CNSSI No. 1253
15 March 2012

SECURITY CATEGORIZATION AND CONTROL SELECTION FOR NATIONAL SECURITY SYSTEMS

Version 2

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

NATIONAL MANAGER

FOREWORD

1. The Committee on National Security Systems Instruction (CNSSI) No. 1253, "Security Categorization and Control Selection for National Security Systems," provides all Federal Government departments, agencies, bureaus, and offices with a process for security categorization of National Security Systems (NSS). It references a comprehensive set of security controls and enhancements that may be applied to any NSS. CNSSI 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, Senior Information Security Officers, and others 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," (Reference 1), which outlines the roles and responsibilities for securing NSS, and applicable sections of the Federal Information Security Management Act (FISMA) of 2002.

3. This Instruction is formatted to align with the section 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," (Reference 3) to ensure CNSSI No. 1253 serves as a companion document to NIST SP 800-53.

4. CNSSI No. 1253 is effective upon receipt.

5. Additional copies of this Instruction may be obtained from the CNSS Secretariat or the CNSS website: http://www.cnss.gov.

FOR THE NATIONAL MANAGER

//s//

DEBORA A. PLUNKETT

CNSS Secretariat (IE32). National Security Agency. 9800 Savage Road, STE 6716. Ft Meade, MD 20755-6716
Office: (410) 854-6805 Unclassified FAX: (410) 854-6814
CNSS@radium.ncsc.mil

TABLE OF CONTENTS

TABLE OF FIGURES AND TABLES

CHAPTER ONE

1. INTRODUCTION

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. As part of the Joint Task Force Transformation Initiative Working Group, the Committee on National Security Systems (CNSS) has worked with representatives from the Civil, Defense, and Intelligence Communities to produce a unified information security framework and to ensure NIST SP 800-53 contains security controls to meet the requirements of National Security Systems (NSS).[1] As a result of these collaborative efforts, the Director of National Intelligence and the Secretary of Defense have directed that the processes and controls described in NIST SP 800-53, as amended by this Instruction, shall apply to all NSS. This means NIST SP 800-53 now provides a common foundation for information security controls across the U.S. Federal Government.

1.1 PURPOSE AND SCOPE

This Instruction serves as a companion document to NIST SP 800-53 for organizations that employ NSS. It establishes the processes for categorizing NSS and the information they process and for appropriately selecting security controls for NSS from NIST SP 800-53. This Instruction applies to all components[2] of NSS. For NSS, where differences between the NIST documentation and this Instruction occur, this Instruction is authoritative.

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 NSS results in some variance from the non-NSS sector with respect to the process for information and information system categorization. This Instruction, therefore, provides the processes for categorizing NSS and the information they process and for selecting security controls to provide appropriate protections for NSS.

To support reciprocity among national security community members, this Instruction provides, in Appendix J, a set of organization-defined values for key parameters where NIST SP 800-53 leaves the determination of those values up to the implementing organization. These values are provided for all controls requiring such values that are included on one or more baselines, where a standard value for that parameter for all NSS has been determined.

---

[1] 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 defines the phrase "national security system", and provides government-wide requirements for information security.

[2] 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.

1.2 TARGET AUDIENCE

This Instruction serves the national security community's information security and information assurance (IA) professionals, including those responsible for—

- Information systems, information security, or risk management and oversight (e.g., Chief Information Officers [CIO], Risk Executive (Function), Senior Information Security Officers [SISO], and Authorizing Officials)

- Information system development (e.g., program and project managers, mission/application owners, system designers, system/application programmers, Information Security Systems Engineers [ISSE], and Information Security Architects)

- Information security implementation and operation (e.g., information system owners, data stewards, ISSEs, information system administrators, Information System Security Officers [ISSO], and Information System Security Managers [ISSM])

- Information system and information security assessment and monitoring (e.g., auditors, Inspectors General [IGs], evaluators, ISSOs, and assessors).

1.3 KEY DIFFERENCES BETWEEN CNSSI NO. 1253 AND NIST PUBLICATIONS

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.

- Both FIPS 200 (Reference 10) and NIST 800-53 apply the concept of a high-water mark (HWM) when categorizing information systems using the worst-case potential impact of a loss of confidentiality, integrity, or availability of information or of an information system as the basis for categorization. That is, after the potential impact values for the confidentiality, integrity, and availability security objectives are each determined, the highest of the three is selected as the overall impact level[3] (single value), or HWM, for the system. This Instruction does not adopt this HWM usage for information systems. When establishing the security category of an NSS, the values determined for confidentiality, integrity, and availability are retained. Retaining the discrete values 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 and supplementing of controls. The definition for what constitutes a low, moderate, or high confidentiality, integrity, and availability value is included in Chapter 2, Section 2.1.

- Potential impact is only one factor used in the method for categorizing NSS for confidentiality. Additional factors considered are the aggregation of information on the system, system environment, and attributes of users. The categorization method is described in Chapter 2, Section 2.1.

[3] The overall impact level is a term used in FIPS 200. This term is not used in and is not applicable to NSS.

- The methodology provided in this Instruction supplements the use of security control baselines with the use of security control overlays, as applicable. The result is a set of security controls that will more appropriately protect an NSS and reduce the need for tailoring and its required justification. Overlays are described in Appendix K.

- It is the policy within the national security community that member organizations practice reciprocity with respect to the assessment of NSSs and NSS components to the greatest extent practicable. Reciprocity may reduce the cost and time to implement systems and system components. To facilitate reciprocity, this document provides explicit sets of controls, referred to as baselines, for organizations to use in the control selection process described in Chapter 3 of this document. These baselines are provided in Appendix D.

CHAPTER TWO

2. CATEGORIZING NSS AND THE INFORMATION THEY CONTAIN

The Risk Management Framework (RMF), described in NIST SP 800-37 (Reference 4), provides organizations a framework for risk management within their information system development activities. For each information system, the first step in the RMF is to categorize the system and the information it processes. This correlates to the initiation (concept/requirements definition) phase of the system development life cycle (SDLC).

Security categorization is the process of characterizing information or an information system by determining the appropriate values for factors that definitively represent the protection needs of the information or the information system. The following sections establish the security categorization guidelines for NSS and the information they contain. These guidelines describe and specify the use of a single method for completion of the Categorize step in the RMF.

The results of the security categorization are subsequently used in defining the set of controls applied to the system. The set of controls is determined during the Select step of the RMF, the process for which is described in Chapter 3 of this Instruction. Determining the appropriate controls for NSS helps organizations properly manage their NSS-related mission, business, and system risks.

2.1 CATEGORIZATION METHOD

The security categorization method builds on the foundation established in FIPS 199, which defines three impact values (low, moderate, or high) reflecting the potential impact on organizations or individuals should a security breach occur (i.e., a loss of confidentiality, integrity, or availability). Organizations that employ NSS applying these definitions must do so within the context of their organization and the overall national interest.

Security categorization is a two-step process:

Step 1. Determine potential impact values for the information type(s)[4] processed, stored or transmitted by the system.

Step 2. Categorize the information system using appropriate values accounting for potential impact as well as the additional categorization factors identified in Section 2.1.2.

The determination of potential impact for an NSS relies on common definitions for each of the potential impact values. These potential impact values are defined as follows:

[4] 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. NIST SP 800-60 (Volumes I and II) provide an example methodology for determining information types.

- 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.

- 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.***[6]

- 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 Potential Impact Determination for Information Types

The potential impact for each information type on an information system may vary based on the nature of the information. The potential impact for an information type is established by the potential impact resulting from of a loss of confidentiality, integrity, or availability associated

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

[6] Within the national security community it is understood that certain losses are to be expected when performing particular missions.

with it. Determination of the potential impact for an information type is a worst-case assessment of 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 represented as a set of three values, reflecting the potential impact with respect to the three security objectives of confidentiality, integrity, and availability.

Categorization of NSS begins by determining 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 determination of the potential impact for one security objective (e.g., confidentiality) is independent of the potential impact determination of the other two objectives (integrity and availability).

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

> **SC** information type = {(**confidentiality**, *value*), (**integrity,** *value*), (**availability,** *value*)}, where the acceptable values are low, moderate, or high.

2.1.2 Categorization of NSS

The categorization of an NSS must consider the security category of each information type resident on the system. For an NSS, the values assigned to the respective security objectives of integrity and availability will be the highest values from among those security categories that have been determined for each information type resident on the NSS.

Confidentiality Categorization

The Confidentiality categorization of an NSS is derived from the potential impact value (determined in 2.1.1, above) and additional factors, which are:

- Aggregation of information;
- Information system environment; and
- Attributes of users.

The highest potential impact value determined for any of the information types processed, stored or transmitted by the system serves as a point of reference for the confidentiality value of the information system. However, the additional factors listed above may result in the need for the information system's confidentiality value to be lower or higher than the information's confidentiality value.

All classified NSS must be categorized as Moderate or High for confidentiality.

For information systems with information having a confidentiality value of High, if the additional factors permit, the information system categorization for confidentiality may be designated as Moderate.

For information systems with information having a confidentiality value of Moderate or Low, if *at least one* of the additional factors identified above requires, the information system

categorization for confidentiality must be designated higher than the information confidentiality value.

Aggregation of information – If the information system contains information that, when aggregated, increases the risk to the organization, the system's confidentiality value may need to be designated at a value higher than the information confidentiality value.

Information system environment – If the information system is physically located in an environment that is authorized for the processing or open storage of the information processed by the system (e.g., an accredited Sensitive Compartmented Information Facility [SCIF] for SCI information), the system's confidentiality value may be designated at a value lower than the confidentiality value of its information (but not lower than moderate for classified NSS). If the information system is not located in such an environment, the system's confidentiality value may need to be designated higher than the information confidentiality value.

Attributes of users[7] – If the information system must provide capabilities to mitigate the risk of users having access to classified information for which they lack either the required security clearance or the required citizenship; then the system's confidentiality value should be designated as High. If the information system is not required to mitigate these types of risks, then the system's confidentiality value may be designated at a value of Moderate.

Integrity and Availability Categorization

Systems commonly contain information types that may have different potential impacts. In that case, the information type with the highest potential impact for each security objective (integrity and availability) defines the value assigned to that security objective. 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 system's availability value would be designated as Moderate because this is the highest availability potential impact value of information processed by the system. A similar determination is made for the integrity security objective.

The generalized format for expressing the security category (SC) of an NSS is —

> **SC** NSS = {(**confidentiality**, *value*), (**integrity**, *value*), (**availability**, *value*)}, where the acceptable values are low, moderate, or high.

[7] This section of CNSSI No. 1253 describes the effect that some user attributes have on system confidentiality categorization, which in turn drives the selection of specific baselines of security controls. While all appropriate security control overlays must be applied, some user attributes require the selection and application of specific security control overlays. This includes, but is not limited to, overlays needed when the system must provide capabilities to mitigate the risk of users having access to information for which they lack either the required security clearances, the required citizenship, or the required formal access approvals for compartments. Section 3.2 and Appendix K of this Instruction provide additional guidance on security control overlays.

CHAPTER THREE

3. CONTROL SELECTION WITHIN THE RISK MANAGEMENT FRAMEWORK

Once security categorization is successfully accomplished in accordance with the process described in Chapter 2 for an information system, Step 2 of the RMF requires the organization to determine the appropriate security controls to apply to the NSS in order to properly manage their mission, business, and system risks.

Because NSS provide unique capabilities, operate in diverse environments, and are subject to advanced cyber threats, an organization-wide risk-based approach must be taken when defining and implementing the security controls for an NSS. This risk-based approach to control selection considers effectiveness, efficiency, operational needs, and constraints resulting from applicable public laws, executive orders, directives, policies, and other official guidance. NIST SP 800-39 (Reference 5) provides guidance for an integrated, organization-wide program for managing information security risk to organizational operations, organizational assets, individuals, other organizations, and the Nation resulting from the operation and use of federal information systems. Key to developing an organization-wide risk-based approach is the establishment of a risk tolerance by the Authorizing Official or Risk Executive (Function) to guide control selection and security engineering activities for all NSS under their purview.

The following sections establish the risk-based security control selection guidelines for NSS. These guidelines describe and specify the use of a security control selection methodology, as well as the process for selecting and applying overlays, tailoring, and supplementing the baseline (i.e., the initial control set).

The process for selecting security controls for an NSS is a four-step process:

Step 1. Select the initial set of security controls.

Step 2. Select and apply security control overlays.

Step 3. Tailor the set of security controls.

Step 4. Supplement the tailored set of security controls.

3.1 SELECTING THE INITIAL SET OF SECURITY CONTROLS

Selecting the initial control set, or baseline, is the process of aggregating the controls identified in table D-1 provided in Appendix D, corresponding to the security categorization of the system (i.e., the values determined for each security objective [confidentiality, integrity, and availability]).

3.2 SELECTING AND APPLYING SECURITY CONTROL OVERLAYS

Security control overlays are specifications of security controls and supporting guidance used to complement the security control baselines and parameter values in CNSSI No. 1253 and to complement the supplemental guidance in NIST SP 800-53. Organizations select and apply

security control overlays by using the guidance in each of the standardized, approved and CNSS-published overlays.

Applying one or more required overlays provides a structured form of tailoring (as described in Section 3.3) and supplementation (as described in Section 3.4) of the initially-selected set of security controls. Applying one or more overlays can reduce, but does not necessarily eliminate completely, the need for additional tailoring and supplementing controls.

If the use of multiple overlays results in conflicts between the application or removal of security controls, the Authorizing Official (or designee), in coordination with the information owner/steward, will resolve the conflict. If a control is added or removed by the application of an overlay, the security plan must reflect the change with the justification being the application of the specific overlay(s) directing the change. Further guidance on overlays is provided in Appendix K of this document.

3.3 TAILORING THE SET OF SECURITY CONTROLS

Authorizing officials, the Risk Executive (Function), and other decision-makers may find it necessary to tailor (modify) a control set. The resultant set of security controls derived from tailoring is referred to as the tailored control set. NIST SP 800-53 identifies three types of tailoring activities:

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

Refer to and use NIST SP 800-53, Section 3.3 for initial guidance on tailoring controls. Use the remainder of this section for additional tailoring guidance for NSS.

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 outweighs the security need for screen or session lock capability.

Organizations should remove security controls only as a function of specified, risk-based determinations. Tailoring decisions, including the specific rationale (i.e., mapping to risk tolerance) for those decisions, are documented in the security plan for the information system.

Every selected control must be accounted for either by the organization or the information system owner. If a selected control is not implemented, then the rationale for not implementing the control must be documented in the security plan.

3.3.1 **Scoping Guidance**

There are a number of factors that may affect the security controls that apply to an NSS, and may result in the tailoring of the control set. These factors include those described in NIST SP

800-53, Section 3.3, as well as the mobility of the physical hosting environment, and the processing and storage capabilities of an NSS.

Mobility

The mobility of the physical hosting environment can impact the set of security controls selected for the system. The 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 set of security controls should be tailored appropriately to account for the difference in the mobility and accessibility of the location housing an NSS.

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 PE-7, Visitor Control, may be met by the system's mobility, because they generally preclude casual visitors.

Processing and Storage Capability

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 may not have the same general processing and storage capabilities assumed for the categorized controls. This does not preclude organizations from selectively applying the recommended controls to these types 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) while in other instances it would be impractical (e.g., physical and environmental controls).

