Defense Security Service

Industrial Security Field Operations

National Industrial Security Program Authorization Office

Defense Security Service (DSS) Assessment and Authorization Process Manual (DAAPM)

Version 1.3

June 4, 2018

EXECUTIVE SUMMARY

The policy of the U.S. Government is that all classified information must be appropriately safeguarded to assure the confidentiality of that information, as well as the integrity and availability of that information when required by contract. This Defense Security Service (DSS) Assessment and Authorization Process Manual (DAAPM) is intended for use by cleared contractors participating in the National Industrial Security Program (NISP). It provides standardized security policies and procedures for use in safeguarding classified information processed by cleared contractors' Information Systems (ISs) operating under the security cognizance of the DSS.

Federal agencies, to include the Department of Defense (DoD), Special Access Program (SAP), and Intelligence communities, are adopting common guidelines to streamline and build reciprocity into the Assessment and Authorization process, formerly known as Certification and Accreditation (C&A). The DAAPM transitions the DSS C&A processes to the Risk Management Framework (RMF) made applicable to cleared contractors by DoD 5220.22-M, Change 2, *National Industrial Security Program Operating Manual (NISPOM),* issued on May 18, 2016. The DAAPM implements RMF processes and guidelines from the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*, NIST SP 800-53, Version 4, *Recommended Security and Privacy Controls for Federal Information Systems and Organizations*, NIST SP 800-53A, Revision 4, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*, the *Committee on National Security Systems (CNSS) Instruction No. 1253*, *Security Categorization and Control Selection for National Security Systems*, and Committee on National Security Systems Directive (CNSSD) 504, *Directive on Protecting National Security Systems From Insider Threat*. The DAAPM also incorporates Insider Threat minimum requirements defined in the NISPOM, which are consistent with the requirements of Executive Order (E.O.) 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing of Classified Information*, and the Presidential Memorandum, *National Insider Threat Policy and Minimum Standards for Executive Branch Threat Programs*. Changes to these core documents will be incorporated through the Change Management Process outlined in Section 2 of this manual.

This process manual is not intended to be relied upon or construed to create any right or benefit, substantive or procedural, enforceable at law against the United States, its agencies, officers or employees. The Federal Government reserves the right and has the obligation to impose any security method, safeguard, or restriction it believes necessary to verify that unauthorized access to classified information is effectively precluded and that performance of classified contracts is not adversely affected.

Table of Contents

1 INTRODUCTION

1.1 Background

Federal agencies have adopted the NIST RMF as a common set of guidelines for the Assessment and Authorization of Information Systems (ISs). In an effort to streamline and build reciprocity into the DSS processes, DSS is adopting these standards as well, so that all cleared contractor ISs that process classified information as part of the NISP are authorized under the RMF Assessment and Authority process. The RMF focuses on a more holistic and strategic process for the risk management of ISs, and on processes and procedures designed to develop trust across the Federal Government. Implementation of the RMF provides organizations with a disciplined, structured, flexible, and repeatable process for managing risk related to the operation and use of ISs.

To enable information sharing within the Federal Government, the NIST has a statutory responsibility to develop minimum requirements for the secure operation of ISs processing classified information, to include Assessment and Authorization processes. DSS is ensuring that its policies and procedures comply with these standards, and that they align with the Federal Government's approach to IS security and the protection of information associated with classified contracts under the NISP.

1.2 Applicability and Reciprocity

Cleared contractors processing classified information under the cognizance of DSS will follow the guidance contained within this manual to complete the RMF process and obtain IS authorization. DSS will Assess and Authorize SAP information systems in accordance with the Joint Special Access Program (JSAP) Implementation Guide (JSIG) when directed by contractual requirements. If contractual guidance is not provided, DSS will apply the DAAPM.

Reciprocity, as defined in CNSSI 4009, is a, "Mutual agreement among participating enterprises to accept each other's security assessments in order to reuse IS resources and/or to accept each other's assessed security posture in order to share information." This does not imply blind acceptance. The body of evidence used for assessments of the subject system will be provided to the other participants who have a vested interest in establishing a mutual agreement. The receiving party will review the assessment evidence to determine the security posture of the IS and identify items that may require negotiations. Only security controls or test items that were initially omitted are subject to evaluation/testing to assure the system meets all requirements for a successful reciprocal agreement.

1.3 References

In addition to this process manual, key documents supporting the assessment and authorization of classified ISs under DSS cognizance include:

- DoD 5220.22-M Change-2, National Industrial Security Program Operating Manual (NISPOM)
- NIST Special Publications (SP):
    - NIST SP 800-30, Guide for Conducting Risk Assessments

- NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal ISs
- NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View
- NIST SP 800-53, Rev 4, Recommended Security Controls for Federal Information Systems and Organizations
- NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans

- CNSSI 1253, Security Categorization and Control Selection for National Security Systems
- CNSSD 504, Directive on Protecting National Security Systems From Insider Threat

Additional references pertaining to this document can be found in Appendix M.

