and if classified information is found, the incident handling policy is followed.	(b)

CNTL NO. (Enhancement)	CONTROL NAME	800-53 VARIABLE TEXT	DEFINED VALUE FOR NSS
AC-21	User-Based Collaboration and Information Sharing	The organization: a.Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for [*Assignment: organization-defined information sharing circumstances where user discretion is required*]; and b.Employs [*Assignment: list of organization-defined information sharing circumstances and automated mechanisms or manual processes required*] to assist users in making information sharing/collaboration decisions.	a. b.
AC-22	Publicly Accessible Content	The organization: … d. Reviews the content on the publicly-accessible information for non-public information [*Assignment: organization-defined frequency*]; and ….	
Awareness and Training			
AT-1	Security Awareness And Training Policy And Procedures	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: …	
AT-2	Security Awareness	The organization provides basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users, when required by system changes, and [*Assignment: organization-defined frequency*] thereafter.	…at least annually
AT-3	Security Training	The organization provides role-based security-related training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) [*Assignment: organization-defined frequency*] thereafter.	…at least annually
AT-3(1)	Security Training	The organization provides employees with initial and [*Assignment: organization-defined frequency*] training in the employment and operation of environmental controls.	
AT-3(2)	Security Training	The organization provides employees with initial and [*Assignment: organization-defined frequency*] training in the employment and operation of physical security controls.	
AT-4	Security Training Records	The organization: … b.Retains individual training records for [*Assignment: organization-defined time period*].	b.
Audit and Accountability			
AU-1	Security Audit And Accountability Policy And Procedures	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: …	

CNTL NO. (Enhancement)	CONTROL NAME	800-53 VARIABLE TEXT	DEFINED VALUE FOR NSS
AU-2	Auditable Events	The organization: a.Determines, based on a risk assessment and mission/business needs, that the information system must be capable of auditing the following events: [*Assignment: organization-defined list of auditable events*; … d. Determines, based on current threat information and ongoing assessment of risk, that the following events are to be audited within the information system: [*Assignment: organization-defined subset of the auditable events defined in AU-2 a to be audited along with the frequency of (or situation requiring) auditing for each identified event*	**a.** (a) Successful and unsuccessful attempts to access, modify, or delete security objects, (b) Successful and unsuccessful logon attempts, (c) Privileged activities or other system level access, (d) Starting and ending time for user access to the system, (e) Concurrent logons from different workstations, (f) Successful and unsuccessful accesses to objects, (g) All program initiations, (h) All direct access to the information system. **d**. *Refer to* **a.** *above.*
AU-2 (3)	Auditable Events	The organization reviews and updates the list of auditable events [*Assignment: organization-defined frequency*].	
AU-3 (1)	Content of Audit Records	The information system includes [*Assignment: organization-defined additional, more detailed information*] in the audit records for audit events identified by type, location, or subject.	
AU-3 (2)	Content of Audit Records	The organization centrally manages the content of audit records generated by [*Assignment: organization-defined information system components*].	
AU-5	Response to Audit Processing Failures	The information system: … b. Takes the following additional actions: [*Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)*].	b.
AU-5 (1)	Response to Audit Processing Failures	The information system provides a warning when allocated audit record storage volume reaches [*Assignment: organization-defined percentage] of maximum audit record storage capacity*.	…or at a maximum of 75 percent
AU-5 (2)	Response to Audit Processing Failures	The information system provides a real-time alert when the following audit failure events occur: [*Assignment: organization-defined audit failure events requiring real-time alerts*].	
AU-5 (3)	Response to Audit Processing Failures	The information system enforces configurable traffic volume thresholds representing auditing capacity for network traffic and [*Selection: rejects or delays*] network traffic above those thresholds.	
AU-6	Audit Review, Analysis, and Reporting	The organization: a.Reviews and analyzes information system audit records [*Assignment: organization-defined frequency*] for indications of inappropriate or unusual activity, and reports findings to designated organizational officials; and …	a.at least on a weekly basis