3.3.2 Compensating Security Controls

Compensating security controls are needed because all possible circumstances cannot be anticipated when constructing an initial set of security controls. A variety of circumstances may require the use of compensating security controls:

- The selected control in the catalog cannot be applied to a given NSS.
- The selected control would impose costs beyond the budgetary capabilities of the organization.
- The selected control may have a significantly adverse effect on mission requirements (e.g., need to deploy the system rapidly in a mobile configuration).

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 weaker automated I&A measures than are called for in baseline-derived sets of security controls (e.g., two-factor authentication).

The use of compensating security controls must be documented in the security plan for the information system and approved by the authorizing official.[8] The control(s) being replaced, the compensating controls, and the justification must be addressed in the security plan.

If a selected security control cannot or will not be implemented in the information system and no compensating control(s) will be substituted for the selected control, this decision must be:

1. Documented in the security plan for the information system with a justification for why the control cannot be implemented;

2. Coordinated with the information owner/steward;

3. Approved by the authorizing official; and

4. At the discretion of the authorizing official, included in the Plan of Action and Milestones (POA&M) for the system.

3.3.3. Specification of Organization-Defined Parameters

Appendix J of this Instruction provides values for each control where a value has been established as a standard for all NSS to facilitate reciprocity within the national security community. Based on the risk tolerance or threat scenario for an NSS, some authorizing officials may allow or require systems to diverge from this standard. In these situations, additional technology may be added, or architectural implementations may be modified to adequately mitigate applicable risks. By establishing a standard on key parameters, organizations have a known baseline when accepting assessments of technologies or systems from other national security community organizations and do not have to duplicate the assessment. When reciprocity is to be extended across authorizing officials, or when one system provides security on behalf of another system, values for parameters that differ from those published in Appendix J are negotiated between the relevant authorizing officials and the results are documented in the security plan for each system.

3.4 SUPPLEMENTING THE TAILORED SET OF SECURITY CONTROLS

Supplementation addresses residual risks not adequately mitigated by the tailored control set but may not eliminate all residual risk. In many cases, additional security controls or control enhancements will be needed to address specific threats to or vulnerabilities in an NSS or to

[8] This Instruction encourages organizations to select compensating controls from the NIST SP 800-53 Security Controls Catalog. There may be instances where organization-defined compensating controls should be employed, because the Security Controls Catalog does not contain suitable compensating controls.

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 tailored set of security controls. The inclusion of each control is based on the need to reduce risk to an established tolerance level.

APPENDIX A

REFERENCES

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

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

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

2. Federal Information Security Management Act (P.L. 107-347, Title III), December 2002.

3. National Institute of Standards and Technology Special Publication 800-53, Revision 3,"Recommended Security Controls for Federal Information Systems and Organizations," August 2009.[9]

4. National Institute of Standards and Technology Special Publication 800-37, Revision 1, "Guide for Applying the Risk Management Framework to Federal Information Systems, A Security Life Cycle Approach," February 2010.

5. National Institute of Standards and Technology Special Publication 800-39, "Managing Information Security Risk: Organization, Mission, and Information System View," March 2011.

6. National Institute of Standards and Technology Special Publication 800-59, "Guideline for Identifying an Information System as a National Security System," August 2003.

7. National Institute of Standards and Technology Special Publication 800-60, Revision 1, "Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories," August 2008.

8. National Institute of Standards and Technology Special Publication 800-60, Revision 1, "Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories," August 2008

9. Federal Information Processing Standards Publication 199, "Standards for Security Categorization of Federal Information and Information Systems," February 2004.

10. Federal Information Processing Standards Publication 200, "Minimum Security Requirements for Federal Information and Information Systems," March 2006.

[9] Includes errata update as of 1 May 2010.

APPENDIX B

GLOSSARY
COMMON TERMS AND DEFINITIONS

This publication is written to maximize consistency with the usage of terms in National Institute of Standards and Technology Special Publication 800-53, Revision 3, and Committee on National Security Systems Instruction No. 4009, "National Information Assurance Glossary." Terms and/or definitions unique to this publication are identified below.

Impact	The effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States; of a loss of confidentiality, integrity or availability of information or an information system.
Impact value	The assessed potential impact resulting from a compromise of the confidentiality, integrity, or availability of an information type, expressed as a value of either low, moderate or high.
National security community	The community of Federal Government departments, agencies, bureaus, and offices that employ NSS.
Overlay	A specification of security controls and supporting guidance used to complement the security control baselines and parameter values in CNSSI No. 1253 and to complement the supplemental guidance in NIST SP 800-53. An overlay's specifications may be more stringent or less stringent than the controls and guidance complemented.
Security category	A group of terms that concisely summarizes the results of a security categorization.
Security control baseline	A set of information security controls that has been established through information security strategic planning activities to address one or more specified security categorizations; this set of security controls is intended to be the initial security control set selected for a specific system once that system's security categorization is determined.

APPENDIX C

ACRONYMS
COMMON ABBREVIATIONS

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

CIO	Chief Information Officer
CNSS	Committee on National Security Systems
FISMA	Federal Information Security Management Act
HWM	High Water Mark
IA	Information Assurance
IC	Intelligence Community
IG	Inspector General
ISSE	Information System Security Engineer
ISSM	Information System Security Manager
ISSO	Information System Security Officer
JWICS	Joint Worldwide Intelligence Communications System
NIST	National Institute of Standards and Technology
NSI	National Security Information
NSS	National Security System
PII	Personally Identifiable Information
POA&M	Plan of Actions and Milestones
RMF	Risk Management Framework
SC	Security Category
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SDLC	System Development Life Cycle

SISO	Senior Information Security Officer
SP	Special Publication
U.S.	United States
U.S.C.	United States Code

APPENDIX D

SECURITY CONTROL BASELINES—SUMMARY
BASELINE CONTROLS BY VALUE PER SECURITY OBJECTIVE

Table D–1 identifies the initial security control sets (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 value (Low, Moderate, and High) per security objective (confidentiality, integrity, and availability).

Table D–2 lists the security controls from NIST SP 800-53, Revision 3, Appendix F, and identifies their relationships to security objectives (confidentiality, integrity, and availability). 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.

Table D–1 and D-2 are consistent with the assumptions and guidelines provided in this Appendix. The designation of applicability and relationships in this table is referred to as binning or allocation.

Assumptions and Guidelines for Confidentiality, Integrity, and Availability Binning

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

> **CONFIDENTIALITY (C):** "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 (I):** "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 (A):** "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.

Based on these definitions and a review of the controls and enhancements, the following rules for control allocation were established:

Primary Focus. Each control and/or enhancement was allocated based on whether the security objective(s) were the *primary* focus of the control and/or enhancement. If a security objective was only indirectly affected by a control and/or enhancement, it was not associated with that control and/or enhancement. In some cases, only one objective was the primary focus of a control and/or 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 control baselines do not characterize controls as having relationships with security objectives.

The determination was made that—

- The C and I objectives are largely focused on reading and writing (disclosure and modification).
- The I objective is also concerned with the correctness of actions.
- 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 application of these rules resulted in consequences to the allocations of the various families. For example, the controls and enhancements of the AC family were largely binned as C and I, 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.

Accountability. The controls and enhancements focusing on Accountability (largely the AU and IA families) were allocated C and I, unless explicitly indicated otherwise.

Class of Family. The families that were categorized as Management or Operational were largely allocated to C, I, and A; 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 allocated to A, and the SA and SI families were largely allocated to I.

X-1. The first entry in each family (AU-1, CA-1) was often hard to allocate 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 allocated across the family; therefore it was allocated to C, I, and A in most instances.

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 allocated to C and I. If the control addressed using cryptography to protect the confidentiality of information, then it was allocated only to C.

PE Family. The PE family was a dichotomy. Many of the controls and enhancements were focused on providing physical access control. Those were allocated in a manner comparable to the majority of the AC family. Some of the controls and/or enhancements were focused on environmental issues (e.g., adequate air conditioning). Those controls/enhancements were largely allocated to 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, Moderate, and High Binning

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

- 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.

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

Table D-1 Legend

There are nine columns in Table D-1 labeled in the header rows for the three security objectives (confidentiality, integrity, or availability) and for the three possible values (low, moderate, or high) for each objective. An X in the table within one of these columns signifies the control in that row is allocated to that security objective and at that value specified. A blank signifies the control is not allocated. Some controls are not allocated because even though they represent capabilities that may be required by some organizations under some circumstances, they are not considered necessary for NSS based on any value for confidentiality, integrity, or availability. Controls not allocated can be allocated through the application of overlays or 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.

There is an additional column in Table D-1 indicating whether the controls are suggested to be implemented as common controls. Common controls are security controls that are inherited by one or more organizational information systems.

This column is intended to provide guidance to assist with implementation planning. The final determination of which controls will be implemented as common controls will vary depending on the system and its intended environment/deployment. All controls selected for an information system must be addressed in the security plan, whether those controls are implemented by the information system or inherited from a common control provider. Evidence must be included or referenced in the security plan to show the information system actually receives protection from the inheritable security controls; that is, inheritable does not equate to inherited.

Table D–1: Security Control Baselines

ID	Title	Confidentiality			Integrity			Availability			Suggested Common
		L	M	H	L	M	H	L	M	H	
AC-1	Access Control Policy And Procedures	X	X	X	X	X	X	X	X	X	X
AC-2	Account Management	X	X	X	X	X	X				X
AC-2(1)	Account Management	X	X	X	X	X	X				
AC-2(2)	Account Management	X	X	X	X	X	X				
AC-2(3)	Account Management	X	X	X	X	X	X				
AC-2(4)	Account Management	X	X	X	X	X	X				
AC-2(5)	Account Management										X
AC-2(6)	Account Management										
AC-2(7)	Account Management	X	X	X	X	X	X				
AC-3	Access Enforcement	X	X	X	X	X	X				
~~AC-3(1)~~	~~Access Enforcement~~ [Withdrawn][10]	-	-	-	-	-	-	-	-	-	
AC-3(2)	Access Enforcement										
AC-3(3)	Access Enforcement										
AC-3(4)	Access Enforcement	X	X	X	X	X	X				
AC-3(5)	Access Enforcement										
AC-3(6)	Access Enforcement			X							
AC-4	Information Flow Enforcement	X	X	X	X	X	X				
AC-4(1)	Information Flow Enforcement										
AC-4(2)	Information Flow Enforcement										
AC-4(3)	Information Flow Enforcement										
AC-4(4)	Information Flow Enforcement										
AC-4(5)	Information Flow Enforcement										
AC-4(6)	Information Flow Enforcement										
AC-4(7)	Information Flow Enforcement										
AC-4(8)	Information Flow Enforcement										
AC-4(9)	Information Flow Enforcement										
AC-4(10)	Information Flow Enforcement										
AC-4(11)	Information Flow Enforcement										
AC-4(12)	Information Flow Enforcement										
AC-4(13)	Information Flow Enforcement										
AC-4(14)	Information Flow Enforcement										
AC-	Information Flow Enforcement										

[10] Table entries marked with [Withdrawn] were withdrawn from NIST SP 800-53.

ID	Title	Confidentiality			Integrity			Availability			Suggested Common
		L	M	H	L	M	H	L	M	H	
4(15)											
AC-4(16)	Information Flow Enforcement										
AC-4(17)	Information Flow Enforcement										
AC-5	Separation Of Duties	X	X	X	X	X	X				
AC-6	Least Privilege	X	X	X	X	X	X				X
AC-6(1)	Least Privilege	X	X	X	X	X	X				X
AC-6(2)	Least Privilege	X	X	X	X	X	X				X
AC-6(3)	Least Privilege										
AC-6(4)	Least Privilege										
AC-6(5)	Least Privilege	X	X	X	X	X	X				X
AC-6(6)	Least Privilege			X			X				X
AC-7	Unsuccessful Login Attempts	X	X	X	X	X	X	X	X	X	
AC-7(1)	Unsuccessful Login Attempts		X	X		X	X				
AC-7(2)	Unsuccessful Login Attempts										
AC-8	System Use Notification	X	X	X	X	X	X				
AC-9	Previous Logon (Access) Notification					X	X				
AC-9(1)	Previous Logon (Access) Notification										
AC-9(2)	Previous Logon (Access) Notification										
AC-9(3)	Previous Logon (Access) Notification										
AC-10	Concurrent Session Control					X	X		X	X	
AC-11	Session Lock	X	X	X	X	X	X				
AC-11(1)	Session Lock	X	X	X							
~~AC-12~~	~~Session Termination~~ [Withdrawn]	-	-	-	-	-	-	-	-	-	
~~AC-13~~	~~Supervision And Review — Access Control~~ [Withdrawn]	-	-	-	-	-	-	-	-	-	
AC-14	Permitted Actions Without Identification Or Authentication	X	X	X	X	X	X				
AC-14(1)	Permitted Actions Without Identification Or Authentication		X	X		X	X				
~~AC-15~~	~~Automated Marking~~ [Withdrawn]	-	-	-	-	-	-	-	-	-	
AC-16	Security Attributes										
AC-16(1)	Security Attributes										
AC-16(2)	Security Attributes										
AC-16(3)	Security Attributes										
AC-16(4)	Security Attributes										
AC-	Security Attributes										

ID	Title	Confidentiality			Integrity			Availability			Suggested Common
		L	M	H	L	M	H	L	M	H	
16(5)											
AC-17	Remote Access	X	X	X	X	X	X				X
AC-17(1)	Remote Access	X	X	X	X	X	X				
AC-17(2)	Remote Access	X	X	X	X	X	X				
AC-17(3)	Remote Access	X	X	X	X	X	X				
AC-17(4)	Remote Access	X	X	X	X	X	X				
AC-17(5)	Remote Access	X	X	X	X	X	X				X
AC-17(6)	Remote Access	X	X	X							X
AC-17(7)	Remote Access	X	X	X	X	X	X				
AC-17(8)	Remote Access	X	X	X	X	X	X				
AC-18	Wireless Access Restrictions	X	X	X	X	X	X				X
AC-18(1)	Wireless Access Restrictions	X	X	X	X	X	X				
AC-18(2)	Wireless Access Restrictions	X	X	X	X	X	X				X
AC-18(3)	Wireless Access Restrictions	X	X	X	X	X	X				
AC-18(4)	Wireless Access Restrictions	X	X	X	X	X	X				X
AC-18(5)	Wireless Access Restrictions	X	X	X	X	X	X				X
AC-19	Access Control For Mobile Devices	X	X	X	X	X	X				
AC-19(1)	Access Control For Mobile Devices	X	X	X							
AC-19(2)	Access Control For Mobile Devices	X	X	X	X	X	X				X
AC-19(3)	Access Control For Mobile Devices	X	X	X	X	X	X				X
AC-19(4)	Access Control For Mobile Devices	X	X	X							X
AC-20	Use Of External Information Systems	X	X	X	X	X	X				X
AC-20(1)	Use Of External Information Systems	X	X	X	X	X	X				X
AC-20(2)	Use Of External Information Systems	X	X	X							X
AC-21	User-Based Collaboration And Information Sharing										
AC-21(1)	User-Based Collaboration And Information Sharing										
AC-22	Publicly Accessible Content	X	X	X							X

