Defense Security Service

Industrial Security Field Operations

NISP Authorization Office (NAO)

(Formerly Office of the Designated Approving Authority)

NISPOM to NIST (800-53r4)
Security Control Mapping
For
DSS Risk Management Framework

May 2016

Table of Contents

NIST Security Controls

Foreword

This document is intended to reduce duplication of compliance effort by displaying the differences between the National Institute of Standards and Technology (NIST) (800-53r4) security standards and those of the National Industrial Security Program Operating Manual (NISPOM). Implementing this guideline should provide the most efficient path to compliance with NISP Risk Management Framework (RMF) requirements, and the creation of repeatable assessment procedures that are effective at discovering and mitigating unacceptable risk.

This document's layout displays the familiar NISPOM references from the DSS Certification and Accreditation process, and overlays the NIST RMF security controls for easy comparison. The resulting map highlights the differences between the old (NISPOM) and the new (NIST/ RMF). At first glance, NIST/RMF appears to be a significant expansion; however, NIST/RMF adds few additional requirements. NIST/RMF provides greater detail and relevance to existing requirements, in contrast to NISPOM's more generalized and outdated requirements. The resulting regulations are more current, transparent and standardized.

Transitioning to risk-based decision-making mirrors similar changes in other fields, like finance, insurance and program management. Utilizing a "check-the-box" mentality does not adequately assess hazards in those fields, and does not build an effective security program either. Properly implementing the RMF process and procedures in this guideline ensures adequate security controls are established, residual risks are identified and evaluated before accessing the IS, and security plans are continuously monitored for their effectiveness. More than simply achieving compliance, implementing RMF will assure leadership that security personnel have used critical thinking to ascertain the threat picture, assess risks, and have instituted sufficient security controls to protect assets from theft and organization information systems from intrusion.

Note that this document does not imply a one-to-one substitution of security controls. Additionally, your organization's contractual requirements may supersede this guideline document. Please evaluate appropriately.

Revision History

Release Date:	Summary of Changes:	Version Number:
25 May 2016	Original publication.	1.0

NISPOM to NIST (800-53r4) Security Control Mapping

NIST Control		NISPOM Controls	
Access Controls			
AC-1	Access Controls Policy and Procedures	8-101	Responsibilities
		8-606	Access Controls (Access). The IS shall store and preserve the integrity of the sensitivity of all information internal to the IS.
AC-2	Account Management	8-606	Access Controls (Access). The IS shall store and preserve the integrity of the sensitivity of all information internal to the IS.
AC-3	Access Enforcement	8-606	Access Controls (Access). The IS shall store and preserve the integrity of the sensitivity of all information internal to the IS.
AC-4	Information Flow Enforcement	None	
AC-5	Separation of Duties	8-611	Separation of Function Requirements (Separation). At Protection Level 3 the functions of the ISSO and the system manager shall not be performed by the same person.
AC-6	Least Privilege	8-303	Identification and Authentication Management. As the complexity of a specific IS and the associated residual risk for this system increase, the need for identification and authentication of users and process becomes more significant. Identification and authentication controls are required to ensure that users have the appropriate clearances and need-to-know for the information on a particular system and shall be managed in accordance with procedures identified in the SSP.
AC-7	Unsuccessful Logon Attempts	8-609	Session Controls (SessCtrl).
AC-8	System Use Notification	8-609	Session Controls (SessCtrl).
AC-9	Previous Logon (Access) Notification	8-609	Session Controls (SessCtrl).
AC-10	Concurrent Session Control	8-609	Session Controls (SessCtrl).
AC-11	Session Lock	8-609	Session Controls (SessCtrl).
AC-12	Session Termination	8-311	Configuration management (CM) ensures that protection features are implemented and maintained in the system. CM applies a level of discipline and control to the processes of system maintenance and modification. CM provides system users with a measure of assurance that the implemented system represents the approved system.
		8-609	Session Controls (SessCtrl).
AC-13	**Withdrawn**		
AC-14	Permitted Actions without Identification or Authentication	8-501	Single-user, Stand-alone Systems. Extensive technical protection measures are normally inappropriate and inordinately expensive for single-user, stand-alone systems. The CSA can approve administrative and environmental protection measures for such systems.

		8-504	Tactical, Embedded, Data Acquisition, and Special-Purpose Systems. Some systems are incapable of alteration by users and are designed and implemented to provide a very limited set of predetermined functions. Certain tactical or so-called "embedded" systems fall into this category, as do some data-acquisition systems and some other special-purpose systems. Those systems also have the characteristics that: first and most importantly, there are no general users on the system. If the CSA determines that such a system is sufficiently incapable of alteration and that the application(s) running on the system provide an adequate level of security, than the system does not have to meet additional security requirements specified for more-general-purpose systems in this section. The CSA and implementers are cautioned to be sure that such systems do, in all operational situations, provide the separation appropriate to the system's protection level.
		8-505	Systems with Group Authenticators. Many security measures specified in this section implicitly assume that the system includes an acceptable level of individual accountability. This is normally ensured by the use of unique user identifiers and authenticators. Operationally, the design of some systems necessitates more than one individual using the same identifier/ authenticator combination. Such situations are often referred to as requiring the use of group authenticators. In general the use of group authenticators precludes the association of a particular act with the individual who initiated that act. In turn, this can preclude assignment of responsibility and can exacerbate the difficulties involved in incident investigation. Group authenticators shell be used only for broader access after the use of a unique authenticator for initial identification and authentication, and documented in SSP. Group authenticators may not be shared with anyone outside of the group.
AC-15	**Withdrawn**		
AC-16	Security Attributes	8-306	Marking Hardware, Output, and Media. Markings on hardware, output, and media shall conform to Chapter 4 of this manual. If the required marking is impractical or interferes with the operation of the media, the CSA may approve alternate marking procedures.
AC-17	Remote Access	None	
AC-18	Wireless Access	8-311	Configuration management (CM) ensures that protection features are implemented and maintained in the system. CM applies a level of discipline and control to the processes of system maintenance and modification. CM provides system users with a measure of assurance that the implemented system represents the approved system.
AC-19	Access Control for Mobile Devices	8-610	Security documentation includes all descriptions of the security features, design descriptions of security-relevant software and hardware, certification packages, and system security plans. The SSP is the basic system protection document and evidence that the proposed system, or update to an existing system, meets the protection profile requirements. The SSP is used throughout the certification and approval process and serves for the lifetime of the system as the formal record of the system and its environment as approved for operation. The SSP also serves as the basis for inspections of the system. Information common to several systems at a facility or information contained in other documents may be attached to or referenced in the SSP.
AC-20	Use of External Information Systems	8-700	Interconnected Systems Management. The characteristics and capabilities of an IS implemented as networks require special security considerations. This section states additional requirements on a network or expands on the security requirements stated in Section 6 as they apply to a network.