1.4 Changes in Terminology

The below table provides a mapping between terms previously associated with C&A activities and new terms adopted under RMF.

Table 1 Terminology Changes

Old Term	New Term
Certification and Accreditation (C&A) Process	Assessment and Authorization
Certification	Assessment
Accreditation	Authorization
Requirements (Security or Identification and Authentication (IA))	Security Controls
Protection Level (PL)	Security Categorization
Level of Concern	Impact Level
Self-Certification	Type Authorization
IS Profile	System Security Plan (SSP)
Designated Approving Authority (DAA)	Authorizing Official (AO)
IS Security Professional (ISSP)	ISSP/Security Control Assessor (SCA)
Customer, Government Contracting Authority (GCA), etc.	Information Owner (IO)
Program Manager (PM)	Information System Owner (ISO*)
Guest System	Federal Information System
Trusted Download	Assured File Transfer (AFT)
Disestablishment of an IS	IS Decommissioning Strategy
*PM and ISO terms are used interchangeably	

2 CHANGE MANAGEMENT PROCESS

The DAAPM is a living document to be updated bi-annually with each proposed change receiving individual consideration as to its implementation guidance and timelines. The DSS NISP Authorization Office (NAO) has overall responsibility for content management of the DAAPM; however, this is accomplished through a change management process involving one member from the NISP Administration and Policy Analysis (NAPA) and one industry representative from the NISP Information Systems Authorization (NISA) Working Group. This group is referred to as the Configuration Management Team (CMT). Changes to the DAAPM must be aligned to, and consistent with, the NIST and CNSS processes for the security of information systems processing classified information.

The CMT's purpose is to evaluate proposed changes, review existing implementation guidance, and develop implementation and transition guidance for NISP cleared contractors under DSS cognizance. CMT members are responsible for collecting, prioritizing, and determining the priority of proposed changes from their respective communities. Topics for consideration include, but are not limited to: security control requirements, implementation, testing, and validation, as well as security assessment and system authorization processes.

The CMT conducts quarterly review boards to introduce new items for consideration, review previously identified proposals, and make final adjudication decisions on proposed changes to the Process Manual. As changes are accepted and implemented, the CMT lead annotates the details of the changes in the DAAPM change log, which is a permanent part of the DAAPM. CMT members may request ad-hoc meetings as required to address high priority issues, and items recognized by all parties as administrative in nature may be worked through email channels for immediate implementation upon CMT approval. The NAO has final approval authority for all changes to the DAAPM.

Understanding that the DAAPM is a living document, the final security related requirements for each IS are those identified in the DSS approved System Security Plan (SSP). DSS personnel use the SSP as the document from which to evaluate the system requirements during IS Assessment and Authorization efforts and Security Vulnerability Assessments (SVAs). Figure 1 shows the flow of changes into the DAAPM.

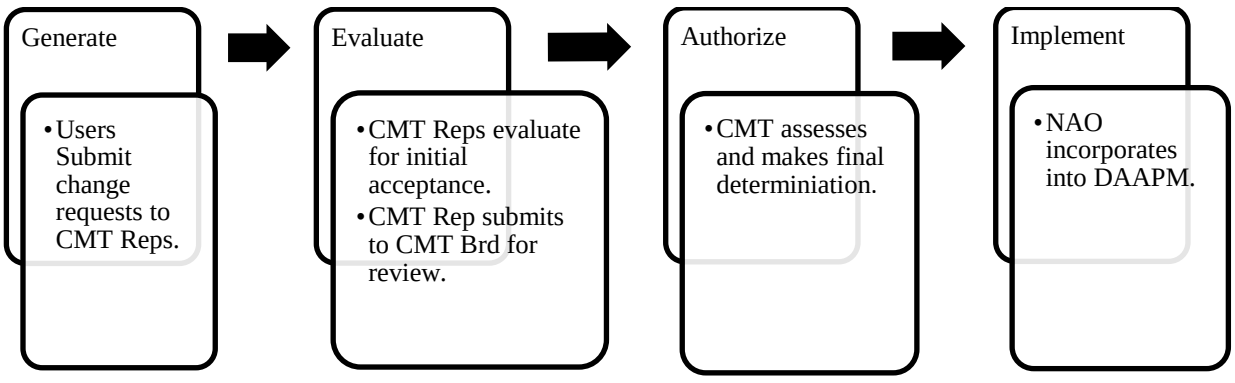

Figure 1 DAAPM Change Management Flow

3 ROLES AND RESPONSIBILITIES

The roles and responsibilities of the personnel involved with the RMF are summarized in the paragraphs below.