ID	Title	Confidentiality			Integrity			Availability			Suggested Common
		L	M	H	L	M	H	L	M	H	
AT-1	Security Awareness And Training Policy And Procedures	X	X	X	X	X	X	X	X	X	X
AT-2	Security Awareness	X	X	X	X	X	X	X	X	X	X
AT-2(1)	Security Awareness										
AT-3	Security Training	X	X	X	X	X	X	X	X	X	
AT-3(1)	Security Training										
AT-3(2)	Security Training	X	X	X	X	X	X	X	X	X	
AT-4	Security Training Records	X	X	X	X	X	X	X	X	X	X
AT-5	Contacts With Security Groups And Associations	X	X	X	X	X	X	X	X	X	X
AU-1	Audit And Accountability Policy And Procedures	X	X	X	X	X	X	X	X	X	X
AU-2	Auditable Events	X	X	X	X	X	X				
~~AU-2(1)~~	~~Auditable Events~~ [Withdrawn]	-	-	-	-	-	-	-	-	-	
~~AU-2(2)~~	~~Auditable Events~~ [Withdrawn]	-	-	-	-	-	-	-	-	-	
AU-2(3)	Auditable Events	X	X	X	X	X	X				
AU-2(4)	Auditable Events	X	X	X	X	X	X				X
AU-3	Content Of Audit Records	X	X	X	X	X	X				
AU-3(1)	Content Of Audit Records	X	X	X	X	X	X				
AU-3(2)	Content Of Audit Records	X	X	X	X	X	X				X
AU-4	Audit Storage Capacity							X	X	X	
AU-5	Response To Audit Processing Failures							X	X	X	
AU-5(1)	Response To Audit Processing Failures							X	X	X	
AU-5(2)	Response To Audit Processing Failures								X	X	
AU-5(3)	Response To Audit Processing Failures										
AU-5(4)	Response To Audit Processing Failures										
AU-6	Audit Review, Analysis, And Reporting	X	X	X	X	X	X				X
AU-6(1)	Audit Review, Analysis, And Reporting		X	X		X	X				
~~AU-6(2)~~	~~Audit Review, Analysis, And Reporting~~ [Withdrawn]	-	-	-	-	-	-	-	-	-	
AU-6(3)	Audit Review, Analysis, And Reporting	X	X	X	X	X	X				X
AU-6(4)	Audit Review, Analysis, And Reporting										
AU-6(5)	Audit Review, Analysis, And Reporting										
AU-6(6)	Audit Review, Analysis, And Reporting										
AU-6(7)	Audit Review, Analysis, And Reporting										
~~AU-6(8)~~	~~Audit Review, Analysis, And Reporting~~ [Withdrawn]	-	-	-	-	-	-	-	-	-	
AU-6(9)	Audit Review, Analysis, And Reporting										
AU-7	Audit Reduction And Report Generation		X	X		X	X				
AU-7(1)	Audit Reduction And Report Generation		X	X		X	X				
AU-8	Time Stamps				X	X	X				

ID	Title	Confidentiality			Integrity			Availability			Suggested Common
		L	M	H	L	M	H	L	M	H	
AU-8(1)	Time Stamps				X	X	X				
AU-9	Protection Of Audit Information	X	X	X	X	X	X				
AU-9(1)	Protection Of Audit Information										
AU-9(2)	Protection Of Audit Information								X	X	
AU-9(3)	Protection Of Audit Information						X				
AU-9(4)	Protection Of Audit Information				X	X	X				X
AU-10	Non-Repudiation					X	X				
AU-10(1)	Non-Repudiation										
AU-10(2)	Non-Repudiation										
AU-10(3)	Non-Repudiation										
AU-10(4)	Non-Repudiation										
AU-10(5)	Non-Repudiation					X	X				
AU-11	Audit Record Retention							X	X	X	X
AU-12	Audit Generation	X	X	X	X	X	X	X	X	X	
AU-12(1)	Audit Generation						X				
AU-12(2)	Audit Generation										
AU-13	Monitoring For Information Disclosure										X
AU-14	Session Audit										
AU-14(1)	Session Audit										
CA-1	Security Assessment And Authorization Policies And Procedures	X	X	X	X	X	X	X	X	X	X
CA-2	Security Assessments	X	X	X	X	X	X	X	X	X	
CA-2(1)	Security Assessments	X	X	X	X	X	X	X	X	X	X
CA-2(2)	Security Assessments			X			X			X	
CA-3	Information System Connections	X	X	X	X	X	X				
CA-3(1)	Information System Connections	X	X	X							X
CA-3(2)	Information System Connections		X	X							X
~~CA-4~~	~~Security Certification~~ [Withdrawn]	-	-	-	-	-	-	-	-	-	
CA-5	Plan Of Action And Milestones	X	X	X	X	X	X	X	X	X	
CA-5(1)	Plan Of Action And Milestones										
CA-6	Security Authorization	X	X	X	X	X	X	X	X	X	
CA-7	Continuous Monitoring	X	X	X	X	X	X	X	X	X	
CA-7(1)	Continuous Monitoring	X	X	X	X	X	X	X	X	X	X
CA-7(2)	Continuous Monitoring	X	X	X	X	X	X	X	X	X	

ID	Title	Confidentiality			Integrity			Availability			Suggested Common
		L	M	H	L	M	H	L	M	H	
CM-1	Configuration Management Policy And Procedures	X	X	X	X	X	X				X
CM-2	Baseline Configuration				X	X	X				
CM-2(1)	Baseline Configuration				X	X	X				
CM-2(2)	Baseline Configuration						X				
CM-2(3)	Baseline Configuration					X	X				
CM-2(4)	Baseline Configuration										
CM-2(5)	Baseline Configuration				X	X	X				
CM-2(6)	Baseline Configuration										
CM-3	Configuration Change Control				X	X	X				X
CM-3(1)	Configuration Change Control						X				
CM-3(2)	Configuration Change Control					X	X				
CM-3(3)	Configuration Change Control										
CM-3(4)	Configuration Change Control				X	X	X				X
CM-4	Security Impact Analysis				X	X	X				
CM-4(1)	Security Impact Analysis					X	X				
CM-4(2)	Security Impact Analysis				X	X	X				
CM-5	Access Restrictions For Change				X	X	X				
CM-5(1)	Access Restrictions For Change										
CM-5(2)	Access Restrictions For Change				X	X	X				
CM-5(3)	Access Restrictions For Change						X				
CM-5(4)	Access Restrictions For Change										
CM-5(5)	Access Restrictions For Change				X	X	X				X
CM-5(6)	Access Restrictions For Change				X	X	X				X
CM-5(7)	Access Restrictions For Change										
CM-6	Configuration Settings				X	X	X				
CM-6(1)	Configuration Settings					X	X				
CM-6(2)	Configuration Settings						X				
CM-6(3)	Configuration Settings				X	X	X				
CM-6(4)	Configuration Settings										
CM-7	Least Functionality	X	X	X	X	X	X				
CM-7(1)	Least Functionality	X	X	X	X	X	X				
CM-7(2)	Least Functionality		X	X		X	X				
CM-7(3)	Least Functionality	X	X	X	X	X	X				X
CM-8	Information System Component Inventory				X	X	X				
CM-8(1)	Information System Component Inventory				X	X	X				
CM-8(2)	Information System Component Inventory						X				X

ID	Title	Confidentiality			Integrity			Availability			Suggested Common
		L	M	H	L	M	H	L	M	H	
CM-8(3)	Information System Component Inventory						X				
CM-8(4)	Information System Component Inventory				X	X	X				
CM-8(5)	Information System Component Inventory				X	X	X				
CM-8(6)	Information System Component Inventory										
CM-9	Configuration Management Plan				X	X	X				
CM-9(1)	Configuration Management Plan										
CP-1	Contingency Planning Policy And Procedures	X	X	X	X	X	X	X	X	X	X
CP-2	Contingency Plan							X	X	X	
CP-2(1)	Contingency Plan								X	X	
CP-2(2)	Contingency Plan								X	X	X
CP-2(3)	Contingency Plan								X	X	X
CP-2(4)	Contingency Plan								X	X	X
CP-2(5)	Contingency Plan									X	X
CP-2(6)	Contingency Plan									X	X
CP-3	Contingency Training							X	X	X	
CP-3(1)	Contingency Training									X	
CP-3(2)	Contingency Training										
CP-4	Contingency Plan Testing And Exercises							X	X	X	
CP-4(1)	Contingency Plan Testing And Exercises								X	X	
CP-4(2)	Contingency Plan Testing And Exercises									X	
CP-4(3)	Contingency Plan Testing And Exercises										
CP-4(4)	Contingency Plan Testing And Exercises										
~~CP-5~~	~~Contingency Plan Update~~ [Withdrawn]	-	-	-	-	-	-	-	-	-	
CP-6	Alternate Storage Site								X	X	X
CP-6(1)	Alternate Storage Site								X	X	X
CP-6(2)	Alternate Storage Site									X	X
CP-6(3)	Alternate Storage Site								X	X	X
CP-7	Alternate Processing Site								X	X	
CP-7(1)	Alternate Processing Site								X	X	X
CP-7(2)	Alternate Processing Site								X	X	X
CP-7(3)	Alternate Processing Site								X	X	
CP-7(4)	Alternate Processing Site								X	X	X
CP-7(5)	Alternate Processing Site		X	X		X	X		X	X	

ID	Title	Confidentiality			Integrity			Availability			Suggested Common
		L	M	H	L	M	H	L	M	H	
CP-8	Telecommunications Services								X	X	X
CP-8(1)	Telecommunications Services								X	X	X
CP-8(2)	Telecommunications Services								X	X	X
CP-8(3)	Telecommunications Services									X	X
CP-8(4)	Telecommunications Services									X	X
CP-9	Information System Backup	X	X	X	X	X	X	X	X	X	
CP-9(1)	Information System Backup				X	X	X	X	X	X	
CP-9(2)	Information System Backup						X			X	
CP-9(3)	Information System Backup									X	X
~~CP-9(4)~~	~~Information System Backup~~ [Withdrawn]	-	-	-	-	-	-	-	-	-	
CP-9(5)	Information System Backup								X	X	
CP-9(6)	Information System Backup										
CP-10	Information System Recovery And Reconstitution							X	X	X	
~~CP-10(1)~~	~~Information System Recovery And Reconstitution~~ [Withdrawn]	-	-	-	-	-	-	-	-	-	
CP-10(2)	Information System Recovery And Reconstitution				X	X	X	X	X	X	
CP-10(3)	Information System Recovery And Reconstitution										
CP-10(4)	Information System Recovery And Reconstitution										
CP-10(5)	Information System Recovery And Reconstitution										
CP-10(6)	Information System Recovery And Reconstitution										
IA-1	Identification And Authentication Policy And Procedures	X	X	X	X	X	X				X
IA-2	Identification And Authentication (Organizational Users)	X	X	X	X	X	X				
IA-2(1)	Identification And Authentication (Organizational Users)	X	X	X	X	X	X				
IA-2(2)	Identification And Authentication (Organizational Users)		X	X		X	X				
IA-2(3)	Identification And Authentication (Organizational Users)		X	X		X	X				
IA-2(4)	Identification And Authentication (Organizational Users)		X	X		X	X				
IA-2(5)	Identification And Authentication (Organizational Users)	X	X	X	X	X	X				
IA-2(6)	Identification And Authentication (Organizational Users)										
IA-2(7)	Identification And Authentication (Organizational Users)										
IA-2(8)	Identification And Authentication (Organizational Users)	X	X	X	X	X	X				

ID	Title	Confidentiality			Integrity			Availability			Suggested Common
		L	M	H	L	M	H	L	M	H	
IA-2(9)	Identification And Authentication (Organizational Users)		X	X		X	X				
IA-3	Device Identification And Authentication	X	X	X	X	X	X				
IA-3(1)	Device Identification And Authentication	X	X	X	X	X	X				
IA-3(2)	Device Identification And Authentication	X	X	X	X	X	X				
IA-3(3)	Device Identification And Authentication	X	X	X	X	X	X				X
IA-4	Identifier Management	X	X	X	X	X	X				X
IA-4(1)	Identifier Management										
IA-4(2)	Identifier Management										
IA-4(3)	Identifier Management										
IA-4(4)	Identifier Management	X	X	X	X	X	X				X
IA-4(5)	Identifier Management										
IA-5	Authenticator Management	X	X	X	X	X	X				X
IA-5(1)	Authenticator Management	X	X	X	X	X	X				
IA-5(2)	Authenticator Management				X	X	X				
IA-5(3)	Authenticator Management				X	X	X				X
IA-5(4)	Authenticator Management	X	X	X	X	X	X				
IA-5(5)	Authenticator Management										
IA-5(6)	Authenticator Management	X	X	X	X	X	X				X
IA-5(7)	Authenticator Management	X	X	X							
IA-5(8)	Authenticator Management	X	X	X	X	X	X				X
IA-6	Authenticator Feedback	X	X	X							
IA-7	Cryptographic Module Authentication	X	X	X	X	X	X				
IA-8	Identification And Authentication (Non-Organizational Users)	X	X	X	X	X	X				
IR-1	Incident Response Policy And Procedures	X	X	X	X	X	X	X	X	X	X
IR-2	Incident Response Training	X	X	X	X	X	X	X	X	X	
IR-2(1)	Incident Response Training			X			X			X	
IR-2(2)	Incident Response Training						X			X	
IR-3	Incident Response Testing And Exercises	X	X	X	X	X	X	X	X	X	
IR-3(1)	Incident Response Testing And Exercises										
IR-4	Incident Handling	X	X	X	X	X	X	X	X	X	X
IR-4(1)	Incident Handling	X	X	X	X	X	X	X	X	X	X
IR-4(2)	Incident Handling										
IR-4(3)	Incident Handling	X	X	X	X	X	X	X	X	X	

ID	Title	Confidentiality			Integrity			Availability			Suggested Common
		L	M	H	L	M	H	L	M	H	
IR-4(4)	Incident Handling	X	X	X	X	X	X	X	X	X	X
IR-4(5)	Incident Handling										
IR-5	Incident Monitoring	X	X	X	X	X	X	X	X	X	X
IR-5(1)	Incident Monitoring						X			X	X
IR-6	Incident Reporting	X	X	X	X	X	X	X	X	X	X
IR-6(1)	Incident Reporting	X	X	X	X	X	X	X	X	X	X
IR-6(2)	Incident Reporting	X	X	X	X	X	X	X	X	X	X
IR-7	Incident Response Assistance	X	X	X	X	X	X	X	X	X	X
IR-7(1)	Incident Response Assistance	X	X	X	X	X	X	X	X	X	X
IR-7(2)	Incident Response Assistance	X	X	X	X	X	X	X	X	X	X
IR-8	Incident Response Plan	X	X	X	X	X	X	X	X	X	X
MA-1	System Maintenance Policy And Procedures	X	X	X	X	X	X	X	X	X	X
MA-2	Controlled Maintenance	X	X	X	X	X	X	X	X	X	
MA-2(1)	Controlled Maintenance	X	X	X	X	X	X	X	X	X	
MA-2(2)	Controlled Maintenance						X			X	
MA-3	Maintenance Tools				X	X	X	X	X	X	
MA-3(1)	Maintenance Tools					X	X		X	X	X
MA-3(2)	Maintenance Tools				X	X	X	X	X	X	X
MA-3(3)	Maintenance Tools	X	X	X							
MA-3(4)	Maintenance Tools										
MA-4	Non-Local Maintenance				X	X	X				
MA-4(1)	Non-Local Maintenance										
MA-4(2)	Non-Local Maintenance				X	X	X				
MA-4(3)	Non-Local Maintenance	X	X	X	X	X	X	X	X	X	
MA-4(4)	Non-Local Maintenance										
MA-4(5)	Non-Local Maintenance				X	X	X				X
MA-4(6)	Non-Local Maintenance	X	X	X	X	X	X				
MA-4(7)	Non-Local Maintenance				X	X	X				
MA-5	Maintenance Personnel	X	X	X	X	X	X	X	X	X	
MA-5(1)	Maintenance Personnel	X	X	X	X	X	X	X	X	X	
MA-5(2)	Maintenance Personnel										X
MA-5(3)	Maintenance Personnel										X
MA-5(4)	Maintenance Personnel										
MA-6	Timely Maintenance								X	X	
MP-1	Media Protection Policy And Procedures	X	X	X	X	X	X	X	X	X	X
MP-2	Media Access	X	X	X							X
MP-2(1)	Media Access										