AC-21	Information Sharing	None	
AC-22	Publicly Accessible Content	None	
AC-23	Data Mining Protection	None	
AC-24	Access Control Decisions	None	
AC-25	Reference Monitor	None	
Awareness and Training			
AT-1	Security Awareness and Training Policy and Procedures	8-101	Responsibilities.
AT-2	Security Awareness Training	8-101	Responsibilities.
AT-3	Role-Based Security Training	8-101	Responsibilities.
		8-103	See IS Security Manager (ISSM) responsibilities.
		8-104	See IS Security Officer(s) (ISSO) responsibilities.
AT-4	Security Training Records	8-103	See ISSM responsibilities.
		8-104	See ISSO responsibilities.
AT-5	**Withdrawn**		
Audit and Accountability			
AU-1	Audit and Accountability Policy and Procedures	8-602	Audit Capability. Security auditing involves recognizing, recording, storing, and analyzing information related to security-relevant activities. The audit records can be used to determine which activities occurred and which user or process was responsible for them.
AU-2	Audit Events	8-602	Audit Capability. Security auditing involves recognizing, recording, storing, and analyzing information related to security-relevant activities. The audit records can be used to determine which activities occurred and which user or process was responsible for them.
AU-3	Content of Audit Records	8-602	Audit Capability. Security auditing involves recognizing, recording, storing, and analyzing information related to security-relevant activities. The audit records can be used to determine which activities occurred and which user or process was responsible for them.
AU-4	Audit Storage Capacity	8-602	Audit Capability. Security auditing involves recognizing, recording, storing, and analyzing information related to security-relevant activities. The audit records can be used to determine which activities occurred and which user or process was responsible for them.
AU-5	Response to Audit Processing Failures	8-602	Audit Capability. Security auditing involves recognizing, recording, storing, and analyzing information related to security-relevant activities. The audit records can be used to determine which activities occurred and which user or process was responsible for them.
AU-6	Audit Review, Analysis, and Reporting	8-602	Audit Capability. Security auditing involves recognizing, recording, storing, and analyzing information related to security-relevant activities. The audit records can be used to determine which activities occurred and which user or process was responsible for them.
AU-7	Audit Reduction and Report Generation	8-602	Audit Capability. Security auditing involves recognizing, recording, storing, and analyzing information related to security-relevant activities. The audit records can be used to determine which activities occurred and which user or process was responsible for them.
AU-8	Time Stamps	8-602	Audit Capability. Security auditing involves recognizing, recording, storing, and analyzing information related to security-relevant activities. The audit records can be used to determine which activities occurred and which user or process was responsible for them.

AU-9	Protection of Audit Information	8-602	Audit Capability. Security auditing involves recognizing, recording, storing, and analyzing information related to security-relevant activities. The audit records can be used to determine which activities occurred and which user or process was responsible for them.
AU-10	Non-repudiation	8-602	Audit Capability. Security auditing involves recognizing, recording, storing, and analyzing information related to security-relevant activities. The audit records can be used to determine which activities occurred and which user or process was responsible for them.
AU-11	Audit Record Retention	8-602	Audit Capability. Security auditing involves recognizing, recording, storing, and analyzing information related to security-relevant activities. The audit records can be used to determine which activities occurred and which user or process was responsible for them.
AU-12	Audit Generation	8-602	Audit Capability. Security auditing involves recognizing, recording, storing, and analyzing information related to security-relevant activities. The audit records can be used to determine which activities occurred and which user or process was responsible for them.
AU-13	Monitoring for Information Disclosure	8-602	Audit Capability. Security auditing involves recognizing, recording, storing, and analyzing information related to security-relevant activities. The audit records can be used to determine which activities occurred and which user or process was responsible for them.
AU-14	Session Audit	8-602	Audit Capability. Security auditing involves recognizing, recording, storing, and analyzing information related to security-relevant activities. The audit records can be used to determine which activities occurred and which user or process was responsible for them.
AU-15	Alternate Audit Capability	8-602	Audit Capability. Security auditing involves recognizing, recording, storing, and analyzing information related to security-relevant activities. The audit records can be used to determine which activities occurred and which user or process was responsible for them.
AU-16	Cross-Organizational Auditing	8-602	Audit Capability. Security auditing involves recognizing, recording, storing, and analyzing information related to security-relevant activities. The audit records can be used to determine which activities occurred and which user or process was responsible for them.
Security Assessment and Authorization			
CA-1	Security Assessment and Authorization Policies and Procedures	8-200	The Certification and Accreditation (C&A) process is an integral part of the life cycle of an IS. The identification of protection measures occurs during system design or development. The formal C&A occurs after the protection measures have been implemented and any required IS protection documentation has been approved. Certification validates that the protection measures described in the SSP have been implemented on the system and that the protection measures are functioning properly. Accreditation is the approval by the CSA for the system to process classified information.
		8-201	Certification Process. Certification is the comprehensive evaluation of the technical and non-technical security features of an IS and other safeguards, made as part of and in support of the accreditation process, to establish the extent to which a particular design and implementation meet a specified set of security requirements. The certification process subjects the system to appropriate verification that protection measures have been correctly implemented. The ISSM shall review and certify to the CSA that all systems have the appropriate protection measures in place and validate that they provide that protection intended. The CSA may conduct an onsite assessment to validate the ISSM's review and certification of the IS.

		8-202	The accreditation of an IS is the official management decision to permit operation of an IS in a specified environment at an acceptable level of risk, based on the implementation of a CSA approved set of technical, managerial and procedural safeguards. All IS certifications shall be reviewed and IS accredited to operate by the CSA.
		8-610	Security documentation includes all descriptions of the security features, design descriptions of security-relevant software and hardware, certification packages, and system security plans. The SSP is the basic system protection document and evidence that the proposed system, or update to an existing system, meets the protection profile requirements. The SSP is used throughout the certification and approval process and serves for the lifetime of the system as the formal record of the system and its environment as approved for operation. The SSP also serves as the basis for inspections of the system. Information common to several systems at a facility or information contained in other documents may be attached to or referenced in the SSP.
CA-2	Security Assessments	8-610	Security documentation includes all descriptions of the security features, design descriptions of security-relevant software and hardware, certification packages, and system security plans. The SSP is the basic system protection document and evidence that the proposed system, or update to an existing system, meets the protection profile requirements. The SSP is used throughout the certification and approval process and serves for the lifetime of the system as the formal record of the system and its environment as approved for operation. The SSP also serves as the basis for inspections of the system. Information common to several systems at a facility or information contained in other documents may be attached to or referenced in the SSP.
CA-3	System Interconnections	8-610	Security documentation includes all descriptions of the security features, design descriptions of security-relevant software and hardware, certification packages, and system security plans. The SSP is the basic system protection document and evidence that the proposed system, or update to an existing system, meets the protection profile requirements. The SSP is used throughout the certification and approval process and serves for the lifetime of the system as the formal record of the system and its environment as approved for operation. The SSP also serves as the basis for inspections of the system. Information common to several systems at a facility or information contained in other documents may be attached to or referenced in the SSP.
CA-4	**Withdrawn**		
CA-5	Plan of Action and Milestones	8-610	Security documentation includes all descriptions of the security features, design descriptions of security-relevant software and hardware, certification packages, and system security plans. The SSP is the basic system protection document and evidence that the proposed system, or update to an existing system, meets the protection profile requirements. The SSP is used throughout the certification and approval process and serves for the lifetime of the system as the formal record of the system and its environment as approved for operation. The SSP also serves as the basis for inspections of the system. Information common to several systems at a facility or information contained in other documents may be attached to or referenced in the SSP.
CA-6	Security Authorization	8-202	The accreditation of an IS is the official management decision to permit operation of an IS in a specified environment at an acceptable level of risk, based on the implementation of a CSA approved set of technical, managerial and procedural safeguards. All IS certifications shall be reviewed and IS accredited to operate by the CSA.