CNTL NO. (Enhancement)	CONTROL NAME	800-53 VARIABLE TEXT	DEFINED VALUE FOR NSS
AU-6 (8)	Audit Review, Analysis, and Reporting	The organization employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications: [*Assignment: organization-defined list of inappropriate or unusual activities that are to result in alerts*].	
AU-8 (1)	Time Stamps	The information system synchronizes internal information system clocks [*Assignment: organization-defined frequency*] with [*Assignment: organization-defined authoritative time source*].	…or at least every 24 hours
AU-9 (2)	Protection of Audit Information	The information system backs up audit records [*Assignment: organization-defined frequency*] onto a different system or media than the system being audited.	… not less than weekly
AU-10 (5)	Non-repudiation	The organization employs [*Selection: FIPS-validated; NSA-approved*] cryptography to implement digital signatures.	
AU-11	Audit Record Retention	The organization retains audit records for [*Assignment: organization-defined time period*] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.	… minimum of 5 years for Sensitive Compartmented Information; … minimum of 5 years for Sources And Methods Intelligence information; …minimum of 1 year for unclassified.
AU-12	Audit Generation	The information system: a.Provides audit record generation capability for the list of auditable events defined in AU-2 at [*Assignment: organization-defined information system components*]; …	a.
AU-12 (1)	Audit Generation	The information system compiles audit records from [*Assignment: organization-defined information system components*] into a system-wide (logical or physical) audit trail that is time-correlated to within [*Assignment: Organization-defined level of tolerance for relationship between time stamps of individual records in the audit trail*].	
AU-13	Monitoring for Information Disclosure	The organization monitors open source information for evidence of unauthorized exfiltration or disclosure of organizational information [*Assignment: organization-defined frequency*].	
Security Assessment and Authorization			
CA-1	Security Assessment And Authorization Policy And Procedures	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: …	

CNTL NO. (Enhancement)	CONTROL NAME	800-53 VARIABLE TEXT	DEFINED VALUE FOR NSS
CA-2	Security Assessments	The organization: a. … b. Assesses the security controls in the information system [*Assignment: organization-defined frequency*] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.	b. … at least annually
CA-2 (2)	Security Assessments	The organization includes as part of security control assessments, [*Assignment: organization-defined frequency*], [*Selection: announced; unannounced*], [*Selection: in-depth monitoring; malicious user testing; penetration testing; red team exercises;* [*Assignment: organization-defined other forms of security testing*]].	
CA-5	Plan of Action and Milestones	The organization: a. … b. Updates existing plan of action and milestones [*Assignment: organization-defined frequency*], based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.	b. …or not less than annually
CA-6	Security Authorization	The organization: … c.Updates the security authorization [*Assignment: organization-defined frequency*] or when there is a significant change to the system.	c.
CA-7	Continuous Monitoring	The organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes: d. Reporting the security state of the information system to appropriate organizational officials [*Assignment: organization-defined frequency].*	d.
CA-7(2)	Continuous Monitoring	The organization plans, schedules, and conducts assessments [*Assignment: organization-defined frequency*], [*Selection: announced; unannounced*], [*Selection: in-depth monitoring; malicious user testing; penetration testing; red team exercises;* [*Assignment: organization-defined other forms of security assessment*]] to ensure compliance with all vulnerability mitigation procedures.	
Configuration Management			
CM-1	Configuration Management Policy And Procedures	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: …	
CM-2 (1)	Baseline Configuration	The organization reviews and updates the baseline configuration of the information system: (a) [*Assignment: organization-defined frequency*]; (b) When required due to [*Assignment organization-defined circumstances*]; and …	(a) (b)
CM-2 (4)	Baseline Configuration	The organization: (a) Develops and maintains [*Assignment: organization-defined list of software programs not authorized to execute on the information system*]; …	(a)

CNTL NO. (Enhancement)	CONTROL NAME	800-53 VARIABLE TEXT	DEFINED VALUE FOR NSS
CM-2 (5)	Baseline Configuration	The organization: (a) Develops and maintains [*Assignment: organization-defined list of software programs authorized to execute on the information system*]; …	(a)
CM-3	Configuration Change Control	The organization: … f. Coordinates and provides oversight for configuration change control activities through [*Assignment: organization-defined configuration change control element (e.g., committee, board*] that convenes [*Selection: (one or more): [Assignment: organization-defined frequency*]; [*Assignment: organization-defined configuration change conditions]*].	f. Configuration Control Board
CM-3(1)	Configuration Change Control	The organization employs automated mechanisms to: … (c)Highlight approvals that have not been received by [*Assignment: organization-defined time period*];	(c)
CM-3(4)	Configuration Change Control	The organization requires an information security representative to be a member of the [*Assignment: organization-defined configuration change control element (e.g., committee, board)*].	Configuration Control Board
CM-5 (2)	Access Restrictions for Change	The organization conducts audits of information system changes [*Assignment: organization-defined frequency*] and when indications so warrant to determine whether unauthorized changes have occurred.	
CM-5 (3)	Access Restrictions for Change	The information system prevents the installation of [*Assignment: organization-defined critical software programs*] that are not signed with a certificate that is recognized and approved by the organization.	
CM-5 (4)	Access Restrictions for Change	The organization enforces a two-person rule for changes to [*Assignment: organization-defined information system components and system-level information*].	
CM-5 (5)	Access Restrictions for Change	The organization: … (b)Reviews and reevaluates information system developer/integrator privileges [*Assignment: organization-defined frequency*].	(b)
CM-5 (7)	Access Restrictions for Change	The information system automatically implements [*Assignment: organization-defined safeguards and countermeasures*] if security functions (or mechanisms) are changed inappropriately.	
CM-6	Configuration Settings	The organization: a. Establishes and documents mandatory configuration settings for information technology products employed within the information system using [*Assignment: organization-defined security configuration checklists*] that reflect the most restrictive mode consistent with operational requirements; …	
CM-6 (2)	Configuration Settings	The organization employs automated mechanisms to respond to unauthorized changes to [*Assignment: organization-defined configuration settings*].	