ID	Title	Confidentiality			Integrity			Availability			Suggested Common
		L	M	H	L	M	H	L	M	H	
MP-2(2)	Media Access		X	X		X	X				
MP-3	Media Marking	X	X	X							
MP-4	Media Storage	X	X	X							
MP-4(1)	Media Storage			X							
MP-5	Media Transport	X	X	X	X	X	X				X
~~MP-5(1)~~	~~Media Transport~~ [Withdrawn]	-	-	-	-	-	-	-	-	-	
MP-5(2)	Media Transport	X	X	X	X	X	X				X
MP-5(3)	Media Transport										X
MP-5(4)	Media Transport		X	X		X	X				
MP-6	Media Sanitization	X	X	X							X
MP-6(1)	Media Sanitization		X	X							X
MP-6(2)	Media Sanitization	X	X	X							X
MP-6(3)	Media Sanitization	X	X	X							
MP-6(4)	Media Sanitization	X	X	X							X
MP-6(5)	Media Sanitization	X	X	X							X
MP-6(6)	Media Sanitization	X	X	X							X
PE-1	Physical And Environmental Protection Policy And Procedures	X	X	X	X	X	X	X	X	X	X
PE-2	Physical Access Authorizations	X	X	X	X	X	X	X	X	X	X
PE-2(1)	Physical Access Authorizations	X	X	X	X	X	X	X	X	X	X
PE-2(2)	Physical Access Authorizations										
PE-2(3)	Physical Access Authorizations	X	X	X							X
PE-3	Physical Access Control	X	X	X	X	X	X	X	X	X	X
PE-3(1)	Physical Access Control			X			X				X
PE-3(2)	Physical Access Control	X	X	X							X
PE-3(3)	Physical Access Control	X	X	X	X	X	X				X
PE-3(4)	Physical Access Control			X			X				
PE-3(5)	Physical Access Control										
PE-3(6)	Physical Access Control						X				X
PE-4	Access Control For Transmission Medium		X	X		X	X				X
PE-5	Access Control For Output Devices	X	X	X							
PE-6	Monitoring Physical Access	X	X	X	X	X	X	X	X	X	
PE-6(1)	Monitoring Physical Access								X	X	
PE-6(2)	Monitoring Physical Access										
PE-7	Visitor Control	X	X	X	X	X	X				X
PE-7(1)	Visitor Control	X	X	X	X	X	X				X
PE-7(2)	Visitor Control										
PE-8	Access Records	X	X	X	X	X	X				X

ID	Title	Confidentiality			Integrity			Availability			Suggested Common
		L	M	H	L	M	H	L	M	H	
PE-8(1)	Access Records										
PE-8(2)	Access Records			X							
PE-9	Power Equipment And Power Cabling							X	X	X	X
PE-9(1)	Power Equipment And Power Cabling										
PE-9(2)	Power Equipment And Power Cabling								X	X	
PE-10	Emergency Shutoff							X	X	X	X
~~PE-10(1)~~	~~Emergency Shutoff~~	-	-	-	-	-	-	-	-	-	
PE-11	Emergency Power								X	X	
PE-11(1)	Emergency Power								X		X
PE-11(2)	Emergency Power									X	X
PE-12	Emergency Lighting							X	X	X	X
PE-12(1)	Emergency Lighting								X	X	X
PE-13	Fire Protection							X	X	X	X
PE-13(1)	Fire Protection									X	X
PE-13(2)	Fire Protection									X	X
PE-13(3)	Fire Protection									X	X
PE-13(4)	Fire Protection									X	X
PE-14	Temperature And Humidity Controls							X	X	X	X
PE-14(1)	Temperature And Humidity Controls								X	X	X
PE-14(2)	Temperature And Humidity Controls								X	X	X
PE-15	Water Damage Protection							X	X	X	X
PE-15(1)	Water Damage Protection										
PE-16	Delivery And Removal	X	X	X				X	X	X	X
PE-17	Alternate Work Site		X	X		X	X		X	X	
PE-18	Location Of Information System Components										X
PE-18(1)	Location Of Information System Components										X
PE-19	Information Leakage		X	X		X	X				
PE-19(1)	Information Leakage		X	X		X	X				
PL-1	Security Planning Policy And Procedures	X	X	X	X	X	X	X	X	X	X
PL-2	System Security Plan	X	X	X	X	X	X	X	X	X	
PL-2(1)	System Security Plan	X	X	X	X	X	X	X	X	X	
PL-2(2)	System Security Plan	X	X	X	X	X	X	X	X	X	
~~PL-3~~	~~System Security Plan Update~~ [Withdrawn]	-	-	-	-	-	-	-	-	-	
PL-4	Rules Of Behavior	X	X	X	X	X	X	X	X	X	
PL-4(1)	Rules Of Behavior										X
PL-5	Privacy Impact Assessment	X	X	X							

ID	Title	Confidentiality			Integrity			Availability			Suggested Common
		L	M	H	L	M	H	L	M	H	
PL-6	Security-Related Activity Planning	X	X	X	X	X	X	X	X	X	
PS-1	Personnel Security Policy And Procedures	X	X	X	X	X	X	X	X	X	X
PS-2	Position Categorization	X	X	X	X	X	X	X	X	X	X
PS-3	Personnel Screening	X	X	X	X	X	X				
PS-3(1)	Personnel Screening	X	X	X							
PS-3(2)	Personnel Screening	X	X	X							
PS-4	Personnel Termination	X	X	X	X	X	X	X	X	X	
PS-5	Personnel Transfer	X	X	X	X	X	X	X	X	X	
PS-6	Access Agreements	X	X	X	X	X	X				X
PS-6(1)	Access Agreements	X	X	X	X	X	X				X
PS-6(2)	Access Agreements	X	X	X							X
PS-7	Third-Party Personnel Security	X	X	X	X	X	X				X
PS-8	Personnel Sanctions	X	X	X	X	X	X	X	X	X	X
RA-1	Risk Assessment Policy And Procedures	X	X	X	X	X	X	X	X	X	X
RA-2	Security Categorization	X	X	X	X	X	X	X	X	X	
RA-3	Risk Assessment	X	X	X	X	X	X	X	X	X	
~~RA-4~~	~~Risk Assessment Update~~ [Withdrawn]	-	-	-	-	-	-	-	-	-	
RA-5	Vulnerability Scanning	X	X	X	X	X	X	X	X	X	
RA-5(1)	Vulnerability Scanning	X	X	X	X	X	X	X	X	X	
RA-5(2)	Vulnerability Scanning	X	X	X	X	X	X	X	X	X	
RA-5(3)	Vulnerability Scanning										X
RA-5(4)	Vulnerability Scanning	X	X	X	X	X	X	X	X	X	
RA-5(5)	Vulnerability Scanning	X	X	X	X	X	X	X	X	X	
RA-5(6)	Vulnerability Scanning										
RA-5(7)	Vulnerability Scanning	X	X	X	X	X	X	X	X	X	
RA-5(8)	Vulnerability Scanning										
RA-5(9)	Vulnerability Scanning						X				
SA-1	System And Services Acquisition Policy And Procedures	X	X	X	X	X	X				X
SA-2	Allocation Of Resources				X	X	X				
SA-3	Life Cycle Support				X	X	X				
SA-4	Acquisitions				X	X	X				
SA-4(1)	Acquisitions					X	X				X
SA-4(2)	Acquisitions						X				X
SA-4(3)	Acquisitions						X				X
SA-4(4)	Acquisitions										
SA-4(5)	Acquisitions						X				X
SA-4(6)	Acquisitions	X	X	X							X

ID	Title	Confidentiality			Integrity			Availability			Suggested Common
		L	M	H	L	M	H	L	M	H	
SA-4(7)	Acquisitions										
SA-5	Information System Documentation				X	X	X				
SA-5(1)	Information System Documentation				X	X	X				
SA-5(2)	Information System Documentation				X	X	X				
SA-5(3)	Information System Documentation					X	X				
SA-5(4)	Information System Documentation						X				
SA-5(5)	Information System Documentation										
SA-6	Software Usage Restrictions	X	X	X	X	X	X				
SA-6(1)	Software Usage Restrictions										
SA-7	User Installed Software				X	X	X				
SA-8	Security Engineering Principles				X	X	X				X
SA-9	External Information System Services				X	X	X				
SA-9(1)	External Information System Services				X	X	X				
SA-10	Developer Configuration Management				X	X	X				
SA-10(1)	Developer Configuration Management				X	X	X				
SA-10(2)	Developer Configuration Management										
SA-11	Developer Security Testing				X	X	X				
SA-11(1)	Developer Security Testing						X				
SA-11(2)	Developer Security Testing						X				
SA-11(3)	Developer Security Testing										
SA-12	Supply Chain Protection	X	X	X	X	X	X	X	X	X	X
SA-12(1)	Supply Chain Protection										
SA-12(2)	Supply Chain Protection	X	X	X	X	X	X	X	X	X	X
SA-12(3)	Supply Chain Protection										
SA-12(4)	Supply Chain Protection										
SA-12(5)	Supply Chain Protection										
SA-12(6)	Supply Chain Protection										
SA-12(7)	Supply Chain Protection										
SA-13	Trustworthiness										
SA-14	Critical Information System Components										
SA-14(1)	Critical Information System Components										

ID	Title	Confidentiality			Integrity			Availability			Suggested Common
		L	M	H	L	M	H	L	M	H	
SC-1	System And Communications Protection Policy And Procedures	X	X	X	X	X	X	X	X	X	X
SC-2	Application Partitioning	X	X	X	X	X	X				
SC-2(1)	Application Partitioning	X	X	X	X	X	X				
SC-3	Security Function Isolation						X				
SC-3(1)	Security Function Isolation										
SC-3(2)	Security Function Isolation										
SC-3(3)	Security Function Isolation										
SC-3(4)	Security Function Isolation										
SC-3(5)	Security Function Isolation										
SC-4	Information In Shared Resources	X	X	X							
SC-4(1)	Information In Shared Resources										
SC-5	Denial Of Service Protection							X	X	X	
SC-5(1)	Denial Of Service Protection							X	X	X	
SC-5(2)	Denial Of Service Protection								X	X	
SC-6	Resource Priority									X	
SC-7	Boundary Protection	X	X	X	X	X	X				
SC-7(1)	Boundary Protection	X	X	X	X	X	X				
SC-7(2)	Boundary Protection	X	X	X	X	X	X				
SC-7(3)	Boundary Protection	X	X	X	X	X	X				
SC-7(4)	Boundary Protection	X	X	X	X	X	X				
SC-7(5)	Boundary Protection	X	X	X	X	X	X				
SC-7(6)	Boundary Protection										
SC-7(7)	Boundary Protection	X	X	X	X	X	X				
SC-7(8)	Boundary Protection	X	X	X	X	X	X				
SC-7(9)	Boundary Protection										
SC-7(10)	Boundary Protection										
SC-7(11)	Boundary Protection				X	X	X				
SC-7(12)	Boundary Protection	X	X	X	X	X	X	X	X	X	
SC-7(13)	Boundary Protection	X	X	X	X	X	X				
SC-7(14)	Boundary Protection	X	X	X	X	X	X				
SC-7(15)	Boundary Protection										
SC-7(16)	Boundary Protection										
SC-7(17)	Boundary Protection										
SC-	Boundary Protection	X	X	X	X	X	X	X	X	X	

ID	Title	Confidentiality			Integrity			Availability			Suggested Common
		L	M	H	L	M	H	L	M	H	
7(18)											
SC-8	Transmission Integrity				X	X	X				
SC-8(1)	Transmission Integrity					X	X				
SC-8(2)	Transmission Integrity						X				
SC-9	Transmission Confidentiality	X	X	X							
SC-9(1)	Transmission Confidentiality	X	X	X							
SC-9(2)	Transmission Confidentiality		X	X							
SC-10	Network Disconnect	X	X	X	X	X	X				
SC-11	Trusted Path				X	X	X				
SC-12	Cryptographic Key Establishment And Management	X	X	X	X	X	X				X
SC-12(1)	Cryptographic Key Establishment And Management							X	X	X	
SC-12(2)	Cryptographic Key Establishment And Management										
SC-12(3)	Cryptographic Key Establishment And Management										
SC-12(4)	Cryptographic Key Establishment And Management										
SC-12(5)	Cryptographic Key Establishment And Management										
SC-13	Use Of Cryptography	X	X	X	X	X	X				
SC-13(1)	Use Of Cryptography										
SC-13(2)	Use Of Cryptography										
SC-13(3)	Use Of Cryptography										
SC-13(4)	Use Of Cryptography					X	X				
SC-14	Public Access Protections				X	X	X	X	X	X	
SC-15	Collaborative Computing Devices	X	X	X							
SC-15(1)	Collaborative Computing Devices	X	X	X							
SC-15(2)	Collaborative Computing Devices	X	X	X	X	X	X				
SC-15(3)	Collaborative Computing Devices	X	X	X	X	X	X				
SC-16	Transmission Of Security Attributes										
SC-16(1)	Transmission Of Security Attributes										
SC-17	Public Key Infrastructure Certificates	X	X	X	X	X	X				X
SC-18	Mobile Code				X	X	X				
SC-18(1)	Mobile Code				X	X	X				

ID	Title	Confidentiality			Integrity			Availability			Suggested Common
		L	M	H	L	M	H	L	M	H	
SC-18(2)	Mobile Code				X	X	X				X
SC-18(3)	Mobile Code				X	X	X				
SC-18(4)	Mobile Code				X	X	X				
SC-19	Voice Over Internet Protocol	X	X	X	X	X	X				
SC-20	Secure Name / Address Resolution Service (Authoritative Source)				X	X	X				
SC-20(1)	Secure Name / Address Resolution Service (Authoritative Source)				X	X	X				
SC-21	Secure Name / Address Resolution Service (Recursive Or Caching Resolver)				X	X	X				
SC-21(1)	Secure Name / Address Resolution Service (Recursive Or Caching Resolver)				X	X	X				
SC-22	Architecture And Provisioning For Name / Address Resolution Service	X	X	X	X	X	X	X	X	X	
SC-23	Session Authenticity				X	X	X				
SC-23(1)	Session Authenticity				X	X	X				
SC-23(2)	Session Authenticity				X	X	X				
SC-23(3)	Session Authenticity				X	X	X				
SC-23(4)	Session Authenticity				X	X	X				
SC-24	Fail In Known State	X	X	X	X	X	X				
SC-25	Thin Nodes										
SC-26	Honeypots										
SC-26(1)	Honeypots										
SC-27	Operating System-Independent Applications										
SC-28	Protection Of Information At Rest	X	X	X	X	X	X				
SC-28(1)	Protection Of Information At Rest			X			X				
SC-29	Heterogeneity										
SC-30	Virtualization Techniques										
SC-30(1)	Virtualization Techniques										
SC-30(2)	Virtualization Techniques										
SC-31	Covert Channel Analysis										
SC-31(1)	Covert Channel Analysis										