		8-610	Security documentation includes all descriptions of the security features, design descriptions of security-relevant software and hardware, certification packages, and system security plans. The SSP is the basic system protection document and evidence that the proposed system, or update to an existing system, meets the protection profile requirements. The SSP is used throughout the certification and approval process and serves for the lifetime of the system as the formal record of the system and its environment as approved for operation. The SSP also serves as the basis for inspections of the system. Information common to several systems at a facility or information contained in other documents may be attached to or referenced in the SSP.
		8-614	Security Testing (Test). Certification and ongoing security testing are the verification of correct operation of the protection measures in a system. The ISSM will perform and document the required tests.
CA-7	Continuous Monitoring	8-202	The accreditation of an IS is the official management decision to permit operation of an IS in a specified environment at an acceptable level of risk, based on the implementation of a CSA approved set of technical, managerial and procedural safeguards. All IS certifications shall be reviewed and IS accredited to operate by the CSA.
		8-610	Security documentation includes all descriptions of the security features, design descriptions of security-relevant software and hardware, certification packages, and system security plans. The SSP is the basic system protection document and evidence that the proposed system, or update to an existing system, meets the protection profile requirements. The SSP is used throughout the certification and approval process and serves for the lifetime of the system as the formal record of the system and its environment as approved for operation. The SSP also serves as the basis for inspections of the system. Information common to several systems at a facility or information contained in other documents may be attached to or referenced in the SSP.
		8-614	Security Testing (Test). Certification and ongoing security testing are the verification of correct operation of the protection measures in a system. The ISSM will perform and document the required tests.
CA-8	Penetration Testing	8-610	Security documentation includes all descriptions of the security features, design descriptions of security-relevant software and hardware, certification packages, and system security plans. The SSP is the basic system protection document and evidence that the proposed system, or update to an existing system, meets the protection profile requirements. The SSP is used throughout the certification and approval process and serves for the lifetime of the system as the formal record of the system and its environment as approved for operation. The SSP also serves as the basis for inspections of the system. Information common to several systems at a facility or information contained in other documents may be attached to or referenced in the SSP.
		8-614	Security Testing (Test). Certification and ongoing security testing are the verification of correct operation of the protection measures in a system. The ISSM will perform and document the required tests.

CA-9	Internal System Connections	8-610	Security documentation includes all descriptions of the security features, design descriptions of security-relevant software and hardware, certification packages, and system security plans. The SSP is the basic system protection document and evidence that the proposed system, or update to an existing system, meets the protection profile requirements. The SSP is used throughout the certification and approval process and serves for the lifetime of the system as the formal record of the system and its environment as approved for operation. The SSP also serves as the basis for inspections of the system. Information common to several systems at a facility or information contained in other documents may be attached to or referenced in the SSP.
		8-700	Interconnected Systems Management. The characteristics and capabilities of an IS implemented as networks require special security considerations. This section states additional requirements on a network or expands on the security requirements stated in Section 6 as they apply to a network.
Configuration Management			
CM-1	Configuration Management Policy and Procedures	8-311	Configuration management (CM) ensures that protection features are implemented and maintained in the system. CM applies a level of discipline and control to the processes of system maintenance and modification. CM provides system users with a measure of assurance that the implemented system represents the approved system.
		8-610	Security documentation includes all descriptions of the security features, design descriptions of security-relevant software and hardware, certification packages, and system security plans. The SSP is the basic system protection document and evidence that the proposed system, or update to an existing system, meets the protection profile requirements. The SSP is used throughout the certification and approval process and serves for the lifetime of the system as the formal record of the system and its environment as approved for operation. The SSP also serves as the basis for inspections of the system. Information common to several systems at a facility or information contained in other documents may be attached to or referenced in the SSP.
CM-2	Baseline Configuration	8-202	The accreditation of an IS is the official management decision to permit operation of an IS in a specified environment at an acceptable level of risk, based on the implementation of a CSA approved set of technical, managerial and procedural safeguards. All IS certifications shall be reviewed and IS accredited to operate by the CSA.
		8-311	Configuration management (CM) ensures that protection features are implemented and maintained in the system. CM applies a level of discipline and control to the processes of system maintenance and modification. CM provides system users with a measure of assurance that the implemented system represents the approved system.
		8-610	Security documentation includes all descriptions of the security features, design descriptions of security-relevant software and hardware, certification packages, and system security plans. The SSP is the basic system protection document and evidence that the proposed system, or update to an existing system, meets the protection profile requirements. The SSP is used throughout the certification and approval process and serves for the lifetime of the system as the formal record of the system and its environment as approved for operation. The SSP also serves as the basis for inspections of the system. Information common to several systems at a facility or information contained in other documents may be attached to or referenced in the SSP.
CM-3	Configuration Change Control	8-103	See ISSM responsibilities.
		8-104	See ISSO responsibilities.

		8-311	Configuration management (CM) ensures that protection features are implemented and maintained in the system. CM applies a level of discipline and control to the processes of system maintenance and modification. CM provides system users with a measure of assurance that the implemented system represents the approved system.
		8-610	Security documentation includes all descriptions of the security features, design descriptions of security-relevant software and hardware, certification packages, and system security plans. The SSP is the basic system protection document and evidence that the proposed system, or update to an existing system, meets the protection profile requirements. The SSP is used throughout the certification and approval process and serves for the lifetime of the system as the formal record of the system and its environment as approved for operation. The SSP also serves as the basis for inspections of the system. Information common to several systems at a facility or information contained in other documents may be attached to or referenced in the SSP.
CM-4	Security Impact Analysis	8-103	See ISSM responsibilities.
		8-104	See ISSO responsibilities.
		8-311	Configuration management (CM) ensures that protection features are implemented and maintained in the system. CM applies a level of discipline and control to the processes of system maintenance and modification. CM provides system users with a measure of assurance that the implemented system represents the approved system.
		8-610	Security documentation includes all descriptions of the security features, design descriptions of security-relevant software and hardware, certification packages, and system security plans. The SSP is the basic system protection document and evidence that the proposed system, or update to an existing system, meets the protection profile requirements. The SSP is used throughout the certification and approval process and serves for the lifetime of the system as the formal record of the system and its environment as approved for operation. The SSP also serves as the basis for inspections of the system. Information common to several systems at a facility or information contained in other documents may be attached to or referenced in the SSP.
CM-5	Access Restrictions for Change	8-311	Configuration management (CM) ensures that protection features are implemented and maintained in the system. CM applies a level of discipline and control to the processes of system maintenance and modification. CM provides system users with a measure of assurance that the implemented system represents the approved system.
		8-610	Security documentation includes all descriptions of the security features, design descriptions of security-relevant software and hardware, certification packages, and system security plans. The SSP is the basic system protection document and evidence that the proposed system, or update to an existing system, meets the protection profile requirements. The SSP is used throughout the certification and approval process and serves for the lifetime of the system as the formal record of the system and its environment as approved for operation. The SSP also serves as the basis for inspections of the system. Information common to several systems at a facility or information contained in other documents may be attached to or referenced in the SSP.
CM-6	Configuration Settings	8-202	The accreditation of an IS is the official management decision to permit operation of an IS in a specified environment at an acceptable level of risk, based on the implementation of a CSA approved set of technical, managerial and procedural safeguards. All IS certifications shall be reviewed and IS accredited to operate by the CSA.