CNTL NO. (Enhancement)	CONTROL NAME	800-53 VARIABLE TEXT	DEFINED VALUE FOR NSS
CM-7	Least Functionality	The organization configures the information system to provide only essential capabilities and specifically prohibits or restricts the use of the following functions, ports, protocols, and/or services: [*Assignment: organization-defined list of prohibited or restricted functions, ports, protocols, and/or services*].	
CM-7 (1)	Least Functionality	The organization reviews the information system [*Assignment: organization-defined frequency*], to identify and eliminate unnecessary functions, ports, protocols, and/or services.	or at least annually
CM-7 (2)	Least Functionality	The organization employs automated mechanisms to prevent program execution in accordance with [*Selection (one or more): list of authorized software programs; list of unauthorized software programs; rules authorizing the terms and conditions of software program usage*].	
CM-7 (3)	Least Functionality	The organization ensures compliance with [*Assignment: organization-defined registration requirements for ports, protocols, and services*].	
CM-8	Information System Component Inventory	The organization develops, documents, and maintains an inventory of information system components that: … d.Includes [*Assignment: organization-defined information deemed necessary to achieve effective property accountability*]; and …	
CM-8 (3)	Information System Component Inventory	The organization: (a)Employs automated mechanisms [*Assignment: organization-defined frequency*] to detect the addition of unauthorized components/devices into the information system; and …	(a)
CM-8 (4)	Information System Component Inventory	The organization includes in property accountability information for information system components, a means for identifying by [*Selection (one or more): name; position; role*] individuals responsible for administering those components.	
Contingency Planning			
CP-1	Contingency Planning Policy And Procedures	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: …	
CP-2	Contingency Plan	The organization: … b. Distributes copies of the contingency plan to [*Assignment: organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements*]; … d. Reviews the contingency plan for the information system [*Assignment: organization-defined frequency*]; … f. Communicates contingency plan changes to [*Assignment: organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements*].	b. d. … at least yearly f.

CNTL NO. (Enhancement)	CONTROL NAME	800-53 VARIABLE TEXT	DEFINED VALUE FOR NSS
CP-2 (3)	Contingency Plan	The organization plans for the resumption of essential missions and business functions within [*Assignment: organization-defined time period*] of contingency plan activation.	within 24 hours
CP-2 (4)	Contingency Plan	The organization plans for the full resumption of essential missions and business functions within [*Assignment: organization-defined time period*] of contingency plan activation.	within 5 days
CP-3	Contingency Training	The organization trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training [*Assignment: organization-defined frequency*].	… at least annually
CP-4	Contingency Plan Testing and Exercises	The organization: a.Tests and/or exercises the contingency plan for the information system [*Assignment: organization-defined frequency*] using [*Assignment: organization-defined tests and/or exercises*] to determine the plan's effectiveness and the organization's readiness to execute the plan; and …	a. … at least annually
CP-7	Alternate Processing Site	The organization: a.Establishes an alternate processing site including necessary agreements to permit the resumption of information system operations for essential missions and business functions within [*Assignment: organization-defined time period consistent with recovery time objectives*] when the primary processing capabilities are unavailable; …	a. not to exceed 24 hours
CP-8	Telecommunications Services	The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of information system operations for essential missions and business functions within [*Assignment: organization-defined time period*] when the primary telecommunications capabilities are unavailable.	not to exceed 24 hours
CP-9	Information System Backup	The organization: a.Conducts backups of user-level information contained in the information system [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*]; b.Conducts backups of system-level information contained in the information system [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*]; c.Conducts backups of information system documentation including security-related documentation [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*]; and …	a.… or at least weekly b.… or at least weekly
CP-9 (1)	Information System Backup	The organization tests backup information [*Assignment: organization-defined frequency*] to verify media reliability and information integrity.	… or not less than monthly