ID	Title	Confidentiality			Integrity			Availability			Suggested Common
		L	M	H	L	M	H	L	M	H	
SC-32	Information System Partitioning		X	X		X	X				
SC-33	Transmission Preparation Integrity						X				
SC-34	Non-modifiable executable programs										
SC-34(1)	Non-modifiable executable programs										
SC-34(2)	Non-modifiable executable programs										
SI-1	System And Information Integrity Policy And Procedures	X	X	X	X	X	X	X	X	X	X
SI-2	Flaw Remediation				X	X	X				
SI-2(1)	Flaw Remediation										
SI-2(2)	Flaw Remediation					X	X				
SI-2(3)	Flaw Remediation				X	X	X				X
SI-2(4)	Flaw Remediation				X	X	X				
SI-3	Malicious Code Protection				X	X	X				
SI-3(1)	Malicious Code Protection				X	X	X				X
SI-3(2)	Malicious Code Protection				X	X	X				
SI-3(3)	Malicious Code Protection				X	X	X				
SI-3(4)	Malicious Code Protection										
SI-3(5)	Malicious Code Protection										
SI-3(6)	Malicious Code Protection										
SI-4	Information System Monitoring				X	X	X				
SI-4(1)	Information System Monitoring				X	X	X				
SI-4(2)	Information System Monitoring				X	X	X				
SI-4(3)	Information System Monitoring										
SI-4(4)	Information System Monitoring	X	X	X	X	X	X				
SI-4(5)	Information System Monitoring				X	X	X				
SI-4(6)	Information System Monitoring				X	X	X				
SI-4(7)	Information System Monitoring				X	X	X	X	X	X	
SI-4(8)	Information System Monitoring	X	X	X	X	X	X	X	X	X	
SI-4(9)	Information System Monitoring				X	X	X				
SI-4(10)	Information System Monitoring										
SI-4(11)	Information System Monitoring	X	X	X							
SI-4(12)	Information System Monitoring	X	X	X	X	X	X				
SI-4(13)	Information System Monitoring										
SI-4(14)	Information System Monitoring	X	X	X	X	X	X				
SI-4(15)	Information System Monitoring	X	X	X	X	X	X				
SI-4(16)	Information System Monitoring				X	X	X				
SI-4(17)	Information System Monitoring	X	X	X	X	X	X				X
SI-5	Security Alerts, Advisories, And				X	X	X				X

ID	Title	Confidentiality			Integrity			Availability			Suggested Common
		L	M	H	L	M	H	L	M	H	
	Directives										
SI-5(1)	Security Alerts, Advisories, And Directives				X	X	X				X
SI-6	Security Functionality Verification				X	X	X				
SI-6(1)	Security Functionality Verification				X	X	X				
SI-6(2)	Security Functionality Verification										
SI-6(3)	Security Functionality Verification				X	X	X				X
SI-7	Software And Information Integrity						X				
SI-7(1)	Software And Information Integrity						X				
SI-7(2)	Software And Information Integrity						X				
SI-7(3)	Software And Information Integrity										
SI-7(4)	Software And Information Integrity										
SI-8	Spam Protection				X	X	X	X	X	X	
SI-8(1)	Spam Protection				X	X	X	X	X	X	X
SI-8(2)	Spam Protection				X	X	X	X	X	X	
SI-9	Information Input Restrictions				X	X	X				
SI-10	Information Input Validation					X	X				
SI-11	Error Handling				X	X	X				
SI-12	Information Output Handling And Retention	X	X	X	X	X	X				
SI-13	Predictable Failure Prevention									X	
SI-13(1)	Predictable Failure Prevention										
SI-13(2)	Predictable Failure Prevention										
SI-13(3)	Predictable Failure Prevention										
SI-13(4)	Predictable Failure Prevention										
PM-1	Information Security Program Plan	X	X	X	X	X	X	X	X	X	X
PM-2	Senior Information Security Officer	X	X	X	X	X	X	X	X	X	X
PM-3	Information Security Resources	X	X	X	X	X	X	X	X	X	X
PM-4	Plan of Action and Milestones Process	X	X	X	X	X	X	X	X	X	X
PM-5	Information System Inventory	X	X	X	X	X	X	X	X	X	X
PM-6	Information Security Measures of Performance	X	X	X	X	X	X	X	X	X	X
PM-7	Enterprise Architecture	X	X	X	X	X	X	X	X	X	X
PM-8	Critical Infrastructure Plan	X	X	X	X	X	X	X	X	X	X
PM-9	Risk Management Strategy	X	X	X	X	X	X	X	X	X	X
PM-10	Security Authorization Process	X	X	X	X	X	X	X	X	X	X
PM-11	Mission/Business Process Definition	X	X	X	X	X	X	X	X	X	X

Table D-2: Control Relationships to Security Objectives

ID	Title	C	I	A
AC-1	Access Control Policy And Procedures	X	X	X
AC-2	Account Management	X	X	
AC-2(1)	Account Management	X	X	
AC-2(2)	Account Management	X	X	
AC-2(3)	Account Management	X	X	
AC-2(4)	Account Management	X	X	
AC-2(5)	Account Management	X	X	
AC-2(6)	Account Management	X	X	
AC-2(7)	Account Management	X	X	
AC-3	Access Enforcement	X	X	
~~AC-3(1)~~	~~Access Enforcement~~ [Withdrawn]	-	-	-
AC-3(2)	Access Enforcement	X	X	
AC-3(3)	Access Enforcement	X	X	
AC-3(4)	Access Enforcement	X	X	
AC-3(5)	Access Enforcement	X	X	
AC-3(6)	Access Enforcement	X		
AC-4	Information Flow Enforcement	X	X	
AC-4(1)	Information Flow Enforcement	X	X	
AC-4(2)	Information Flow Enforcement	X	X	
AC-4(3)	Information Flow Enforcement	X	X	
AC-4(4)	Information Flow Enforcement	X	X	
AC-4(5)	Information Flow Enforcement	X	X	
AC-4(6)	Information Flow Enforcement	X	X	
AC-4(7)	Information Flow Enforcement	X	X	
AC-4(8)	Information Flow Enforcement	X	X	
AC-4(9)	Information Flow Enforcement	X	X	
AC-4(10)	Information Flow Enforcement	X	X	
AC-4(11)	Information Flow Enforcement	X	X	
AC-4(12)	Information Flow Enforcement	X	X	
AC-4(13)	Information Flow Enforcement	X	X	
AC-4(14)	Information Flow Enforcement	X	X	
AC-4(15)	Information Flow Enforcement	X	X	
AC-4(16)	Information Flow Enforcement	X	X	
AC-4(17)	Information Flow Enforcement	X	X	
AC-5	Separation Of Duties	X	X	
AC-6	Least Privilege	X	X	
AC-6(1)	Least Privilege	X	X	
AC-6(2)	Least Privilege	X	X	
AC-6(3)	Least Privilege	X	X	
AC-6(4)	Least Privilege	X	X	
AC-6(5)	Least Privilege	X	X	
AC-6(6)	Least Privilege	X	X	
AC-7	Unsuccessful Login Attempts	X	X	X
AC-7(1)	Unsuccessful Login Attempts	X	X	
AC-7(2)	Unsuccessful Login Attempts	X		
AC-8	System Use Notification	X	X	
AC-9	Previous Logon (Access) Notification		X	
AC-9(1)	Previous Logon (Access) Notification		X	
AC-9(2)	Previous Logon (Access) Notification		X	

ID	Title	C	I	A
AC-9(3)	Previous Logon (Access) Notification		X	
AC-10	Concurrent Session Control		X	X
AC-11	Session Lock	X	X	
AC-11(1)	Session Lock	X		
~~AC-12~~	~~Session Termination~~ [Withdrawn]	-	-	-
~~AC-13~~	~~Supervision And Review — Access Control~~ [Withdrawn]	-	-	-
AC-14	Permitted Actions Without Identification Or Authentication	X	X	
AC-14(1)	Permitted Actions Without Identification Or Authentication	X	X	
~~AC-15~~	~~Automated Marking~~ [Withdrawn]	-	-	-
AC-16	Security Attributes	X	X	
AC-16(1)	Security Attributes	X	X	
AC-16(2)	Security Attributes		X	
AC-16(3)	Security Attributes		X	
AC-16(4)	Security Attributes	X	X	
AC-16(5)	Security Attributes	X		
AC-17	Remote Access	X	X	
AC-17(1)	Remote Access	X	X	
AC-17(2)	Remote Access	X	X	
AC-17(3)	Remote Access	X	X	
AC-17(4)	Remote Access	X	X	
AC-17(5)	Remote Access	X	X	
AC-17(6)	Remote Access	X		
AC-17(7)	Remote Access	X	X	
AC-17(8)	Remote Access	X	X	
AC-18	Wireless Access Restrictions	X	X	
AC-18(1)	Wireless Access Restrictions	X	X	
AC-18(2)	Wireless Access Restrictions	X	X	
AC-18(3)	Wireless Access Restrictions	X	X	
AC-18(4)	Wireless Access Restrictions	X	X	
AC-18(5)	Wireless Access Restrictions	X	X	
AC-19	Access Control For Mobile Devices	X	X	
AC-19(1)	Access Control For Mobile Devices	X		
AC-19(2)	Access Control For Mobile Devices	X	X	
AC-19(3)	Access Control For Mobile Devices	X	X	
AC-19(4)	Access Control For Mobile Devices	X		
AC-20	Use Of External Information Systems	X	X	
AC-20(1)	Use Of External Information Systems	X	X	
AC-20(2)	Use Of External Information Systems	X		
AC-21	User-Based Collaboration And Information Sharing	X		
AC-21(1)	User-Based Collaboration And Information Sharing	X		
AC-22	Publicly Accessible Content	X		
AT-1	Security Awareness And Training Policy And Procedures	X	X	X
AT-2	Security Awareness	X	X	X
AT-2(1)	Security Awareness	X	X	X
AT-3	Security Training	X	X	X
AT-3(1)	Security Training			X
AT-3(2)	Security Training	X	X	X
AT-4	Security Training Records	X	X	X
AT-5	Contacts With Security Groups And Associations	X	X	X
AU-1	Audit And Accountability Policy And Procedures	X	X	X
AU-2	Auditable Events	X	X	

ID	Title	C	I	A
~~AU-2(1)~~	~~Auditable Events~~ [Withdrawn]	-	-	-
~~AU-2(2)~~	~~Auditable Events~~ [Withdrawn]	-	-	-
AU-2(3)	Auditable Events	X	X	
AU-2(4)	Auditable Events	X	X	
AU-3	Content Of Audit Records	X	X	
AU-3(1)	Content Of Audit Records	X	X	
AU-3(2)	Content Of Audit Records	X	X	
AU-4	Audit Storage Capacity			X
AU-5	Response To Audit Processing Failures			X
AU-5(1)	Response To Audit Processing Failures			X
AU-5(2)	Response To Audit Processing Failures			X
AU-5(3)	Response To Audit Processing Failures			X
AU-5(4)	Response To Audit Processing Failures	X	X	
AU-6	Audit Review, Analysis, And Reporting	X	X	
AU-6(1)	Audit Review, Analysis, And Reporting	X	X	
~~AU-6(2)~~	~~Audit Review, Analysis, And Reporting~~ [Withdrawn]	-	-	-
AU-6(3)	Audit Review, Analysis, And Reporting	X	X	
AU-6(4)	Audit Review, Analysis, And Reporting	X	X	
AU-6(5)	Audit Review, Analysis, And Reporting	X	X	
AU-6(6)	Audit Review, Analysis, And Reporting	X	X	
AU-6(7)	Audit Review, Analysis, And Reporting	X	X	
~~AU-6(8)~~	~~Audit Review, Analysis, And Reporting~~ [Withdrawn]	-	-	-
AU-6(9)	Audit Review, Analysis, And Reporting	X	X	
AU-7	Audit Reduction And Report Generation	X	X	
AU-7(1)	Audit Reduction And Report Generation	X	X	
AU-8	Time Stamps		X	
AU-8(1)	Time Stamps		X	
AU-9	Protection Of Audit Information	X	X	
AU-9(1)	Protection Of Audit Information		X	
AU-9(2)	Protection Of Audit Information			X
AU-9(3)	Protection Of Audit Information		X	
AU-9(4)	Protection Of Audit Information		X	
AU-10	Non-Repudiation		X	
AU-10(1)	Non-Repudiation		X	
AU-10(2)	Non-Repudiation		X	
AU-10(3)	Non-Repudiation		X	
AU-10(4)	Non-Repudiation		X	
AU-10(5)	Non-Repudiation		X	
AU-11	Audit Record Retention			X
AU-12	Audit Generation	X	X	X
AU-12(1)	Audit Generation		X	
AU-12(2)	Audit Generation		X	
AU-13	Monitoring For Information Disclosure	X		
AU-14	Session Audit			X
AU-14(1)	Session Audit			X
CA-1	Security Assessment And Authorization Policies And Procedures	X	X	X
CA-2	Security Assessments	X	X	X
CA-2(1)	Security Assessments	X	X	X
CA-2(2)	Security Assessments	X	X	X
CA-3	Information System Connections	X	X	
CA-3(1)	Information System Connections	X		

ID	Title	C	I	A
CA-3(2)	Information System Connections	X		
~~CA-4~~	~~Security Certification~~ [Withdrawn]	-	-	-
CA-5	Plan Of Action And Milestones	X	X	X
CA-5(1)	Plan Of Action And Milestones	X	X	X
CA-6	Security Authorization	X	X	X
CA-7	Continuous Monitoring	X	X	X
CA-7(1)	Continuous Monitoring	X	X	X
CA-7(2)	Continuous Monitoring	X	X	X
CM-1	Configuration Management Policy And Procedures	X	X	
CM-2	Baseline Configuration		X	
CM-2(1)	Baseline Configuration		X	
CM-2(2)	Baseline Configuration		X	
CM-2(3)	Baseline Configuration		X	
CM-2(4)	Baseline Configuration		X	
CM-2(5)	Baseline Configuration		X	
CM-2(6)	Baseline Configuration		X	
CM-3	Configuration Change Control		X	
CM-3(1)	Configuration Change Control		X	
CM-3(2)	Configuration Change Control		X	
CM-3(3)	Configuration Change Control		X	
CM-3(4)	Configuration Change Control		X	
CM-4	Security Impact Analysis		X	
CM-4(1)	Security Impact Analysis		X	
CM-4(2)	Security Impact Analysis		X	
CM-5	Access Restrictions For Change		X	
CM-5(1)	Access Restrictions For Change		X	
CM-5(2)	Access Restrictions For Change		X	
CM-5(3)	Access Restrictions For Change		X	
CM-5(4)	Access Restrictions For Change		X	
CM-5(5)	Access Restrictions For Change		X	
CM-5(6)	Access Restrictions For Change		X	
CM-5(7)	Access Restrictions For Change		X	
CM-6	Configuration Settings		X	
CM-6(1)	Configuration Settings		X	
CM-6(2)	Configuration Settings		X	
CM-6(3)	Configuration Settings		X	
CM-6(4)	Configuration Settings		X	
CM-7	Least Functionality	X	X	
CM-7(1)	Least Functionality	X	X	
CM-7(2)	Least Functionality	X	X	
CM-7(3)	Least Functionality	X	X	
CM-8	Information System Component Inventory		X	
CM-8(1)	Information System Component Inventory		X	
CM-8(2)	Information System Component Inventory		X	
CM-8(3)	Information System Component Inventory		X	
CM-8(4)	Information System Component Inventory		X	
CM-8(5)	Information System Component Inventory		X	
CM-8(6)	Information System Component Inventory		X	
CM-9	Configuration Management Plan		X	
CM-9(1)	Configuration Management Plan		X	
CP-1	Contingency Planning Policy And Procedures	X	X	X