		8-311	Configuration management (CM) ensures that protection features are implemented and maintained in the system. CM applies a level of discipline and control to the processes of system maintenance and modification. CM provides system users with a measure of assurance that the implemented system represents the approved system.
CM-7	Least Functionality	None	
CM-8	Information System Component Inventory	None	
CM-9	Configuration Management Plan	None	
CM-10	Software Usage Restrictions	None	
CM-11	User-Installed Software	None	
Contingency Planning			
CP-1	Contingency Planning Policy and Procedures	8-603	Backup and Restoration of Data (Backup). The regular backup of information is necessary to ensure that users have continuing access to the information. The periodic checking of backup inventory and testing of the ability to restore information validates that the overall backup process is working.
CP-2	Contingency Plan	8-614	Security Testing (Test). Certification and ongoing security testing are the verification of correct operation of the protection measures in a system. The ISSM will perform and document the required tests.
CP-3	Contingency Training	8-615	If disaster recovery planning is contractually mandated, the ISSM will develop a plan that identifies the facility's mission essential applications and information, procedures for the backup of all essential information and software on a regular basis, and testing procedures.
CP-4	Contingency Plan Testing	8-615	If disaster recovery planning is contractually mandated, the ISSM will develop a plan that identifies the facility's mission essential applications and information, procedures for the backup of all essential information and software on a regular basis, and testing procedures.
CP-5	**Withdrawn**		
CP-6	Alternate Storage Site	8-603	Backup and Restoration of Data (Backup). The regular backup of information is necessary to ensure that users have continuing access to the information. The periodic checking of backup inventory and testing of the ability to restore information validates that the overall backup process is working.
CP-7	Alternate Processing Site	8-603	Backup and Restoration of Data (Backup). The regular backup of information is necessary to ensure that users have continuing access to the information. The periodic checking of backup inventory and testing of the ability to restore information validates that the overall backup process is working.
CP-8	Telecommunications Services	8-615	If disaster recovery planning is contractually mandated, the ISSM will develop a plan that identifies the facility's mission essential applications and information, procedures for the backup of all essential information and software on a regular basis, and testing procedures.
CP-9	Information System Backup	8-603	Backup and Restoration of Data (Backup). The regular backup of information is necessary to ensure that users have continuing access to the information. The periodic checking of backup inventory and testing of the ability to restore information validates that the overall backup process is working.

		8-612	System Recovery (SR). System recovery addresses the functions that respond to failures in the SSS or interruptions in operation. Recovery actions ensure that the SSS is returned to a condition where all security-relevant functions are operational or system operation is suspended.
CP-10	Information System Recovery and Reconstitution	8-613	System Assurance (SysAssur). System assurance includes those components of a system (hardware, software, firmware, and communications) that are essential to maintaining the security policy(ies) of the system, (e.g. Security Support Structure).
CP-11	Alternate Communications Protocols	8-601	Alternate Power Source (Power). An alternate power source ensures that the system availability is maintained in the event of a loss of primary power. An APS can also provide a time period for orderly system shutdown or the transfer of system operations to another system or power source.
		8-603	Backup and Restoration of Data (Backup). The regular backup of information is necessary to ensure that users have continuing access to the information. The periodic checking of backup inventory and testing of the ability to restore information validates that the overall backup process is working.
		8-615	If disaster recovery planning is contractually mandated, the ISSM will develop a plan that identifies the facility's mission essential applications and information, procedures for the backup of all essential information and software on a regular basis, and testing procedures.
CP-12	Safe Mode	8-615	If disaster recovery planning is contractually mandated, the ISSM will develop a plan that identifies the facility's mission essential applications and information, procedures for the backup of all essential information and software on a regular basis, and testing procedures.
CP-13	Alternative Security Mechanisms	8-605	Data Transmission (Trans). Information protection is required whenever classified information is to be transmitted through areas or components where individuals not authorized to have access to the information may have unescorted physical or uncontrolled electronic access to the information or communications media (e.g., outside the system perimeter).
		8-607	Identification and Authentication (I&A).
		8-610	Security documentation includes all descriptions of the security features, design descriptions of security-relevant software and hardware, certification packages, and system security plans. The SSP is the basic system protection document and evidence that the proposed system, or update to an existing system, meets the protection profile requirements. The SSP is used throughout the certification and approval process and serves for the lifetime of the system as the formal record of the system and its environment as approved for operation. The SSP also serves as the basis for inspections of the system. Information common to several systems at a facility or information contained in other documents may be attached to or referenced in the SSP.
Identification and Authentication			
IA-1	Identification and Authentication Policy and Procedures	8-607	Identification and Authentication (I&A).
IA-2	Identification and Authentication (Organizational Users)	8-607	Identification and Authentication (I&A).

IA-3	Device Identification and Authentication	8-607	Identification and Authentication (I&A).
IA-4	Identifier Management	8-607	Identification and Authentication (I&A).
IA-5	Authenticator Management	8-607	Identification and Authentication (I&A).
IA-6	Authenticator Feedback	8-607	Identification and Authentication (I&A).
IA-7	Cryptographic Module Authentication	8-607	Identification and Authentication (I&A).
IA-8	Identification and Authentication (Non-Organizational Users)	8-607	Identification and Authentication (I&A).
IA-9	Service Identification and Authentication	8-607	Identification and Authentication (I&A).
IA-10	Adaptive Identification and Authentication	8-607	Identification and Authentication (I&A).
IA-11	Re-authentication	8-607	Identification and Authentication (I&A).
Incident Response			
IR-1	Incident Response Policy and Procedures	8-101	Responsibilities.
		8-103	See ISSM responsibilities.
IR-2	Incident Response Training	8-103	See ISSM responsibilities.
		8-104	See ISSO responsibilities.
IR-3	Incident Response Testing	8-104	See ISSO responsibilities.
IR-4	Incident Handling	1-303	Reports of loss, Compromise, or Suspected Compromise.
		4-218	Inadvertent Release.
IR-5	Incident Monitoring	1-303	Reports of loss, Compromise, or Suspected Compromise.
		4-218	Inadvertent Release.
IR-6	Incident Reporting	1-303	Reports of loss, Compromise, or Suspected Compromise.
		4-218	Inadvertent Release.
IR-7	Incident Response Assistance	None	
IR-8	Incident Response Plan	8-103	See ISSM responsibilities.
		1-302	Reports to be Submitted to the CSA.
IR-9	Information Spillage Response	8-103	See ISSM responsibilities.
IR-10	Integrated Information Security Analysis Team	None	