3.1 Authorizing Official (AO)

The AO is the senior official or executive with the authority to formally assume responsibility for operating an IS at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and national security. Responsibilities of the AO include, but are not limited to:

a. Ensuring each IS is properly assessed and authorized based on its environment of operation, security impact levels, and required security controls.

b. Evaluating threats and vulnerabilities to ISs to ascertain the need for additional safeguards.

c. Issuing security authorization decisions.

d. Verifying records are maintained for all IS authorizations under his/her purview.

e. Confirming IS security is an element of the life cycle process.

f. Ensuring guidance and support related to the secure operation of IS is provided to cleared contractor personnel as necessary.

g. Coordinating cyber incident responses related to classified ISs.

h. Reviewing and approving Interconnection Security Agreement (ISA)/Memorandum of Understanding or Agreements (MOU/A) associated with IS processing classified information.

3.2 Security Control Assessor (SCA)

The SCA is an ISSP appointed by the AO to act on their behalf in the oversight of cleared contractors' ISs processing classified information. Responsibilities of the SCA include, but are not limited to:

a. Conducting a comprehensive assessment of the management, operational, and technical security controls employed within or inherited by an IS to determine the overall effectiveness of the controls.

b. Reviewing Risk Assessment Reports (RARs) and providing feedback to the Information System Security Manager (ISSM) regarding the completeness of the risk assessment and appropriateness of planned safeguards.

c. Assessing the severity of any weaknesses or deficiencies discovered in the IS and its environment of operation, and recommending corrective actions to address identified vulnerabilities.

d. Providing advice and assistance, as needed.

e. Evaluating threats and vulnerabilities to ISs to ascertain the need for additional safeguards.

f. Ensuring security assessments are completed for each IS.

g. Preparing the final Security Assessment Report (SAR), which contains the results and vulnerabilities at the conclusion of each security assessment.

h. Reviewing Plans of Action and Milestones (POA&Ms) to ensure weaknesses are identified, effective/acceptable mitigation strategies are planned, and timelines are acceptable and on track.

i. Developing security authorization package and providing risk-based recommendations to the AO.

j. Assessing proposed changes to ISs, their environment of operation, and mission needs that could affect system authorization.

3.3 Common Control Provider (CCP)

A CCP is an individual, group, or organization responsible for the development, implementation, assessment, and monitoring of common controls (e.g., security controls inherited by ISs). Responsibilities of the CCP include, but are not limited to:

a. Documenting the common controls in an SSP.

b. Ensuring that assessments of common controls are carried out as required.

c. Documenting assessment vulnerabilities.

d. Providing SSPs, POA&Ms, and SARs associated with common controls to the ISSMs inheriting those controls.

3.4 Information Owner (IO)

An IO is an organizational official with statutory, management, or operational authority for specific information. The IO position is occupied by a government employee with capital investment authority. A single IS may contain information from multiple IOs. Responsibilities of the IO include, but are not limited to:

a. Establishing the policies and procedures governing generation, collection, processing, dissemination, and disposal of classified information.

b. Establishing the rules for appropriate use and protection of the subject information (e.g., DD Form 254 and Security Classification Guide (SCG)); retains that responsibility even when the information is shared with or provided to other organizations in information sharing environments.

c. Providing sensitivity of information under the ISO's purview.

d. Retaining risk assumption responsibilities for their organization.

e. Providing Confidentiality, Integrity, and Availability (CIA) Security Impact Levels associated with the IO's data when contractual requirements differ from the DSS baseline or if concern is raised based on the RAR.

f. Providing concurrence when the categorization deviates from the DSS baseline of Moderate-Low-Low (M-L-L).

g. Providing unique requirements for managing the IO's data (e.g., incident response, information contamination to other systems/media, unique audit requirements, etc.).

h. Providing handling requirements.

3.5 Information System Owner (ISO)

The ISO (e.g., cleared contractor Program Manager) is primarily responsible for managing system development, operations, and maintenance at the program level. The ISO oversees the overall procurement, development, integration, modification, operation and maintenance of an IS. Responsibilities of the ISO include:

a. Ensuring that the planning and execution of all RMF activities are aligned, integrated with, and supportive of the system acquisition process.

b. Establishing data ownership and responsibilities for each IS.

c. Verifying program specific requirements (e.g., accountability, access, and special handling) are enforced.

d. Overseeing the development, maintenance, and tracking of the SSP.

e. Ensuring the system is deployed and operated according to the agreed-upon security requirements.

f. Appointing IS user and determining access rights.

g. Planning and budgeting for adequate on-site information security resources.

h. Enforcing training requirements for individuals participating in the RMF.