ID	Title	C	I	A
CP-2	Contingency Plan			X
CP-2(1)	Contingency Plan			X
CP-2(2)	Contingency Plan			X
CP-2(3)	Contingency Plan			X
CP-2(4)	Contingency Plan			X
CP-2(5)	Contingency Plan			X
CP-2(6)	Contingency Plan			X
CP-3	Contingency Training			X
CP-3(1)	Contingency Training			X
CP-3(2)	Contingency Training			X
CP-4	Contingency Plan Testing And Exercises			X
CP-4(1)	Contingency Plan Testing And Exercises			X
CP-4(2)	Contingency Plan Testing And Exercises			X
CP-4(3)	Contingency Plan Testing And Exercises			X
CP-4(4)	Contingency Plan Testing And Exercises			X
~~CP-5~~	~~Contingency Plan Update~~ [Withdrawn]	-	-	-
CP-6	Alternate Storage Site			X
CP-6(1)	Alternate Storage Site			X
CP-6(2)	Alternate Storage Site			X
CP-6(3)	Alternate Storage Site			X
CP-7	Alternate Processing Site			X
CP-7(1)	Alternate Processing Site			X
CP-7(2)	Alternate Processing Site			X
CP-7(3)	Alternate Processing Site			X
CP-7(4)	Alternate Processing Site			X
CP-7(5)	Alternate Processing Site	X	X	X
CP-8	Telecommunications Services			X
CP-8(1)	Telecommunications Services			X
CP-8(2)	Telecommunications Services			X
CP-8(3)	Telecommunications Services			X
CP-8(4)	Telecommunications Services			X
CP-9	Information System Backup	X	X	X
CP-9(1)	Information System Backup		X	X
CP-9(2)	Information System Backup		X	X
CP-9(3)	Information System Backup			X
~~CP-9(4)~~	~~Information System Backup~~ [Withdrawn]	-	-	-
CP-9(5)	Information System Backup			X
CP-9(6)	Information System Backup			X
CP-10	Information System Recovery And Reconstitution			X
~~CP-10(1)~~	~~Information System Recovery And Reconstitution~~ [Withdrawn]	-	-	-
CP-10(2)	Information System Recovery And Reconstitution		X	X
CP-10(3)	Information System Recovery And Reconstitution			X
CP-10(4)	Information System Recovery And Reconstitution		X	X
CP-10(5)	Information System Recovery And Reconstitution			X
CP-10(6)	Information System Recovery And Reconstitution		X	X
IA-1	Identification And Authentication Policy And Procedures	X	X	
IA-2	Identification And Authentication (Organizational Users)	X	X	
IA-2(1)	Identification And Authentication (Organizational Users)	X	X	
IA-2(2)	Identification And Authentication (Organizational Users)	X	X	
IA-2(3)	Identification And Authentication (Organizational Users)	X	X	
IA-2(4)	Identification And Authentication (Organizational Users)	X	X	

ID	Title	C	I	A
IA-2(5)	Identification And Authentication (Organizational Users)	X	X	
IA-2(6)	Identification And Authentication (Organizational Users)			
IA-2(7)	Identification And Authentication (Organizational Users)	X	X	
IA-2(8)	Identification And Authentication (Organizational Users)	X	X	
IA-2(9)	Identification And Authentication (Organizational Users)	X	X	
IA-3	Device Identification And Authentication	X	X	
IA-3(1)	Device Identification And Authentication	X	X	
IA-3(2)	Device Identification And Authentication	X	X	
IA-3(3)	Device Identification And Authentication	X	X	
IA-4	Identifier Management	X	X	
IA-4(1)	Identifier Management	X	X	
IA-4(2)	Identifier Management		X	
IA-4(3)	Identifier Management		X	
IA-4(4)	Identifier Management	X	X	
IA-4(5)	Identifier Management	X	X	
IA-5	Authenticator Management	X	X	
IA-5(1)	Authenticator Management	X	X	
IA-5(2)	Authenticator Management		X	
IA-5(3)	Authenticator Management		X	
IA-5(4)	Authenticator Management	X	X	
IA-5(5)	Authenticator Management	X	X	
IA-5(6)	Authenticator Management	X	X	
IA-5(7)	Authenticator Management	X		
IA-5(8)	Authenticator Management	X	X	
IA-6	Authenticator Feedback	X		
IA-7	Cryptographic Module Authentication	X	X	
IA-8	Identification And Authentication (Non-Organizational Users)	X	X	
IR-1	Incident Response Policy And Procedures	X	X	X
IR-2	Incident Response Training	X	X	X
IR-2(1)	Incident Response Training	X	X	X
IR-2(2)	Incident Response Training		X	X
IR-3	Incident Response Testing And Exercises	X	X	X
IR-3(1)	Incident Response Testing And Exercises	X	X	X
IR-4	Incident Handling	X	X	X
IR-4(1)	Incident Handling	X	X	X
IR-4(2)	Incident Handling	X	X	X
IR-4(3)	Incident Handling	X	X	X
IR-4(4)	Incident Handling	X	X	X
IR-4(5)	Incident Handling	X	X	
IR-5	Incident Monitoring	X	X	X
IR-5(1)	Incident Monitoring	X	X	X
IR-6	Incident Reporting	X	X	X
IR-6(1)	Incident Reporting	X	X	X
IR-6(2)	Incident Reporting	X	X	X
IR-7	Incident Response Assistance	X	X	X
IR-7(1)	Incident Response Assistance	X	X	X
IR-7(2)	Incident Response Assistance	X	X	X
IR-8	Incident Response Plan	X	X	X
MA-1	System Maintenance Policy And Procedures	X	X	X
MA-2	Controlled Maintenance	X	X	X
MA-2(1)	Controlled Maintenance	X	X	X

ID	Title	C	I	A
MA-2(2)	Controlled Maintenance	X	X	X
MA-3	Maintenance Tools		X	X
MA-3(1)	Maintenance Tools		X	X
MA-3(2)	Maintenance Tools		X	X
MA-3(3)	Maintenance Tools	X		
MA-3(4)	Maintenance Tools		X	
MA-4	Non-Local Maintenance		X	
MA-4(1)	Non-Local Maintenance		X	
MA-4(2)	Non-Local Maintenance		X	
MA-4(3)	Non-Local Maintenance	X	X	X
MA-4(4)	Non-Local Maintenance	X	X	
MA-4(5)	Non-Local Maintenance		X	
MA-4(6)	Non-Local Maintenance	X	X	
MA-4(7)	Non-Local Maintenance		X	
MA-5	Maintenance Personnel	X	X	X
MA-5(1)	Maintenance Personnel	X	X	X
MA-5(2)	Maintenance Personnel	X	X	X
MA-5(3)	Maintenance Personnel	X	X	X
MA-5(4)	Maintenance Personnel	X	X	X
MA-6	Timely Maintenance			X
MP-1	Media Protection Policy And Procedures	X	X	X
MP-2	Media Access	X		
MP-2(1)	Media Access	X	X	
MP-2(2)	Media Access	X	X	
MP-3	Media Marking	X		
MP-4	Media Storage	X		
MP-4(1)	Media Storage	X		
MP-5	Media Transport	X	X	
~~MP-5(1)~~	~~Media Transport~~ [Withdrawn]	-	-	-
MP-5(2)	Media Transport	X	X	
MP-5(3)	Media Transport	X	X	
MP-5(4)	Media Transport	X	X	
MP-6	Media Sanitization	X		
MP-6(1)	Media Sanitization	X		
MP-6(2)	Media Sanitization	X		
MP-6(3)	Media Sanitization	X		
MP-6(4)	Media Sanitization	X		
MP-6(5)	Media Sanitization	X		
MP-6(6)	Media Sanitization	X		
PE-1	Physical And Environmental Protection Policy And Procedures	X	X	X
PE-2	Physical Access Authorizations	X	X	X
PE-2(1)	Physical Access Authorizations	X	X	X
PE-2(2)	Physical Access Authorizations	X	X	
PE-2(3)	Physical Access Authorizations	X		
PE-3	Physical Access Control	X	X	X
PE-3(1)	Physical Access Control	X	X	
PE-3(2)	Physical Access Control	X		
PE-3(3)	Physical Access Control	X	X	
PE-3(4)	Physical Access Control	X	X	
PE-3(5)	Physical Access Control		X	
PE-3(6)	Physical Access Control		X	

ID	Title	C	I	A
PE-4	Access Control For Transmission Medium	X	X	
PE-5	Access Control For Output Devices	X		
PE-6	Monitoring Physical Access	X	X	X
PE-6(1)	Monitoring Physical Access			X
PE-6(2)	Monitoring Physical Access	X	X	X
PE-7	Visitor Control	X	X	
PE-7(1)	Visitor Control	X	X	
PE-7(2)	Visitor Control	X	X	
PE-8	Access Records	X	X	
PE-8(1)	Access Records	X	X	
PE-8(2)	Access Records	X	X	
PE-9	Power Equipment And Power Cabling			X
PE-9(1)	Power Equipment And Power Cabling			X
PE-9(2)	Power Equipment And Power Cabling			X
PE-10	Emergency Shutoff			X
~~PE-10(1)~~	~~Emergency Shutoff~~ [Withdrawn]	-	-	-
PE-11	Emergency Power			X
PE-11(1)	Emergency Power			X
PE-11(2)	Emergency Power			X
PE-12	Emergency Lighting			X
PE-12(1)	Emergency Lighting			X
PE-13	Fire Protection			X
PE-13(1)	Fire Protection			X
PE-13(2)	Fire Protection			X
PE-13(3)	Fire Protection			X
PE-13(4)	Fire Protection			X
PE-14	Temperature And Humidity Controls			X
PE-14(1)	Temperature And Humidity Controls			X
PE-14(2)	Temperature And Humidity Controls			X
PE-15	Water Damage Protection			X
PE-15(1)	Water Damage Protection			X
PE-16	Delivery And Removal	X		X
PE-17	Alternate Work Site	X	X	X
PE-18	Location Of Information System Components			X
PE-18(1)	Location Of Information System Components			X
PE-19	Information Leakage	X	X	
PE-19(1)	Information Leakage	X	X	
PL-1	Security Planning Policy And Procedures	X	X	X
PL-2	System Security Plan	X	X	X
PL-2(1)	System Security Plan	X	X	X
PL-2(2)	System Security Plan	X	X	X
~~PL-3~~	~~System Security Plan Update~~ [Withdrawn]	-	-	-
PL-4	Rules Of Behavior	X	X	X
PL-4(1)	Rules Of Behavior	X		
PL-5	Privacy Impact Assessment	X		
PL-6	Security-Related Activity Planning	X	X	X
PS-1	Personnel Security Policy And Procedures	X	X	X
PS-2	Position Categorization	X	X	X
PS-3	Personnel Screening	X	X	
PS-3(1)	Personnel Screening	X		
PS-3(2)	Personnel Screening	X		

ID	Title	C	I	A
PS-4	Personnel Termination	X	X	X
PS-5	Personnel Transfer	X	X	X
PS-6	Access Agreements	X	X	
PS-6(1)	Access Agreements	X	X	
PS-6(2)	Access Agreements	X		
PS-7	Third-Party Personnel Security	X	X	
PS-8	Personnel Sanctions	X	X	X
RA-1	Risk Assessment Policy And Procedures	X	X	X
RA-2	Security Categorization	X	X	X
RA-3	Risk Assessment	X	X	X
~~RA-4~~	~~Risk Assessment Update~~ [Withdrawn]	-	-	-
RA-5	Vulnerability Scanning	X	X	X
RA-5(1)	Vulnerability Scanning	X	X	X
RA-5(2)	Vulnerability Scanning	X	X	X
RA-5(3)	Vulnerability Scanning	X	X	X
RA-5(4)	Vulnerability Scanning	X	X	X
RA-5(5)	Vulnerability Scanning	X	X	X
RA-5(6)	Vulnerability Scanning	X	X	X
RA-5(7)	Vulnerability Scanning	X	X	X
RA-5(8)	Vulnerability Scanning	X	X	X
RA-5(9)	Vulnerability Scanning	X	X	X
SA-1	System And Services Acquisition Policy And Procedures	X	X	
SA-2	Allocation Of Resources		X	
SA-3	Life Cycle Support		X	
SA-4	Acquisitions		X	
SA-4(1)	Acquisitions		X	
SA-4(2)	Acquisitions		X	
SA-4(3)	Acquisitions		X	
SA-4(4)	Acquisitions		X	
SA-4(5)	Acquisitions		X	
SA-4(6)	Acquisitions	X		
SA-4(7)	Acquisitions		X	
SA-5	Information System Documentation		X	
SA-5(1)	Information System Documentation		X	
SA-5(2)	Information System Documentation		X	
SA-5(3)	Information System Documentation		X	
SA-5(4)	Information System Documentation		X	
SA-5(5)	Information System Documentation		X	
SA-6	Software Usage Restrictions	X	X	
SA-6(1)	Software Usage Restrictions	X	X	
SA-7	User Installed Software		X	
SA-8	Security Engineering Principles		X	
SA-9	External Information System Services		X	
SA-9(1)	External Information System Services		X	
SA-10	Developer Configuration Management		X	
SA-10(1)	Developer Configuration Management		X	
SA-10(2)	Developer Configuration Management		X	
SA-11	Developer Security Testing		X	
SA-11(1)	Developer Security Testing		X	
SA-11(2)	Developer Security Testing		X	
SA-11(3)	Developer Security Testing		X	