Maintenance			
MA-1	System Maintenance Policy and Procedures	8-304	Maintenance. IS are particularly vulnerable to security threats during maintenance activities. The level of risk is a factor of the nature of the maintenance person's duties, the security awareness of the employees, and the maintenance person's access to classified information and facilities.
MA-2	Controlled Maintenance	8-304	Maintenance. IS are particularly vulnerable to security threats during maintenance activities. The level of risk is a factor of the nature of the maintenance person's duties, the security awareness of the employees, and the maintenance person's access to classified information and facilities.
MA-3	Maintenance Tools	8-304	Maintenance. IS are particularly vulnerable to security threats during maintenance activities. The level of risk is a factor of the nature of the maintenance person's duties, the security awareness of the employees, and the maintenance person's access to classified information and facilities.
MA-4	Non-local Maintenance	None	
MA-5	Maintenance Personnel	8-304	Maintenance. IS are particularly vulnerable to security threats during maintenance activities. The level of risk is a factor of the nature of the maintenance person's duties, the security awareness of the employees, and the maintenance person's access to classified information and facilities.
MA-6	Timely Maintenance	8-304	Maintenance. IS are particularly vulnerable to security threats during maintenance activities. The level of risk is a factor of the nature of the maintenance person's duties, the security awareness of the employees, and the maintenance person's access to classified information and facilities.
Media Protection			
MP-1	Media Protection Policy and Procedures	8-306	Marking Hardware, Output, and Media. Markings on hardware, output, and media shall conform to Chapter 4 of this manual. If the required marking is impractical or interferes with the operation of the media, the CSA may approve alternate marking procedures.
		8-309	Protection of Media. Media must be protected to the level of accreditation until an appropriate classification review has been conducted.
MP-2	Media Access	8-310	Review of Output and Media.
MP-3	Media Marking	8-306	Marking Hardware, Output, and Media. Markings on hardware, output, and media shall conform to Chapter 4 of this manual. If the required marking is impractical or interferes with the operation of the media, the CSA may approve alternate marking procedures.
		8-310	Review of Output and Media.
MP-4	Media Storage	8-308	Physical Security.
MP-5	Media Transport	8-605	Data Transmission (Trans). Information protection is required whenever classified information is to be transmitted through areas or components where individuals not authorized to have access to the information may have unescorted physical or uncontrolled electronic access to the information or communications media (e.g., outside the system perimeter).
MP-6	Media Sanitization	8-301	Clearing and Sanitization. Instructions on clearing, sanitization and release of IS media shall be issued by the accrediting CSA.
		8-608	Resource Control (ResrcCtrl) The system shall ensure that resources contain no residual data before being assigned, allocated, or reallocated.

MP-7	Media Use	8-306	Marking Hardware, Output, and Media. Markings on hardware, output, and media shall conform to Chapter 4 of this manual. If the required marking is impractical or interferes with the operation of the media, the CSA may approve alternate marking procedures.
		8-310	Review of Output and Media.
MP-8	Media Downgrading	8-310	Review of Output and Media.
Physical and Environmental Protection			
PE-1	Physical and Environmental Protection Policy and Procedures	8-308	Physical Security.
PE-2	Physical Access Authorizations	8-308	Physical Security.
		5-306	Closed Areas. Due to the size and nature of the classified material, or for operational necessity, it may be necessary to construct closed areas for storage because GSA-approved containers or vaults are unsuitable or impractical. Closed areas must be constructed in accordance with section 8 of this chapter. Access to closed areas must be controlled to preclude unauthorized access. This may be accomplished through the use of a cleared person or by a supplanting access control device or system. Access shall be limited to authorized persons who have an appropriate security clearance and a need-to-know for the classified material/information within the area. Persons without the appropriate level of clearance and/or need to know shall be escorted at all times by an authorized person where inadvertent or unauthorized exposure to classified information cannot otherwise be effectively prevented. Closed areas storing TOP SECRET and SECRET material shall be accorded supplemental protection during non-working hours. During non-working hours and during working hours when the area is unattended, admittance to the area shall be controlled by locked entrances and exits secured by either an approved built-in combination lock or an approved combination or key-operated padlock. It is not necessary to activate the supplemental controls during working hours. Doors secured from the inside with a panic bolt (for example, actuated by a panic bar, a dead bolt, a rigid wood or metal bar) or other means approved by the CSA, will not require additional locking devices.
		5-308	Protection of Combinations to Security Containers, Cabinets, Vaults and Closed Areas. Only a minimum number of authorized persons shall have knowledge of combinations to authorized storage containers. Containers shall bear no external markings indicating the level of classified material authorized for storage.
		6-104	Visit Authorization.
PE-3	Physical Access Control	5-300	General. This section describes the uniform requirements for the physical protection of classified material in the custody of contractors. Where these requirements are not appropriate for protecting specific types or forms of classified material, compensatory provisions shall be developed and approved by the CSA. Nothing in this manual shall be construed to contradict or inhibit compliance with the law or building codes. Cognizant security officials shall work to meet appropriate security needs according to the intent of this manual and at acceptable cost.
		6-104	Visit Authorization.

PE-4	Access Control for Transmission Medium	8-605	Data Transmission (Trans). Information protection is required whenever classified information is to be transmitted through areas or components where individuals not authorized to have access to the information may have unescorted physical or uncontrolled electronic access to the information or communications media (e.g., outside the system perimeter).
PE-5	Access Control for Output Devices	8-310	Review of Output and Media.
PE-6	Monitoring Physical Access	5-300	General. This section describes the uniform requirements for the physical protection of classified material in the custody of contractors. Where these requirements are not appropriate for protecting specific types or forms of classified material, compensatory provisions shall be developed and approved by the CSA. Nothing in this manual shall be construed to contradict or inhibit compliance with the law or building codes. Cognizant security officials shall work to meet appropriate security needs according to the intent of this manual and at acceptable cost.
PE-7	**Withdrawn**		
PE-8	Visitor Access Records	None	
PE-9	Power Equipment and Cabling	None	
PE-10	Emergency Shutoff	None	
PE-11	Emergency Power	None	
PE-12	Emergency Lighting	None	
PE-13	Fire Protection	None	
PE-14	Temperature and Humidity Controls	None	
PE-15	Water Damage Protection	None	
PE-16	Delivery and Removal	None	
PE-17	Alternate Work Site	None	
PE-18	Location of Information System Components	None	
PE-19	Information Leakage	None	
PE-20	Asset Monitoring and Tracking	None	
Planning			
		8-101	Responsibilities.
PL-1	Security Planning Policy and Procedures	8-311	Configuration management (CM) ensures that protection features are implemented and maintained in the system. CM applies a level of discipline and control to the processes of system maintenance and modification. CM provides system users with a measure of assurance that the implemented system represents the approved system.
PL-2	System Security Plan	8-311	Configuration management (CM) ensures that protection features are implemented and maintained in the system. CM applies a level of discipline and control to the processes of system maintenance and modification. CM provides system users with a measure of assurance that the implemented system represents the approved system.