CNTL NO. (Enhancement)	CONTROL NAME	800-53 VARIABLE TEXT	DEFINED VALUE FOR NSS
CP-9 (5)	Information System Backup	The organization transfers information system backup information to the alternate storage site [*Assignment: organization-defined time period and transfer rate consistent with the recovery time and recovery point objectives*].	
CP-10 (3)	Information System Recovery and Reconstitution	The organization provides compensating security controls for [*Assignment: organization-defined circumstances that can inhibit recovery and reconstitution to a known state*].	
CP-10 (4)	Information System Recovery and Reconstitution	The organization provides the capability to re-image information system components within [*Assignment: organization-defined restoration time-periods*] from configuration controlled and integrity protected disk images representing a secure, operational state for the components.	
CP-10 (5)	Information System Recovery and Reconstitution	The organization provides [*Selection: real time; near-real-time*] [*Assignment: organization-defined failover capability for the information system*].	
Identification and Authentication			
IA-1	Identification and Authentication Policy And Procedures	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: …	
IA-2(8)	Identification and Authentication (Organizational Users)	The information system uses [*Assignment: organization-defined replay resistant authentication mechanisms*] for network access to privileged accounts.	
IA-2(9)	Identification and Authentication (Organizational Users)	The information system uses [*Assignment: organization-defined replay resistant authentication mechanisms*] for network access to non-privileged accounts.	
IA-3	Device Identification and Authentication	The information system uniquely identifies and authenticates [*Assignment: organization-defined list of specific and/or types of devices*] before establishing a connection.	
IA-4	Identifier Management	The organization manages information system identifiers for users and devices by: … d.Preventing reuse of user or device identifiers for [*Assignment: organization-defined time period*]; and e.Disabling the user identifier after [*Assignment: organization-defined time period of inactivity*].	d. e. not to exceed 30 days
IA-4(4)	Identifier Management	The organization manages user identifiers by uniquely identifying the user as [*Assignment: organization-defined characteristic identifying user status*].	user's nationality and user's status as a contractor
IA-5	Authenticator Management	The organization manages information system authenticators for users and devices by: … g.Changing/refreshing authenticators [*Assignment: organization-defined time period by authenticator type*]	g. not to exceed 180 days

CNTL NO. (Enhancement)	CONTROL NAME	800-53 VARIABLE TEXT	DEFINED VALUE FOR NSS
IA-5(1)	Authenticator Management	The information system, for password-based authentication: (a)Enforces minimum password complexity of [*Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper case letters, lower case letters, numbers, and special characters, including minimum requirements for each type*] (b)Enforces at least a [*Assignment: organization-defined number of changed characters*] when new passwords are created; … (d) Enforces password minimum and maximum lifetime restrictions of [*Assignment: organization-defined numbers for lifetime minimum, lifetime maximum*]; and (e) Prohibits password reuse for [*Assignment: organization-defined number*] generations.	(a)a case sensitive, 8-character mix of upper case letters, lower case letters, numbers, and special characters, including at least one of each (b)at least four (d) (e) a minimum of 10
IA-5 (3)	Authenticator Management	The organization requires that the registration process to receive [*Assignment: organization-defined types of and/or specific authenticators*] be carried out in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor).	user ID and password
IA-5 (8)	Authenticator Management	The organization takes [*Assignment: organization-defined measures*] to manage the risk of compromise due to individuals having accounts on multiples information systems.	
Incident Response			
IR-1	Incident Response Policy And Procedures	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: …	
IR-2	Incident Response Training	The organization: … b.Provides refresher training [*Assignment: organization-defined frequency*].	b. … at least annually
IR-3	Incident Response Testing and Exercises	The organization tests and/or exercises the incident response capability for the information system [*Assignment: organization-defined frequency*] using [*Assignment: organization-defined tests and/or exercises*] to determine the incident response effectiveness and documents the results.	… at least annually
IR-4(5)	Incident Handling	The organization implements a configurable capability to automatically disable the information system if any of the following security violations are detected: [*Assignment: organization-defined list of security violations*].	
IR-6	Incident Reporting	The organization: a.Requires personnel to report suspected security incidents to the organizational incident response capability within [*Assignment: organization-defined time-period*]; and …	a.