ID	Title	C	I	A
SA-12	Supply Chain Protection	X	X	X
SA-12(1)	Supply Chain Protection	X	X	X
SA-12(2)	Supply Chain Protection	X	X	X
SA-12(3)	Supply Chain Protection	X	X	X
SA-12(4)	Supply Chain Protection	X	X	X
SA-12(5)	Supply Chain Protection	X	X	X
SA-12(6)	Supply Chain Protection	X	X	X
SA-12(7)	Supply Chain Protection	X	X	X
SA-13	Trustworthiness		X	
SA-14	Critical Information System Components		X	
SA-14(1)	Critical Information System Components		X	
SC-1	System And Communications Protection Policy And Procedures	X	X	X
SC-2	Application Partitioning	X	X	
SC-2(1)	Application Partitioning	X	X	
SC-3	Security Function Isolation	X	X	
SC-3(1)	Security Function Isolation	X	X	
SC-3(2)	Security Function Isolation	X	X	
SC-3(3)	Security Function Isolation	X	X	
SC-3(4)	Security Function Isolation	X	X	
SC-3(5)	Security Function Isolation	X	X	
SC-4	Information In Shared Resources	X		
SC-4(1)	Information In Shared Resources	X		
SC-5	Denial Of Service Protection			X
SC-5(1)	Denial Of Service Protection			X
SC-5(2)	Denial Of Service Protection			X
SC-6	Resource Priority			X
SC-7	Boundary Protection	X	X	
SC-7(1)	Boundary Protection	X	X	
SC-7(2)	Boundary Protection	X	X	
SC-7(3)	Boundary Protection	X	X	
SC-7(4)	Boundary Protection	X	X	
SC-7(5)	Boundary Protection	X	X	
SC-7(6)	Boundary Protection	X		
SC-7(7)	Boundary Protection	X	X	
SC-7(8)	Boundary Protection	X	X	
SC-7(9)	Boundary Protection	X	X	
SC-7(10)	Boundary Protection	X		
SC-7(11)	Boundary Protection		X	
SC-7(12)	Boundary Protection	X	X	X
SC-7(13)	Boundary Protection	X	X	
SC-7(14)	Boundary Protection	X	X	
SC-7(15)	Boundary Protection	X	X	
SC-7(16)	Boundary Protection	X		
SC-7(17)	Boundary Protection		X	
SC-7(18)	Boundary Protection	X	X	X
SC-8	Transmission Integrity		X	
SC-8(1)	Transmission Integrity		X	
SC-8(2)	Transmission Integrity		X	
SC-9	Transmission Confidentiality	X		
SC-9(1)	Transmission Confidentiality	X		
SC-9(2)	Transmission Confidentiality	X		

ID	Title	C	I	A
SC-10	Network Disconnect	X	X	
SC-11	Trusted Path		X	
SC-12	Cryptographic Key Establishment And Management	X	X	
SC-12(1)	Cryptographic Key Establishment And Management			X
SC-12(2)	Cryptographic Key Establishment And Management	X	X	
SC-12(3)	Cryptographic Key Establishment And Management	X	X	
SC-12(4)	Cryptographic Key Establishment And Management	X	X	
SC-12(5)	Cryptographic Key Establishment And Management	X	X	
SC-13	Use Of Cryptography	X	X	
SC-13(1)	Use Of Cryptography	X		
SC-13(2)	Use Of Cryptography	X		
SC-13(3)	Use Of Cryptography	X		
SC-13(4)	Use Of Cryptography		X	
SC-14	Public Access Protections		X	X
SC-15	Collaborative Computing Devices	X		
SC-15(1)	Collaborative Computing Devices	X		
SC-15(2)	Collaborative Computing Devices	X	X	
SC-15(3)	Collaborative Computing Devices	X	X	
SC-16	Transmission Of Security Attributes	X	X	
SC-16(1)	Transmission Of Security Attributes		X	
SC-17	Public Key Infrastructure Certificates	X	X	
SC-18	Mobile Code		X	
SC-18(1)	Mobile Code		X	
SC-18(2)	Mobile Code		X	
SC-18(3)	Mobile Code		X	
SC-18(4)	Mobile Code		X	
SC-19	Voice Over Internet Protocol	X	X	
SC-20	Secure Name / Address Resolution Service (Authoritative Source)		X	
SC-20(1)	Secure Name / Address Resolution Service (Authoritative Source)		X	
SC-21	Secure Name / Address Resolution Service (Recursive Or Caching Resolver)		X	
SC-21(1)	Secure Name / Address Resolution Service (Recursive Or Caching Resolver)		X	
SC-22	Architecture And Provisioning For Name / Address Resolution Service	X	X	X
SC-23	Session Authenticity		X	
SC-23(1)	Session Authenticity		X	
SC-23(2)	Session Authenticity		X	
SC-23(3)	Session Authenticity		X	
SC-23(4)	Session Authenticity		X	
SC-24	Fail In Known State	X	X	
SC-25	Thin Nodes		X	
SC-26	Honeypots		X	
SC-26(1)	Honeypots		X	
SC-27	Operating System-Independent Applications		X	
SC-28	Protection Of Information At Rest	X	X	
SC-28(1)	Protection Of Information At Rest	X	X	
SC-29	Heterogeneity		X	
SC-30	Virtualization Techniques		X	
SC-30(1)	Virtualization Techniques		X	
SC-30(2)	Virtualization Techniques		X	
SC-31	Covert Channel Analysis	X		
SC-31(1)	Covert Channel Analysis	X		

ID	Title	C	I	A
SC-32	Information System Partitioning	X	X	
SC-33	Transmission Preparation Integrity		X	
SC-34	Non-modifiable executable programs		X	
SC-34(1)	Non-modifiable executable programs		X	
SC-34(2)	Non-modifiable executable programs		X	
SI-1	System And Information Integrity Policy And Procedures	X	X	X
SI-2	Flaw Remediation		X	
SI-2(1)	Flaw Remediation		X	
SI-2(2)	Flaw Remediation		X	
SI-2(3)	Flaw Remediation		X	
SI-2(4)	Flaw Remediation		X	
SI-3	Malicious Code Protection		X	
SI-3(1)	Malicious Code Protection		X	
SI-3(2)	Malicious Code Protection		X	
SI-3(3)	Malicious Code Protection		X	
SI-3(4)	Malicious Code Protection		X	
SI-3(5)	Malicious Code Protection		X	
SI-3(6)	Malicious Code Protection		X	
SI-4	Information System Monitoring		X	
SI-4(1)	Information System Monitoring		X	
SI-4(2)	Information System Monitoring		X	
SI-4(3)	Information System Monitoring		X	
SI-4(4)	Information System Monitoring	X	X	
SI-4(5)	Information System Monitoring		X	
SI-4(6)	Information System Monitoring		X	
SI-4(7)	Information System Monitoring		X	X
SI-4(8)	Information System Monitoring	X	X	X
SI-4(9)	Information System Monitoring		X	
SI-4(10)	Information System Monitoring	X	X	
SI-4(11)	Information System Monitoring	X		
SI-4(12)	Information System Monitoring	X	X	
SI-4(13)	Information System Monitoring	X	X	X
SI-4(14)	Information System Monitoring	X	X	
SI-4(15)	Information System Monitoring	X	X	
SI-4(16)	Information System Monitoring		X	
SI-4(17)	Information System Monitoring	X	X	
SI-5	Security Alerts, Advisories, And Directives		X	
SI-5(1)	Security Alerts, Advisories, And Directives		X	
SI-6	Security Functionality Verification		X	
SI-6(1)	Security Functionality Verification		X	
SI-6(2)	Security Functionality Verification		X	
SI-6(3)	Security Functionality Verification		X	
SI-7	Software And Information Integrity		X	
SI-7(1)	Software And Information Integrity		X	
SI-7(2)	Software And Information Integrity		X	
SI-7(3)	Software And Information Integrity		X	
SI-7(4)	Software And Information Integrity		X	
SI-8	Spam Protection		X	X
SI-8(1)	Spam Protection		X	X
SI-8(2)	Spam Protection		X	X
SI-9	Information Input Restrictions		X	

ID	Title	C	I	A
SI-10	Information Input Validation		X	
SI-11	Error Handling		X	
SI-12	Information Output Handling And Retention	X	X	
SI-13	Predictable Failure Prevention			X
SI-13(1)	Predictable Failure Prevention			X
SI-13(2)	Predictable Failure Prevention			X
SI-13(3)	Predictable Failure Prevention			X
SI-13(4)	Predictable Failure Prevention			X
PM-1	Information Security Program Plan	X	X	X
PM-2	Senior Information Security Officer	X	X	X
PM-3	Information Security Resources	X	X	X
PM-4	Plan of Action and Milestones Process	X	X	X
PM-5	Information System Inventory	X	X	X
PM-6	Information Security Measures of Performance	X	X	X
PM-7	Enterprise Architecture	X	X	X
PM-8	Critical Infrastructure Plan	X	X	X
PM-9	Risk Management Strategy	X	X	X
PM-10	Security Authorization Process	X	X	X
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, Revision 3, Appendix E, has been deferred at this time from this release of CNSSI No. 1253 pending further review/discussions by the national security community.

APPENDIX F

SECURITY CONTROL CATALOG

SECURITY CONTROLS, ENHANCEMENTS, AND SUPPLEMENTAL GUIDANCE

CNSSI 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 No. 1253. No prioritization of security controls is specified by CNSSI No. 1253.

Organization-defined parameters for security controls included in the baselines and 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 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 use as needed, 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, Revision 3, 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 standard recommended values for organization-defined parameters in National Security Systems (NSS). This table lists all of the security controls (including control enhancements) from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3, which require organization-defined parameters. Table J-1 provides values for each control which this instruction includes in a baseline (see Appendix D), where a value has been established as a standard for all NSS, to facilitate reciprocity within the national security community.

For Table J-1 parameter entries that do not have defined values, organizations must define these appropriately upon selection for use for a specific system, and in coordination with other organizations when they affect reciprocity. Organizations may only establish and use different values for the parameters than those defined herein, when those values are more restrictive, or are consistent with the risk management strategies of the affected organizations, and when doing so does not negatively affect reciprocity.

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

CNTL NO. (Enhancement)	CONTROL NAME	800-53 PARAMETER 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*]: …	…at least annually if not otherwise defined in formal organizational policy
AC-2	Account Management	The organization manages information system accounts, including: … j. Reviewing accounts [*Assignment: organization-defined frequency*].	j. …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 90 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*]; …	*Not appropriate to define at the CNSS level for all NSS.*
AC-3 (2)	Access Enforcement	The information system enforces dual authorization, based on organizational policies and procedures for [*Assignment: organization-defined privileged commands*].	*Not appropriate to define at the CNSS level for all NSS.*

CNTL NO. (Enhancement)	CONTROL NAME	800-53 PARAMETER 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.	*Not appropriate to define at the CNSS level for all NSS.*
AC-3 (5)	Access Enforcement	The information system prevents access to [*Assignment: organization-defined security-relevant information*] except during secure, non-operable system states.	*Not appropriate to define at the CNSS level for all NSS.*
AC-3 (6)	Access Enforcement	The organization encrypts or stores off line in a secure location [*Assignment: organization-defined user and/or system information*].	*Not appropriate to define at the CNSS level for all NSS.*
AC-4 (5)	Information Flow Enforcement	The information system enforces [*Assignment: organization-defined limitations on the embedding of data types within other data types*].	*Not appropriate to define at the CNSS level for all NSS.*
AC-4 (7)	Information Flow Enforcement	The information system enforces [*Assignment: organization-defined one-way flows*] using hardware mechanisms.	*Not appropriate to define at the CNSS level for all NSS.*
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.	*Not appropriate to define at the CNSS level for all NSS.*
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.	*Not appropriate to define at the CNSS level for all NSS.*
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*].	*Not appropriate to define at the CNSS level for all NSS.*
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.	*Not appropriate to define at the CNSS level for all NSS.*
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*].	*Not appropriate to define at the CNSS level for all NSS.*
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*].	*Not appropriate to define at the CNSS level for all NSS.*

CNTL NO. (Enhancement)	CONTROL NAME	800-53 PARAMETER 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.	…privileged 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.	*Not appropriate to define at the CNSS level for all NSS.*
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. …a maximum of 5 …15 minutes b. …locks the account/node for at least 15 minutes, or until unlocked by an administrator
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.	10
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*].	*Not appropriate to define at the CNSS level for all NSS.*
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*].	*Not appropriate to define at the CNSS level for all NSS.*
AC-10	Concurrent Session Control	The information system limits the number of concurrent sessions for each system account to [*Assignment: organization-defined number*].	…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

CNTL NO. (Enhancement)	CONTROL NAME	800-53 PARAMETER TEXT	DEFINED VALUE FOR NSS
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.	*Not appropriate to define at the CNSS level for all 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*].	*Not appropriate to define at the CNSS level for all NSS.*
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.	*Not appropriate to define at the CNSS level for all NSS.*
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.	*Not appropriate to define at the CNSS level for all NSS.*
AC-17 (8)	Remote Access	The organization disables [*Assignment: organization-defined networking protocols within the information system deemed to be non-secure*] except for explicitly identified components in support of specific operational requirements.	*Not appropriate to define at the CNSS level for all NSS.*
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 if not otherwise defined in formal organizational policy
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. *Not appropriate to define at the CNSS level for all NSS.*
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) *Not appropriate to define at the CNSS level for all NSS.*

CNTL NO. (Enhancement)	CONTROL NAME	800-53 PARAMETER 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.	*Not appropriate to define at the CNSS level for all NSS.*
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 ….	…quarterly or as new information is posted
Awareness and Training			
AT-1	Security Awareness And Training Policy And Procedures	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: …	…at least annually if not otherwise defined in formal organizational policy
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.	*Not appropriate to define at the CNSS level for all NSS.*
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 least annually if not otherwise defined in formal organizational policy
AT-4	Security Training Records	The organization: … b. Retains individual training records for [*Assignment: organization-defined time period*].	*b. Not appropriate to define at the CNSS level for all NSS.*
Audit and Accountability			
AU-1	Security Audit And Accountability Policy And Procedures	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: …	…at least annually if not otherwise defined in formal organizational policy

CNTL NO. (Enhancement)	CONTROL NAME	800-53 PARAMETER 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**. All organizations must define a list of audited events in the policy for their organization defined in accordance with AU-1.
AU-2 (3)	Auditable Events	The organization reviews and updates the list of auditable events [*Assignment: organization-defined frequency*].	… at least annually
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.	*Not appropriate to define at the CNSS level for all NSS.*
AU-3 (2)	Content of Audit Records	The organization centrally manages the content of audit records generated by [*Assignment: organization-defined information system components*].	*Not appropriate to define at the CNSS level for all NSS.*
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. *Not appropriate to define at the CNSS level for all NSS.*
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*.	…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*].	…auditing software/hardware errors; failures in the audit capturing mechanisms; and audit storage capacity being reached or exceeded

CNTL NO. (Enhancement)	CONTROL NAME	800-53 PARAMETER TEXT	DEFINED VALUE FOR NSS
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.	*Not appropriate to define at the CNSS level for all NSS.*
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. … on at least on a weekly basis
AU-8 (1)	Time Stamps	The information system synchronizes internal information system clocks [*Assignment: organization-defined frequency*] with [*Assignment: organization-defined authoritative time source*].	…at least every 24 hours *…not appropriate to define at the CNSS level for all NSS.*
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.	*Not appropriate to define at the CNSS level for all NSS.*
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.	…a minimum of 5 years for Sensitive Compartmented Information and Sources And Methods Intelligence information …a minimum of 1 year for all other information (Unclassified through Collateral Top Secret)
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. …all information system and network components
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*].	*Not appropriate to define at the CNSS level for all NSS.* …one second
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*].	*Not appropriate to define at the CNSS level for all NSS.*

Security Assessment and Authorization			
CA-1	Security Assessment And Authorization Policy And Procedures	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: …	…at least annually if not otherwise defined in formal organizational policy
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*]].	*Not appropriate to define at the CNSS level for all NSS.*
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. …at least quarterly
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. …at least every three (3) years, when significant security breaches occur, whenever there is a significant change to the system, or to the environment in which the system operates.
CA-7	Continuous Monitoring	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. …at least annually or when requested by organizational officials
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.	…at least annually, announced, in-depth monitoring
Configuration Management			
CM-1	Configuration Management Policy And Procedures	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: …	…at least annually if not otherwise defined in formal organizational policy