		8-610	Security documentation includes all descriptions of the security features, design descriptions of security-relevant software and hardware, certification packages, and system security plans. The SSP is the basic system protection document and evidence that the proposed system, or update to an existing system, meets the protection profile requirements. The SSP is used throughout the certification and approval process and serves for the lifetime of the system as the formal record of the system and its environment as approved for operation. The SSP also serves as the basis for inspections of the system. Information common to several systems at a facility or information contained in other documents may be attached to or referenced in the SSP.
PL-3	**Withdrawn**		
PL-4	Rules of Behavior	8-103	See ISSM responsibilities.
PL-5	**Withdrawn**		
PL-6	**Withdrawn**		
PL-7	Security Concept of Operations	8-610	Security documentation includes all descriptions of the security features, design descriptions of security-relevant software and hardware, certification packages, and system security plans. The SSP is the basic system protection document and evidence that the proposed system, or update to an existing system, meets the protection profile requirements. The SSP is used throughout the certification and approval process and serves for the lifetime of the system as the formal record of the system and its environment as approved for operation. The SSP also serves as the basis for inspections of the system. Information common to several systems at a facility or information contained in other documents may be attached to or referenced in the SSP.
PL-8	Information Security Architecture	None	
PL-9	Central Management	None	
Personnel Security			
PS-1	Personnel Security Policy and Procedures	8-307	Personnel Security. Personnel with system access play an integral role in protecting information; defining their system security policies; and maintaining and monitoring the confidentiality, integrity, and availability attributes that are inherent within their IS. Duties, responsibilities, privileges, and specific limitations of IS users, both general and privileged, shall be specified in writing. So far as feasible, security duties shall be distributed to preclude any one individual from adversely affecting operations or the integrity of the system. Protection levels for particular IS shall be determined by the clearance level, formal access approvals, and need-to-know held by users of the IS, and the classification level of data processed or stored.
PS-2	Position Risk Designation	8-307	Personnel Security. Personnel with system access play an integral role in protecting information; defining their system security policies; and maintaining and monitoring the confidentiality, integrity, and availability attributes that are inherent within their IS. Duties, responsibilities, privileges, and specific limitations of IS users, both general and privileged, shall be specified in writing. So far as feasible, security duties shall be distributed to preclude any one individual from adversely affecting operations or the integrity of the system. Protection levels for particular IS shall be determined by the clearance level, formal access approvals, and need-to-know held by users of the IS, and the classification level of data processed or stored.
PS-3	Personnel Screening	8-103	See ISSM responsibilities.

		8-104	See ISSO responsibilities.
		8-307	Personnel Security. Personnel with system access play an integral role in protecting information; defining their system security policies; and maintaining and monitoring the confidentiality, integrity, and availability attributes that are inherent within their IS. Duties, responsibilities, privileges, and specific limitations of IS users, both general and privileged, shall be specified in writing. So far as feasible, security duties shall be distributed to preclude any one individual from adversely affecting operations or the integrity of the system. Protection levels for particular IS shall be determined by the clearance level, formal access approvals, and need-to-know held by users of the IS, and the classification level of data processed or stored.
PS-4	Personnel Termination	8-303	Identification and Authentication Management. As the complexity of a specific IS and the associated residual risk for this system increase, the need for identification and authentication of users and process becomes more significant. Identification and authentication controls are required to ensure that users have the appropriate clearances and need-to-know for the information on a particular system and shall be managed in accordance with procedures identified in the SSP.
		5-309	Changing Combinations.
PS-5	Personnel Transfer	8-303	Identification and Authentication Management. As the complexity of a specific IS and the associated residual risk for this system increase, the need for identification and authentication of users and process becomes more significant. Identification and authentication controls are required to ensure that users have the appropriate clearances and need-to-know for the information on a particular system and shall be managed in accordance with procedures identified in the SSP.
		5-309	Changing Combinations.
PS-6	Access Agreements	8-103	See ISSM responsibilities.
		8-104	See ISSO responsibilities.
		8-105	Users of IS. Users of IS are either privileged or general users.
PS-7	Third-Party Personnel Security	8-304	Maintenance. IS are particularly vulnerable to security threats during maintenance activities. The level of risk is a factor of the nature of the maintenance person's duties, the security awareness of the employees, and the maintenance person's access to classified information and facilities.
PS-8	Personnel Sanctions	1-304	Individual Culpability Reports. Contractors shall establish and enforce policies that provide for appropriate administrative actions taken against employees who violate requirements of this Manual.
Risk Assessment			
RA-1	Risk Assessment Policy and Procedures	8-610	Security documentation includes all descriptions of the security features, design descriptions of security-relevant software and hardware, certification packages, and system security plans. The SSP is the basic system protection document and evidence that the proposed system, or update to an existing system, meets the protection profile requirements. The SSP is used throughout the certification and approval process and serves for the lifetime of the system as the formal record of the system and its environment as approved for operation. The SSP also serves as the basis for inspections of the system. Information common to several systems at a facility or information contained in other documents may be attached to or referenced in the SSP.

RA-2	Security Categorization	8-402	The protection level of an IS is determined by the relationship between two parameters: first, the clearance levels, formal access approvals, and need-to-know of users; and second, the level of concern based on the classification of the data on a particular system. The protection level translates into a set of requirements (Tables 5, 6, and 7) that must be implemented in the resulting system. Table 4 presents the criteria for determining the following three protection levels for confidentiality.
RA-3	Risk Assessment	8-402	The protection level of an IS is determined by the relationship between two parameters: first, the clearance levels, formal access approvals, and need-to-know of users; and second, the level of concern based on the classification of the data on a particular system. The protection level translates into a set of requirements (Tables 5, 6, and 7) that must be implemented in the resulting system. Table 4 presents the criteria for determining the following three protection levels for confidentiality.
RA-4	**Withdrawn**		
RA-5	Vulnerability Scanning	8-614	Security Testing (Test). Certification and ongoing security testing are the verification of correct operation of the protection measures in a system. The ISSM will perform and document the required tests.
RA-6	Technical Surveillance Countermeasures Survey	None	
System and Services Acquisition			
SA-1	System and Services Acquisition Policy and Procedures	None	
SA-2	Allocation of Resources	8-100	General Responsibilities and Duties.
		8-200	The Certification and Accreditation (C&A) process is an integral part of the life cycle of an IS. The identification of protection measures occurs during system design or development. The formal C&A occurs after the protection measures have been implemented and any required IS protection documentation has been approved. Certification validates that the protection measures described in the SSP have been implemented on the system and that the protection measures are functioning properly. Accreditation is the approval by the CSA for the system to process classified information.
SA-3	System Development Life Cycle	8-311	Configuration management (CM) ensures that protection features are implemented and maintained in the system. CM applies a level of discipline and control to the processes of system maintenance and modification. CM provides system users with a measure of assurance that the implemented system represents the approved system.
		8-610	Security documentation includes all descriptions of the security features, design descriptions of security-relevant software and hardware, certification packages, and system security plans. The SSP is the basic system protection document and evidence that the proposed system, or update to an existing system, meets the protection profile requirements. The SSP is used throughout the certification and approval process and serves for the lifetime of the system as the formal record of the system and its environment as approved for operation. The SSP also serves as the basis for inspections of the system. Information common to several systems at a facility or information contained in other documents may be attached to or referenced in the SSP.