CNTL NO. (Enhancement)	CONTROL NAME	800-53 VARIABLE TEXT	DEFINED VALUE FOR NSS
IR-8	Incident Response Plan	The organization: … b.Distributes copies of the incident response plan to [*Assignment: organization-defined list of incident response personnel (identified by name and/or by role)and organizational elements*]; c.Reviews the incident response plan [*Assignment: organization-defined frequency*]; … e.Communicates incident response plan changes to [*Assignment: organization-defined list of incident response personnel (identified by name and/or by role) and organizational elements*].	b. c. e.
Maintenance			
MA-1	Maintenance Policy And Procedures	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: …	
MA-4 (5)	Non-Local Maintenance	The organization requires that: (a) Maintenance personnel notify [*Assignment: organization-defined personnel*] when non-local maintenance is planned (i.e., date/time); and …	(a)
MA-6	Timely Maintenance	The organization obtains maintenance support and/or spare parts for [*Assignment: organization-defined list of security-critical information system components and/or key information technology components*] within [*Assignment: organization-defined time period*] of failure.	
Media Protection			
MP-1	Media Protection Policy And Procedures	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: …	
MP-2	Media Access	The organization restricts access to [*Assignment: organization-defined types of digital and non-digital media*] to [*Assignment: organization-defined list of authorized individuals*] using [*Assignment: organization-defined security measures*].	
MP-3	Media Marking	The organization: a.Marks, in accordance with organizational policies and procedures, removable information system media and information system output indicating the distribution limitations, handling caveats and applicable security markings (if any) of the information; and b.Exempts [*Assignment: organization-defined list of removable media types*] from marking as long as the exempted items remain within [*Assignment: organization-defined controlled areas*].	b.
MP-4	Media Storage	The organization: a.Physically controls and securely stores [*Assignment: organization-defined types of digital and non-digital media*] within [*Assignment: organization-defined controlled areas*] using [*Assignment: organization-defined security measures*]; …	a.

CNTL NO. (Enhancement)	CONTROL NAME	800-53 VARIABLE TEXT	DEFINED VALUE FOR NSS
MP-5	Media Transport	The organization: a.Protects and controls [*Assignment: organization-defined types of digital and non-digital media*] during transport outside of controlled areas using [*Assignment: organization-defined security measures*]; …	a.
MP-6 (2)	Media Sanitization	The organization tests sanitization equipment and procedures to verify correct performance [*Assignment: organization-defined frequency*].	
MP-6 (3)	Media Sanitization	The organization sanitizes portable, removable storage devices prior to connecting such devices to the information system under the following circumstances: [*Assignment: organization-defined list of circumstances requiring sanitization of portable, removable storage devices*].	
Physical and Environmental Protection			
PE-1	Physical and Environmental Protection Policy And Procedures	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: …	
PE-2	Physical Access Authorizations	The organization: … c.Reviews and approves the access list and authorization credentials [*Assignment: organization-defined frequency*], removing from the access list, personnel no longer requiring access.	c. … at least annually
PE-3	Physical Access Control	The organization: … f.Inventories physical access devices [*Assignment: organization-defined frequency*]; and g.Changes combinations and keys [*Assignment: organization-defined frequency*] and when keys are lost, combinations are compromised, or individuals are transferred or terminated.	f. g.
PE-3(4)	Physical Access Control	The organization uses lockable physical casings to protect [*Assignment: organization-defined information system components*] from unauthorized physical access.	
PE-3(6)	Physical Access Control	The organization employs a penetration testing process that includes [*Assignment: organization-defined frequency*], unannounced attempts to bypass or circumvent security controls associated with physical access points to the facility.	
PE-6	Monitoring Physical Access	The organization: … b.Reviews physical access logs [*Assignment: organization-defined frequency*]; …	b.
PE-8	Access Records	The organization: … b.Reviews the visitor access records [*Assignment: organization-defined frequency*].	b.at least 90 days
PE-9 (2)	Power Equipment and Power Cabling	The organization employs automatic voltage controls for [*Assignment: organization-defined list of critical information system components*].	

CNTL NO. (Enhancement)	CONTROL NAME	800-53 VARIABLE TEXT	DEFINED VALUE FOR NSS
PE-10	Emergency Shutoff	The organization: … b. Places emergency shutoff switches or devices in [*Assignment: organization-defined location by information system or system component*] to facilitate safe and easy access for personnel; and …	b.
PE-13(4)	Fire Protection	The organization ensures that the facility undergoes [*Assignment: organization-defined frequency*] fire marshal inspections and promptly resolves identified deficiencies	
PE-14	Temperature and Humidity Controls	The organization: a.Maintains temperature and humidity levels within the facility where the information system resides at [*Assignment: organization-defined acceptable levels*]; and b.Monitors temperature and humidity levels [*Assignment: organization-defined frequency*].	a. b.
PE-16	Delivery and Removal	The organization authorizes, monitors, and controls [*Assignment: organization-defined types of information system components*] entering and exiting the facility and maintains records of those items.	
PE-17	Alternate Work Site	The organization: a.Employs [*Assignment: organization-defined management, operational, and technical information system security controls*] at alternate work sites; and …	a.
Planning			
PL-1	Planning Policy And Procedures	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: …	
PL-2	System Security Plan	The organization: … b.Reviews the security plan for the information system [*Assignment: organization-defined frequency*]; and …	b. … at least annually
PL-2 (1)	System Security Plan	The organization: … (b) Reviews and updates the CONOPS [*Assignment: organization-defined frequency*].	(b)
Personnel Security			
PS-1	Personnel Security Policy And Procedures	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: …	
PS-2	Position Categorization	The organization: … c.Reviews and revises position risk designations [*Assignment: organization-defined frequency*].	c. or at least annually
PS-3	Personnel Screening	The organization: … b.Rescreens individuals according to [*Assignment: organization-defined list of conditions requiring rescreening and, where periodic re-screening is so indicated, the frequency of such rescreening*].	b.