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) …at least annually (b) …significant or security relevant changes, or security incidents
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) . . .a list of software programs not authorized to execute on the information system, to include, at a minimum: • Games • Public domain software or "shareware" which have been obtained from unofficial channels • Software applications that have been developed outside Government approved facilities, such as those developed on personally owned computers at home or software acquired via non-U.S. Government channels • Personally owned software • Software purchased using employee funds (from an activity such as a coffee fund) • Software from unknown sources • Illegally copied software in violation of software licensing or copyright rules • Music and video or multimedia compact disks, not procured through official Government channels;
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) *Not appropriate to define at the CNSS level for all NSS.*
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. (1) Configuration Control Board (2) *Not appropriate to define at the CNSS level for all NSS.*
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) …within 90 days

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)*].	…voting member of the 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.	…at least annually
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.	*Not appropriate to define at the CNSS level for all NSS.*
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*].	*Not appropriate to define at the CNSS level for all NSS.*
CM-5 (5)	Access Restrictions for Change	The organization: … (b) Reviews and reevaluates information system developer/integrator privileges [*Assignment: organization-defined frequency*].	(b) …at least annually
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.	*Not appropriate to define at the CNSS level for all NSS.*
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; …	*Not appropriate to define at the CNSS level for all NSS.*
CM-6 (2)	Configuration Settings	The organization employs automated mechanisms to respond to unauthorized changes to [*Assignment: organization-defined configuration settings*].	*Not appropriate to define at the CNSS level for all 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*].	*Not appropriate to define at the CNSS level for all NSS.*
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.	…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*].	*Not appropriate to define at the CNSS level for all NSS.*
CM-7 (3)	Least Functionality	The organization ensures compliance with [*Assignment: organization-defined registration requirements for ports, protocols, and services*].	*Not appropriate to define at the CNSS level for all NSS.*

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 …	d. hardware inventory specifications (manufacturer, type, model, serial number, physical location), software license information, information system/component owner, and for a networked component/device, the machine name.
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) …*Not appropriate to define at the CNSS level for all NSS.*
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.	…position or role
Contingency Planning			
CP-1	Contingency Planning Policy And Procedures	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: …	…at least annually if not otherwise defined in formal organizational policy
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. …key personnel and organizational elements identified in the contingency plan d. …at least annually f. … key personnel and organizational elements identified in the contingency plan
CP-2 (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.	…12 hours or as defined in the contingency plan
CP-2 (4)	Contingency Plan	The organization plans for the full resumption of missions and business functions within [*Assignment: organization-defined time period*] of contingency plan activation.	…5 mission/business days or as defined in the contingency plan
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 or as defined in the contingency plan
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. 1. …at least annually or as defined in the contingency plan 2. *Not appropriate to define at the CNSS level for all NSS.*

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 12 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 12 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. …at least weekly or as defined in the contingency plan b. …at least weekly or as defined in the contingency plan c. …when created or received, when updated, or as defined in the contingency plan
CP-9 (1)	Information System Backup	The organization tests backup information [*Assignment: organization-defined frequency*] to verify media reliability and information integrity.	…not less than monthly, or as defined in the contingency plan
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*].	*Not appropriate to define at the CNSS level for all NSS.*
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*].	*Not appropriate to define at the CNSS level for all NSS.*
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.	*Not appropriate to define at the CNSS level for all NSS.*
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*].	*Not appropriate to define at the CNSS level for all NSS.*
Identification and Authentication			
IA-1	Identification and Authentication Policy And Procedures	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: …	…at least annually if not otherwise defined in formal organizational policy

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.	*Not appropriate to define at the CNSS level for all NSS.*
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.	*Not appropriate to define at the CNSS level for all NSS.*
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.	…all network connected endpoint devices
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. …at least one year e. …not to exceed 35 days
IA-4(4)	Identifier Management	The organization manages user identifiers by uniquely identifying the user as [*Assignment: organization-defined characteristic identifying user status*].	A contractor or government employee and citizenship
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 for passwords.
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) 24 hours minimum and 180 days maximum (e) a minimum of 10 NOTE: The above requirements do not apply to one-time use passwords.
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).	*Not appropriate to define at the CNSS level for all NSS.*

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.	…precautions including advising users that they must not use the same password for any of the following: Domains of differing classification levels. More than one domain of a classification level (e.g., internal agency network and Intelink). More than one privilege level (e.g., user, administrator) ….
Incident Response			
IR-1	Incident Response Policy And Procedures	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: …	…at least annually if not otherwise defined in formal organizational policy
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.	a. …at least annually *b. Not appropriate to define at the CNSS level for all NSS.*
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*].	*Not appropriate to define at the CNSS level for all NSS.*
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. Not appropriate to define at the CNSS level for all 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. …all personnel with a role or responsibility for implementing the incident response plan c. …at least annually (incorporating lessons learned from past incidents) e. …all personnel with a role or responsibility for implementing the incident response plan, not later than 30 days after the change is made
Maintenance			
MA-1	Maintenance Policy And Procedures	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: …	…at least annually if not otherwise defined in formal organizational policy
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) *Not appropriate to define at the CNSS level for all NSS.*

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.	1. *Not appropriate to define at the CNSS level for all NSS.* 2. *Not appropriate to define at the CNSS level for all NSS.*
Media Protection			
MP-1	Media Protection Policy And Procedures	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: …	…at least annually if not otherwise defined in formal organizational policy
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*].	1. *…not appropriate to define at the CNSS level for all NSS.* 2. *…not appropriate to define at the CNSS level for all NSS.* 3. *…not appropriate to define at the CNSS level for all NSS.*
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. 1. *Not appropriate to define at the CNSS level for all NSS.* *2. Not appropriate to define at the CNSS level for all NSS.*
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. (1) …digital and non-digital media containing sensitive, controlled, and/or classified information. (2). …in an area or container approved for processing and storing media based on the sensitivity and/or classification of the information maintained within the media. (3) *Not appropriate to define at the CNSS level for all 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. 1. …digital and non-digital media containing sensitive, controlled, and/or classified information. 2. *Not appropriate to define at the CNSS level for all NSS.*
MP-6 (2)	Media Sanitization	The organization tests sanitization equipment and procedures to verify correct performance [*Assignment: organization-defined frequency*].	… at least annually if not otherwise defined in formal organizational policy

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*].	*Not appropriate to define at the CNSS level for all NSS.*
Physical and Environmental Protection			
PE-1	Physical and Environmental Protection Policy And Procedures	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: …	…at least annually if not otherwise defined in formal organizational policy
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. *…Not appropriate to define at the CNSS level for all NSS.*; g. *…Not appropriate to define at the CNSS level for all NSS.*
PE-3(4)	Physical Access Control	The organization uses lockable physical casings to protect [*Assignment: organization-defined information system components*] from unauthorized physical access.	*Not appropriate to define at the CNSS level for all NSS.*
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.	*Not appropriate to define at the CNSS level for all NSS.*
PE-6	Monitoring Physical Access	The organization: … b. Reviews physical access logs [*Assignment: organization-defined frequency*]; …	b. … at least every 90 days if not otherwise defined in formal organizational policy
PE-8	Access Records	The organization: … b. Reviews the visitor access records [*Assignment: organization-defined frequency*].	b. … at least every 90 days if not otherwise defined in formal organizational policy
PE-9 (2)	Power Equipment and Power Cabling	The organization employs automatic voltage controls for [*Assignment: organization-defined list of critical information system components*].	*Not appropriate to define at the CNSS level for all 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. *Not appropriate to define at the CNSS level for all NSS.*
PE-13(4)	Fire Protection	The organization ensures that the facility undergoes [*Assignment: organization-defined frequency*] fire marshal inspections and promptly resolves identified deficiencies	*Not appropriate to define at the CNSS level for all NSS.*

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. Not appropriate to define at the CNSS level for all NSS.* *b. Not appropriate to define at the CNSS level for all NSS.*
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.	*…Not appropriate to define at the CNSS level for all NSS.*
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. Not appropriate to define at the CNSS level for all NSS.*
Planning			
PL-1	Planning Policy And Procedures	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: …	…at least annually if not otherwise defined in formal organizational policy
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 or when required due to system modifications
PL-2 (1)	System Security Plan	The organization: … (b) Reviews and updates the CONOPS [*Assignment: organization-defined frequency*].	(b) …annually or as required due to system modifications
Personnel Security			
PS-1	Personnel Security Policy And Procedures	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: …	…at least annually if not otherwise defined in formal organizational policy
PS-2	Position Categorization	The organization: … c. Reviews and revises position risk designations [*Assignment: organization-defined frequency*].	c. …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. *Not appropriate to define at the CNSS level for all 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*].	(1) …actions to ensure all system accesses no longer required (need to know) are removed (2) 30 days if not otherwise defined in formal organizational policy
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*]: …	…at least annually if not otherwise defined in formal organizational policy

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. …a risk assessment report or security plan 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. …at least every 180 days *d. Not appropriate to define at the CNSS level for all NSS.*
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 180 days or prior to running scans
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.	*…not appropriate to define at the CNSS level for all NSS.*
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.	*Not appropriate to define at the CNSS level for all NSS.*
System and Services Acquisition			
SA-1	System and Services Acquisition Policy And Procedures	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: …	…at least annually if not otherwise defined in formal organizational policy
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.	Measures in accordance with CNSS Directive 505, Supply Chain Risk Management.
SA-13	Trustworthiness	The organization requires that the information system meets [*Assignment: organization-defined level of trustworthiness*].	*Not appropriate to define at the CNSS level for all NSS.*

SA-14	Critical Information System Components	The organization: a. Determines [*Assignment: organization-defined list of critical information system components that require reimplementation*]; and …	*Not appropriate to define at the CNSS level for all NSS.*
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.	*Not appropriate to define at the CNSS level for all NSS.*
System and Communications Protection			
SC-1	System and Communications Protection Policy And Procedures	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: …	…at least annually if not otherwise defined in formal organizational policy
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*].	Consumption of scarce, limited, or non-renewable resources, destruction or alteration of configuration information, physical destruction or alteration of network components
SC-7 (4)	Boundary Protection	The organization: … (e) Reviews exceptions to the traffic flow policy [*Assignment: organization-defined frequency*]	(e) …at least every 6 months
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.	(1) …all internal communications traffic, except traffic specifically exempted by the Authorizing Official or organizational policy… (2) …networks outside the control of the organization …
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.	*…not appropriate to define at the CNSS level for all NSS.*
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*].	…cross domain solutions and controlled interfaces.
SC-9 (1)	Transmission Confidentiality	The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by [*Assignment: organization-defined alternative physical measures*].	A protected distribution system or in a controlled access area accredited for open storage.
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.	...not more than 1 hour

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 re-authentication*].	*Not appropriate to define at the CNSS level for all NSS.*
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.	*Not appropriate to define at the CNSS level for all NSS.*
SC-13(4)	Use of Cryptography	The organization employs [*Selection: FIPS-validated; NSA-approved*] cryptography to implement digital signatures.	*Not appropriate to define at the CNSS level for all NSS.*
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. Remote activation of centrally managed dedicated VTC Suites located in approved VTC locations
SC-15 (3)	Collaborative Computing Devices	The organization disables or removes collaborative computing devices from information systems in [*Assignment: organization-defined secure work areas*].	*Not appropriate to define at the CNSS level for all NSS.*
SC-17	Public Key Infrastructure Certificates	The organization issues public key certificates under an *[Assignment: organization-defined certificate policy]* or obtains public key certificates under an appropriate certificate policy from an approved service provider.	*Not appropriate to define at the CNSS level for all 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 having limited functionality, with no capability for unmediated access to the services and resources of a computing platform) mobile code may be used.
SC-18 (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*].	*Not appropriate to define at the CNSS level for all NSS.*

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.	(1) …known secure state (2) …all types of failures (3) …information necessary to determine cause of failure and to return to operations with least disruption to mission/ business processes…
SC-27	Operating System-Independent Applications	The information system includes [*Assignment: organization-defined operating system-independent applications*].	*Not appropriate to define at the CNSS level for all 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*].	*Not appropriate to define at the CNSS level for all NSS.*
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.	*Not appropriate to define at the CNSS level for all NSS.*
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	*Not appropriate to define at the CNSS level for all NSS.*
System and Information Integrity			
SI-1	System and Information Integrity Policy And Procedures	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: …	…at least annually if not otherwise defined in formal organizational policy
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.	*Not appropriate to define at the CNSS level for all NSS.*
SI-2 (3)	Flaw Remediation	The organization measures the time between flaw identification and flaw remediation, comparing with [*Assignment: organization-defined benchmarks*].	*Not appropriate to define at the CNSS level for all NSS.*
SI-2 (4)	Flaw Remediation	The organization employs automated patch management tools to facilitate flaw remediation to [*Assignment: organization-defined information system components*].	*Not appropriate to define at the CNSS level for all NSS.*
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. (1) …at least weekly (2) …quarantine malicious code and send an alert to the system administrator

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.	*Not appropriate to define at the CNSS level for all 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. Not appropriate to define at the CNSS level for all NSS.*
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*].	*Not appropriate to define at the CNSS level for all NSS.*
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*].	*1. Not appropriate to define at the CNSS level for all NSS.* *2. Not appropriate to define at the CNSS level for all NSS.*
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*].	*…not appropriate to define at the CNSS level for all NSS.*
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) Not appropriate to define at the CNSS level for all NSS.* *(d) Not appropriate to define at the CNSS level for all NSS.*
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. *Not appropriate to define at the CNSS level for all NSS.*
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.	*Not appropriate to define at the CNSS level for all NSS.* *Not appropriate to define at the CNSS level for all NSS.…* notifies system / security administrator
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 appropriate to define at the CNSS level for all NSS.*

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*].	*Not appropriate to define at the CNSS level for all 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. *Not appropriate to define at the CNSS level for all NSS.*
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. Not appropriate to define at the CNSS level for all NSS.*
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.	*Not appropriate to define at the CNSS level for all NSS.*
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*].	*Not appropriate to define at the CNSS level for all NSS.*
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*].	*Not appropriate to define at the CNSS level for all NSS.*
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*].	*Not appropriate to define at the CNSS level for all NSS.*
Program Management			
PM-1	Security Program Plan	The organization: a. … b. Reviews the organization-wide information security program plan [*Assignment: organization-defined frequency*]	b. At least annually if not otherwise defined in formal organizational policy.

APPENDIX K

OVERLAYS
STANDARD SPECIFICATIONS OF SECURITY CONTROLS AND SUPPORTING GUIDANCE

Overview

An overlay is a specification of security controls and supporting guidance used to complement the security control baselines and parameter values in CNSSI No. 1253 and to complement the supplemental guidance in NIST SP 800-53. An overlay's specifications may be more stringent or less stringent than the controls and guidance complemented. Overlays may be applied to reflect the needs of different information types (e.g., personally identifiable information [PII], financial, or highly sensitive types of intelligence); system functionality needs (e.g., stand-alone systems, cross domain solutions, or controlled interface systems); or environmental or operationally-driven needs (e.g., tactical, space-based, or test environment).

Overlay Development and Implementation

The overlay template (Attachment 1 of CNSSI No. 1253) provides instructions for overlay developers on the appropriate content and format of overlays.

Each standardized, approved, and CNSS-published overlay provides instructions how to implement the specific overlay.

Governance and Publication of Overlays

Overlays are developed, reviewed, approved, and published by organizations authorized for doing so by CNSS, the Director of National Intelligence, or the Secretary of Defense. CNSS provides downloadable copies[11] of the approved and published overlays.

[11] The URLs for the websites providing the overlays will be documented here when identified by CNSS.