SA-4	Acquisition Process	8-302	Examination of Hardware and Software. IS hardware and software shall be examined when received from the vendor and before being placed into use.
		8-613	Examination of Hardware and Software. IS hardware and software shall be examined when received from the vendor and before being placed into use.
SA-5	Information System Documentation	8-202	The accreditation of an IS is the official management decision to permit operation of an IS in a specified environment at an acceptable level of risk, based on the implementation of a CSA approved set of technical, managerial and procedural safeguards. All IS certifications shall be reviewed and IS accredited to operate by the CSA.
		8-302	Examination of Hardware and Software. IS hardware and software shall be examined when received from the vendor and before being placed into use.
		8-610	Security documentation includes all descriptions of the security features, design descriptions of security-relevant software and hardware, certification packages, and system security plans. The SSP is the basic system protection document and evidence that the proposed system, or update to an existing system, meets the protection profile requirements. The SSP is used throughout the certification and approval process and serves for the lifetime of the system as the formal record of the system and its environment as approved for operation. The SSP also serves as the basis for inspections of the system. Information common to several systems at a facility or information contained in other documents may be attached to or referenced in the SSP.
SA-6	**Withdrawn**		
SA-7	**Withdrawn**		
SA-8	Security Engineering Principles	8-311	Configuration management (CM) ensures that protection features are implemented and maintained in the system. CM applies a level of discipline and control to the processes of system maintenance and modification. CM provides system users with a measure of assurance that the implemented system represents the approved system.
SA-9	External Information System Services	8-700	Interconnected Systems Management. The characteristics and capabilities of an IS implemented as networks require special security considerations. This section states additional requirements on a network or expands on the security requirements stated in Section 6 as they apply to a network.
SA-10	Developer Configuration Management	8-613	System Assurance (SysAssur). System assurance includes those components of a system (hardware, software, firmware, and communications) that are essential to maintaining the security policy(ies) of the system, (e.g. Security Support Structure).
SA-11	Developer Security Testing and Evaluation	8-302	Examination of Hardware and Software. IS hardware and software shall be examined when received from the vendor and before being placed into use.
SA-12	Supply Chain Protection	None	
SA-13	Trustworthiness	8-302	Examination of Hardware and Software. IS hardware and software shall be examined when received from the vendor and before being placed into use.
		8-311	Configuration management (CM) ensures that protection features are implemented and maintained in the system. CM applies a level of discipline and control to the processes of system maintenance and modification. CM provides system users with a measure of assurance that the implemented system represents the approved system.
SA-14	Criticality Analysis	None	

SA-15	Development Process, Standards, and Tools	None	
SA-16	Developer-Provided Training	None	
SA-17	Developer Security Architecture and Design	None	
SA-18	Tamper Resistance and Detection	8-308	Physical Security.
SA-19	Component Authenticity	8-302	Examination of Hardware and Software. IS hardware and software shall be examined when received from the vendor and before being placed into use.
SA-20	Customized Development of Critical Components	None	
SA-21	Developer Screening	None	
SA-22	Unsupported System Components	8-302	Examination of Hardware and Software. IS hardware and software shall be examined when received from the vendor and before being placed into use.
System and Communications Protection			
SC-1	System and Communications Protection Policy and Procedures	8-101	Responsibilities
		8-605	Data Transmission (Trans). Information protection is required whenever classified information is to be transmitted through areas or components where individuals not authorized to have access to the information may have unescorted physical or uncontrolled electronic access to the information or communications media (e.g., outside the system perimeter).
SC-2	Application Partitioning	None	
SC-3	Security Function Isolation	8-105	Users of IS. Users of IS are either privileged or general users.
SC-4	Information in Shared Resources	8-609	Session Controls (SessCtrl).
SC-5	Denial of Service Protection	8-701	Controlled Interface Functions.
SC-6	Resource Availability	None	
SC-7	Boundary Protection	8-701	Controlled Interface Functions.
SC-8	Transmission Confidentiality and Integrity	8-605	Data Transmission (Trans). Information protection is required whenever classified information is to be transmitted through areas or components where individuals not authorized to have access to the information may have unescorted physical or uncontrolled electronic access to the information or communications media (e.g., outside the system perimeter).
SC-9	**Withdrawn**		
SC-10	Network Disconnect	8-609	Session Controls (SessCtrl).
SC-11	Trusted Path	None	

SC-12	Cryptographic Key Establishment and Management	None	
SC-13	Cryptographic Protection	9-400	This section was prepared by the National Security Agency. The procedures in this section pertaining to COMSEC information shall apply to contractors when the contractor requires the use of COMSEC systems in the performance of a contract; the contractor is required to install, maintain, or operate COMSEC equipment for the U.S. Government; or the contractor is required to accomplish research, development, or production of COMSEC systems, COMSEC equipment, or related COMSEC material.
SC-14	**Withdrawn**		
SC-15	Collaborative Computing Devices	None	
SC-16	Transmission of Security Attributes	8-700	Interconnected Systems Management. The characteristics and capabilities of an IS implemented as networks require special security considerations. This section states additional requirements on a network or expands on the security requirements stated in Section 6 as they apply to a network.
SC-17	Public Key Infrastructure Certificates	8-303	Identification and Authentication Management. As the complexity of a specific IS and the associated residual risk for this system increase, the need for identification and authentication of users and process becomes more significant. Identification and authentication controls are required to ensure that users have the appropriate clearances and need-to-know for the information on a particular system and shall be managed in accordance with procedures identified in the SSP.
SC-18	Mobile Code	None	
SC-19	Voice Over Internet Protocol	8-700	Interconnected Systems Management. The characteristics and capabilities of an IS implemented as networks require special security considerations. This section states additional requirements on a network or expands on the security requirements stated in Section 6 as they apply to a network.
SC-20	Secure Name /Address Resolution Service	None	
SC-21	Secure Name /Address Resolution Service	None	
SC-22	Architecture and Provisioning for Name / Address Resolution Service	None	
SC-23	Session Authenticity	8-609	Session Controls (SessCtrl).
SC-24	Fail in Known State	8-702	Controlled Interface Requirements.
SC-25	Thin Nodes	8-613	System Assurance (SysAssur). System assurance includes those components of a system (hardware, software, firmware, and communications) that are essential to maintaining the security policy(ies) of the system, (e.g. Security Support Structure).
SC-26	Honeypots	None	
SC-27	Platform-Independent Applications	None	