CNTL NO. (Enhancement)	CONTROL NAME	800-53 VARIABLE TEXT	DEFINED VALUE FOR NSS
PS-5	Personnel Transfer	The organization reviews logical and physical access authorizations to information systems/facilities when personnel are reassigned or transferred to other positions within the organization and initiates [*Assignment: organization-defined transfer or reassignment actions*] within [*Assignment: organization-defined time period following the formal transfer action*].	
PS-6	Access Agreements	The organization: … b.Reviews/updates the access agreements [*Assignment: organization-defined frequency*].	b. at least annually
Risk Assessment			
RA-1	Risk Assessment Policy And Procedures	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: …	
RA-3	Risk Assessment	The organization: … b. Documents risk assessment results in [*Selection: security plan; risk assessment report;* [*Assignment: organization-defined document*]]; c. Reviews risk assessment results [*Assignment: organization-defined frequency*]; and d. Updates the risk assessment [*Assignment: organization-defined frequency*] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.	b. c. at least every 3 years d. at least every 3 years
RA-5	Vulnerability Scanning	The organization: a.Scans for vulnerabilities in the information system and hosted applications [*Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process*] and when new vulnerabilities potentially affecting the system/applications are identified and reported; … d.Remediates legitimate vulnerabilities [*Assignment: organization-defined response times*] in accordance with an organizational assessment of risk; and …	a.no more than 45 days d.
RA-5 (2)	Vulnerability Scanning	The organization updates the list of information system vulnerabilities scanned [*Assignment: organization-defined frequency*] or when new vulnerabilities are identified and reported.	at least every 45 days
RA-5 (5)	Vulnerability Scanning	The organization includes privileged access authorization to [*Assignment: organization-identified information system components*] for selected vulnerability scanning activities to facilitate more thorough scanning.	
RA-5 (7)	Vulnerability Scanning	The organization employs automated mechanisms [*Assignment: organization-defined frequency*] to detect the presence of unauthorized software on organizational information systems and notify designated organizational officials.	
System and Services Acquisition			

CNTL NO. (Enhancement)	CONTROL NAME	800-53 VARIABLE TEXT	DEFINED VALUE FOR NSS
SA-1	System and Services Acquisition Policy And Procedures	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: …	
SA-9 (1)	External Information System Services	The organization: … b. Ensures that the acquisition or outsourcing of dedicated information security services is approved by [*Assignment: organization-defined senior organizational official*].	b. Chief Information Officer
SA-12	Supply Chain Protection	The organization protects against supply chain threats by employing: [*Assignment: organization-defined list of measures to protect against supply chain threats*] as part of a comprehensive, defense-in-breadth information security strategy.	
SA-13	Trustworthiness	The organization requires that the information system meets [*Assignment: organization-defined level of trustworthiness*].	
SA-14	Critical Information System Components	The organization: a. Determines [*Assignment: organization-defined list of critical information system components that require reimplementation*]; and …	a.
SA-14(1)	Critical Information System Components	The organization: … (b) Employs [*Assignment: organization-defined measures*] to ensure that critical security controls for the information system components are not compromised.	(b).
System and Communications Protection			
SC-1	System and Communications Protection Policy And Procedures	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: …	
SC-5	Denial of Service Protection	The information system protects against or limits the effects of the following types of denial of service attacks: [*Assignment: organization-defined list of types of denial of service attacks or reference to source for current list*].	
SC-7 (4)	Boundary Protection	The organization: … (e) Reviews exceptions to the traffic flow policy [*Assignment: organization-defined frequency*]	(e)
SC-7 (8)	Boundary Protection	The information system routes [*Assignment: organization-defined internal communications traffic*] to [*Assignment: organization-defined external networks*] through authenticated proxy servers within the managed interfaces of boundary protection devices.	
SC-7 (13)	Boundary Protection	The organization isolates [*Assignment: organization defined key information security tools, mechanisms, and support components*] from other internal information system components via physically separate subnets with managed interfaces to other portions of the system.	
SC-7 (14)	Boundary Protection	The organization protects against unauthorized physical connections across the boundary protections implemented at [*Assignment: organization-defined list of managed interfaces*].	

CNTL NO. (Enhancement)	CONTROL NAME	800-53 VARIABLE TEXT	DEFINED VALUE FOR NSS
SC-10	Network Disconnect	The information system terminates the network connection associated with a communications session at the end of the session or after [*Assignment: organization-defined time period*] of inactivity.	...no more than 48 hours
SC-11	Trusted Path	The information system establishes a trusted communications path between the user and the following security functions of the system: [*Assignment: organization-defined security functions to include at a minimum, information system authentication and reauthentication*].	
SC-12 (2)	Cryptographic Key Establishment and Management	The organization produces, controls, and distributes symmetric cryptographic keys using [*Selection: NIST-approved, NSA-approved*] key management technology and processes.	
SC-13(4)	Use of Cryptography	The organization employs [*Selection: FIPS- validated; NSA-approved*] cryptography to implement digital signatures.	
SC-15	Collaborative Computing Devices	The information system: a. Prohibits remote activation of collaborative computing devices with the following exceptions: [*Assignment: organization-defined exceptions where remote activation is to be allowed*]; and …	a.
SC-15 (3)	Collaborative Computing Devices	The organization disables or removes collaborative computing devices from information systems in [*Assignment: organization-defined secure work areas*].	

CNTL NO. (Enhancement)	CONTROL NAME	800-53 VARIABLE TEXT	DEFINED VALUE FOR NSS
SC-18 (2)	Mobile Code	The organization ensures the acquisition, development, and/or use of mobile code to be deployed in information systems meets [*Assignment: organization-defined mobile code requirements*].	(a) Emerging mobile code technologies that have not undergone a risk assessment and been assigned to a Risk Category by the CIO are not used. (b) Category 1 mobile code is signed with a code signing certificate; use of unsigned Category 1 mobile code is prohibited; use of Category 1 mobile code technologies that cannot block or disable unsigned mobile code (e.g., Windows Scripting Host) is prohibited. (c) Category 2 mobile code which executes in a constrained environment without access to system resources (e.g., Windows registry, file system, system parameters, and network connections to other than the originating host) may be used. (d) Category 2 mobile code that does not execute in a constrained environment may be used when obtained from a trusted source over an assured channel (e.g., SIPRNet, SSL connection, S/MIME, code is signed with an approved code signing certificate). (e) Category 3 mobile code may be used.
SC-18 (4)	Mobile Code	The information system prevents the automatic execution of mobile code in [*Assignment: organization-defined software applications*] and requires [*Assignment: organization-defined actions*] prior to executing the code.	E-mail prompting the user
SC-23 (4)	Session Authenticity	The information system generates unique session identifiers with [*Assignment: organization-defined randomness requirements*].	
SC-24	Fail in Known State	The information system fails to a [*Assignment: organization-defined known-state*] for [*Assignment: organization-defined types of failures*] preserving [*Assignment: organization-defined system state information*] in failure.	
SC-27	Operating System-Independent Applications	The information system includes [*Assignment: organization-defined operating system-independent applications*].	

CNTL NO. (Enhancement)	CONTROL NAME	800-53 VARIABLE TEXT	DEFINED VALUE FOR NSS
SC-30 (1)	Virtualization Techniques	The organization employs virtualization techniques to support the deployment of a diversity of operating systems and applications that are changed [*Assignment: organization-defined frequency*].	
SC-34	Non-Modifiable Executable Programs	The information system at [*Assignment: organization-defined information system components*]: … b. Loads and executes [*Assignment: organization-defined applications*] from hardware-enforced, read-only media.	b.
SC-34(1)	Non-Modifiable Executable Programs	The organization employs [*Assignment: organization-defined information system components*] with no writeable storage that is persistent across component restart or power on/off	
System and Information Integrity			
SI-1	System and Information Integrity Policy And Procedures	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: …	
SI-2 (2)	Flaw Remediation	The organization employs automated mechanisms [*Assignment: organization-defined frequency*] to determine the state of information system components with regard to flaw remediation.	
SI-2 (3)	Flaw Remediation	The organization measures the time between flaw identification and flaw remediation, comparing with [*Assignment: organization-defined benchmarks*].	
SI-2 (4)	Flaw Remediation	The organization employs automated patch management tools to facilitate flaw remediation to [*Assignment: organization-defined information system components*].	
SI-3	Malicious Code Protection	The organization: … c.Configures malicious code protection mechanisms to: - perform periodic scans of the information system [*Assignment: organization-defined frequency*] and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy; and - [*Selection (one or more): block malicious code; quarantine malicious code; send alert to administrator;* [*Assignment: organization-defined action*]] in response to malicious code detection;	c.
SI-3 (6)	Malicious Code Protection	The organization tests malicious code protection mechanisms [*Assignment: organization-defined frequency*] by introducing a known benign, non-spreading test case into the information system and subsequently verifying that both detection of the test case and associated incident reporting occur, as required.	