SC-28	Protection of Information at Rest	8-604	Changes to Data (Integrity). The control of changes to data includes deterring, detecting, and reporting of successful and unsuccessful attempts to change data. Control of changes to data may range from simply detecting a change attempt to the ability to ensure that only authorized charges are allowed.
SC-29	Heterogeneity	None	
SC-30	Concealment and Misdirection	None	
SC-31	Covert Channel Analysis	None	
SC-32	Information System Partitioning	None	
SC-33	**Withdrawn**		
SC-34	Non-Modifiable Executable Programs	8-302	Examination of Hardware and Software. IS hardware and software shall be examined when received from the vendor and before being placed into use.
		8-304	Maintenance. IS are particularly vulnerable to security threats during maintenance activities. The level of risk is a factor of the nature of the maintenance person's duties, the security awareness of the employees, and the maintenance person's access to classified information and facilities.
		8-311	Configuration management (CM) ensures that protection features are implemented and maintained in the system. CM applies a level of discipline and control to the processes of system maintenance and modification. CM provides system users with a measure of assurance that the implemented system represents the approved system.
SC-35	Honey clients	None	
SC-36	Distributed Processing and Storage	None	
SC-37	Out-of-Band Channels	None	
SC-38	Operations Security	None	
SC-39	Process Isolation	None	
SC-40	Wireless Link Protection	None	
SC-41	Port and I/O Device Access	None	
SC-42	Sensor Capability and Data	None	
SC-43	Usage Restrictions	None	
SC-44	Detonation Chambers	None	
System and Information Integrity			
SI-1	System and Information Integrity Policy and Procedures	8-101	Responsibilities
SI-2	Flaw Remediation	8-311	Configuration management (CM) ensures that protection features are implemented and maintained in the system. CM applies a level of discipline and control to the processes of system maintenance and modification. CM provides system users with a measure of assurance that the implemented system represents the approved system.

		8-610	Security documentation includes all descriptions of the security features, design descriptions of security-relevant software and hardware, certification packages, and system security plans. The SSP is the basic system protection document and evidence that the proposed system, or update to an existing system, meets the protection profile requirements. The SSP is used throughout the certification and approval process and serves for the lifetime of the system as the formal record of the system and its environment as approved for operation. The SSP also serves as the basis for inspections of the system. Information common to several systems at a facility or information contained in other documents may be attached to or referenced in the SSP.
SI-3	Malicious Code Protection	8-305	Malicious Code. Policies and procedures to detect and deter incidents caused by malicious code, such as viruses or unauthorized modification to software, shall be implemented. All files must be checked for viruses before being introduced on an IS and checked for other malicious code as feasible. The use of personal or public domain software is strongly discouraged. Each installation of such software must be approved by the ISSM.
SI-4	Information System Monitoring	8-602	Audit Capability. Security auditing involves recognizing, recording, storing, and analyzing information related to security-relevant activities. The audit records can be used to determine which activities occurred and which user or process was responsible for them.
SI-5	Security Alerts, Advisories, and Directives	8-103	See ISSM responsibilities.
SI-6	Security Function Verification	8-613	System Assurance (SysAssur). System assurance includes those components of a system (hardware, software, firmware, and communications) that are essential to maintaining the security policy(ies) of the system, (e.g. Security Support Structure).
SI-7	Software, Firmware, and Information Integrity	8-302	Examination of Hardware and Software. IS hardware and software shall be examined when received from the vendor and before being placed into use.
SI-8	Spam Protection	8-302	Examination of Hardware and Software. IS hardware and software shall be examined when received from the vendor and before being placed into use.
SI-9	**Withdrawn**		
SI-10	Information Input Validation	None	
SI-11	Error Handling	None	
SI-12	Information Handling and Retention	None	
SI-13	Predictable Failure Prevention	None	
SI-14	Non-Persistence	None	
SI-15	Information Output Filtering	None	
SI-16	Memory Protection	None	
SI-17	Fail-Safe Procedures	None	

NISPOM to NIST (800-53r4) Security Control Mapping

Program Management			
PM-1	Information Security Program Plan	8-100	General Responsibilities and Duties.
PM-2	Senior Information Security Officer	8-101	Responsibilities.
PM-3	Information Security Resources	None	
PM-4	Plan of Action and Milestones Process	8-311	Configuration management (CM) ensures that protection features are implemented and maintained in the system. CM applies a level of discipline and control to the processes of system maintenance and modification. CM provides system users with a measure of assurance that the implemented system represents the approved system.
PM-5	Information System Inventory	8-311	Configuration management (CM) ensures that protection features are implemented and maintained in the system. CM applies a level of discipline and control to the processes of system maintenance and modification. CM provides system users with a measure of assurance that the implemented system represents the approved system.
PM-6	Information Security Measures of Performance	8-311	Configuration management (CM) ensures that protection features are implemented and maintained in the system. CM applies a level of discipline and control to the processes of system maintenance and modification. CM provides system users with a measure of assurance that the implemented system represents the approved system.
PM-7	Enterprise Architecture	8-103	See ISSM responsibilities.
PM-8	Critical Infrastructure Plan	8-104	See ISSO responsibilities.
PM-9	Risk Management Strategy	8-103	See ISSM responsibilities.
PM-10	Security Authorization Process	8-303	Identification and Authentication Management. As the complexity of a specific IS and the associated residual risk for this system increase, the need for identification and authentication of users and process becomes more significant. Identification and authentication controls are required to ensure that users have the appropriate clearances and need-to-know for the information on a particular system and shall be managed in accordance with procedures identified in the SSP.
PM-11	Mission/Business Process Definition	8-303	Identification and Authentication Management. As the complexity of a specific IS and the associated residual risk for this system increase, the need for identification and authentication of users and process becomes more significant. Identification and authentication controls are required to ensure that users have the appropriate clearances and need-to-know for the information on a particular system and shall be managed in accordance with procedures identified in the SSP.
PM-12	Insider Threat Program	None	
PM-13	Information	8-103	See ISSM responsibilities.

	Security Workforce	8-307	Personnel Security. Personnel with system access play an integral role in protecting information; defining their system security policies; and maintaining and monitoring the confidentiality, integrity, and availability attributes that are inherent within their IS. Duties, responsibilities, privileges, and specific limitations of IS users, both general and privileged, shall be specified in writing. So far as feasible, security duties shall be distributed to preclude any one individual from adversely affecting operations or the integrity of the system. Protection levels for particular IS shall be determined by the clearance level, formal access approvals, and need-to-know held by users of the IS, and the classification level of data processed or stored.
PM-14	Testing, Training, and Monitoring	8-302	Examination of Hardware and Software. IS hardware and software shall be examined when received from the vendor and before being placed into use.
PM-15	Contacts with Security Groups and Associations	8-101	Responsibilities.
PM-16	Threat Awareness Program	8-103	See ISSM responsibilities.

Abbreviations

Abbreviation	Description
AC	Access Controls
AT	Awareness and Training
C&A	Certification and Accreditation
CI	Controlled Interface
CM	Configuration management
CP	Contingency Planning
CSA	Cognizant Security Activity
FSO	Facility Security Officer
I&A	Identification and Authentication
I/O	Input/Output
IA	Identification and Authentication
IS	Information System
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
MA	Maintenance
MP	Media Protection
NAO	NISP Authorization Office
NISP	National Industrial Security Program
NISPOM	National Industrial Security Program Operating Manual
NIST	National Institute of Standards and Technology
PE	Physical and Environmental Protection
PL	Planning
PM	Program Management
PS	Personnel Security
RA	Risk Assessment
ResrcCtrl	Resource Control
RMF	Risk Management Framework
SessCtrl	Session Controls
SR	System Recovery
SSP	System Security Plan
SysAssur	System Assurance
Trans	Data Transmission

END OF DOCUMENT