CNTL NO. (Enhancement)	CONTROL NAME	800-53 VARIABLE TEXT	DEFINED VALUE FOR NSS
SI-4	Information System Monitoring	The organization: a. Monitors events on the information system in accordance with [*Assignment: organization-defined monitoring objectives*] and detects information system attacks; …	a.
SI-4 (5)	Information System Monitoring	The information system provides near real-time alerts when the following indications of compromise or potential compromise occur: [*Assignment: organization-defined list of compromise indicators*].	
SI-4 (7)	Information System Monitoring	The information system notifies [*Assignment: organization-defined list of incident response personnel (identified by name and/or by role)*] of suspicious events and takes [*Assignment: organization-defined list of least-disruptive actions to terminate suspicious events*].	
SI-4 (9)	Information System Monitoring	The organization tests/exercises intrusion monitoring tools [*Assignment: organization-defined time-period*].	at least monthly
SI-4 (12)	Information System Monitoring	The organization employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications: [*Assignment: organization-defined list of inappropriate or unusual activities that trigger alerts*].	
SI-4 (13)	Information System Monitoring	The organization: … (c)Uses the traffic/event profiles in tuning system monitoring devices to reduce the number of false positives to [*Assignment: organization-defined measure of false positives*] and the number of false negatives to [*Assignment: organization-defined measure of false negatives*].	(c)
SI-5	Security Alerts, Advisories, and Directives	The organization: … c. Disseminates security alerts, advisories, and directives to [*Assignment: organization-defined list of personnel (identified by name and/or by role)*]; and …	c.
SI-6	Security Functionality Verification	The information system verifies the correct operation of security functions [*Selection (one or more): [Assignment: organization-defined system transitional states]; upon command by user with appropriate privilege; periodically every* [*Assignment: organization-defined time-period*]] and [*Selection (one or more): notifies system administrator; shuts the system down; restarts the system;* [*Assignment: organization-defined alternative action(s)*]] when anomalies are discovered.	upon system startup and/or restart at least every 90 days
SI-7 (1)	Software and Information Integrity	The organization reassesses the integrity of software and information by performing [*Assignment: organization-defined frequency*] integrity scans of the information system.	not to exceed 180 days
SI-7 (4)	Software and Information Integrity	The organization requires use of tamper evident packaging for [*Assignment: organization-defined information system components*] during [*Selection: transportation from vendor to operational site; during operation; both*].	

CNTL NO. (Enhancement)	CONTROL NAME	800-53 VARIABLE TEXT	DEFINED VALUE FOR NSS
SI-11	Error Handling	The information system: a. … b. Generates error messages that provide information necessary for corrective actions without revealing [*Assignment: organization-defined sensitive or potentially harmful information*] in error logs and administrative messages that could be exploited by adversaries; and …	b.
SI-13	Predictable Failure Prevention	The organization: a. Protects the information system from harm by considering mean time to failure for [*Assignment: organization-defined list of information system components*] in specific environments of operation; …	a.
SI-13 (1)	Predictable Failure Prevention	The organization takes the information system component out of service by transferring component responsibilities to a substitute component no later than [*Assignment: organization-defined fraction or percentage*] of mean time to failure.	
SI-13 (2)	Predictable Failure Prevention	The organization does not allow a process to execute without supervision for more than [*Assignment: organization-defined time period*].	
SI-13 (3)	Predictable Failure Prevention	The organization manually initiates a transfer between active and standby information system components at least once per [*Assignment: organization-defined frequency*] if the mean time to failure exceeds [*Assignment: organization-defined time period*].	
SI-13 (4)	Predictable Failure Prevention	The organization, if an information system component failure is detected: (a)Ensures that the standby information system component successfully and transparently assumes its role within [*Assignment: organization-defined time period*]; and (b)[*Selection (one or more): activates* [*Assignment: organization-defined alarm*]; *automatically shuts down the information system*].	(a) (b)
Program Management			
PM-1	Security Program Plan	The organization: a. … b. Reviews the organization-wide information security program plan [*Assignment: organization-defined frequency*]	b.