3.6 Information System Security Manager (ISSM)

The cleared contractor will appoint an employee as the ISSM. The ISSM must be a U.S. citizen. The ISSM is primarily responsible for maintaining the overall security posture of the systems within their organization, and are accountable for the implementation of the RMF. The ISSM serves as the principal advisor on all matters, technical and otherwise, involving the security of ISs under their purview. Responsibilities of an ISSM include, but are not limited to:

a. Developing, maintaining, and overseeing the IS security program and policies for their assigned area of responsibility.

b. Ensuring compliance with current Cyber Security policies, concepts, and measures when designing, procuring, adopting, and developing new IS.

c. Ensuring the fulfillment of IO data requirements (e.g., storage, processing, AFT, incident response, collection, dissemination, and disposal)

d. Developing and implementing an effective IS security education, training, and awareness program.

e. Maintaining a working knowledge of system functions, security policies, technical security safeguards, and operational security measures.

f. Possessing sufficient experience, commanding adequate resources, and being organizationally aligned to ensure prompt support and successful execution of a robust IS security program.

g. Completing training identified in ISSM Required Training Table within one year of appointment.

h. Monitoring all available resources that provide warnings of system vulnerabilities or ongoing attacks and reporting them as necessary.

i. Developing, documenting, and monitoring compliance with and reporting of the cleared contractor facility's IS's security program in accordance with Cognizant Security Activity (CSA)-provided guidelines for management, operational, and technical controls.

j. Performing risk assessments and documenting results in a RAR and keeping the risk assessment current throughout the acquisition/development portion of the IS life cycle.

k. Producing/Developing security documentation (e.g., SSP, POA&M, and supporting artifacts, etc.).

l. Developing, maintaining, and updating POA&Ms in order to identify IS weaknesses, mitigating actions, resources, and timelines for corrective actions; entries in the POA&Ms will be based on vulnerabilities and recommendations identified during assessments.

m. Submitting the SSP and supporting artifacts to the ISSP for AO review and consideration.

n. Certifying to the AO, in writing, each SSP has been implemented; the specified security controls are in place and properly tested; and the IS continues to function as described in the SSP.

o. Ensuring all IS security-related documentation is current and accessible to properly authorized individuals.

p. Implementing security controls that protect the IS during development.

q. Maintaining the SSP in accordance with the agreed-upon security controls.

r. Ensuring audit records are collected and analyzed in accordance with the SSP.

s. Coordinating IS authorizations with the ISSP and AO.

t. Maintaining a repository of all security authorizations for IS under their purview.

u. Managing, maintaining, and executing the Continuous Monitoring Strategy.

v. Conducting periodic assessments of authorized ISs and ensuring corrective actions are taken for all identified findings and vulnerabilities.

w. Monitoring system recovery processes to ensure security features and procedures are properly restored and functioning correctly.

x. Ensuring configuration management policies and procedures are followed.

y. Assessing changes to an IS that could affect the authorization.

z. Verifying enhancements to existing systems provide equal or improved security features and safeguards.

aa. Ensuring approved procedures are used for sanitizing and releasing system components and media.

bb. Ensuring proper measures are taken when an IS incident or vulnerability affecting classified systems or information is discovered.

cc. Reporting all security-related incidents.

dd. Ensuring all users have the requisite security clearances, authorization, and need-to-know.

ee. Briefing users on their responsibilities with regard to IS security, and verifying that cleared contractor personnel are trained on the IS's prescribed security restrictions and safeguards before they are allowed to access the IS.

ff. If applicable, designating an Information System Security Officer (ISSO).

gg. If applicable, overseeing the ISSO under their purview to ensure they follow established IS policies and procedures.

hh. If applicable, ensuring all ISSOs receive the necessary technical security training (e.g., operating system, networking, security management) to carry out their duties.

ii. Coordinating with the cleared contractor's Facility Security Officer (FSO) and the cleared contractor's Insider Threat Program Senior Official (ITPSO) to ensure insider threat awareness is addressed within the cleared contractor's IS programs.

jj. Ensuring user activity monitoring data is analyzed, stored and protected in accordance with the ITPSO policies and procedures.

Table 2 ISSM Required Training

ISSM Required Training	
CDSE Course Name	**CDSE Course Number**
Categorization of the System	CS102.16
Selecting Security Controls	CS103.16
Implementation of Controls	CS104.16
Assessing Security Controls	CS105.16
Authorizing Systems	CS106.16
Monitoring Security Controls	CS107.16
Continuous Monitoring	CS200.16
All **contractually required** training and/or technical certifications must be completed within specified time requirements.	
Note: Completion of training will be evaluated during the SVA.	

3.7 Information System Security Officer (ISSO)

An ISSO is an individual responsible for ensuring the appropriate operational security posture is maintained for an IS. The ISSO must be an U.S. citizen and employed by the cleared contractor or its subcontractor. The ISSO assists the ISSMs in meeting their duties and responsibilities. Responsibilities of the ISSO include, but are not limited to:

a. Ensuring systems are operated, maintained, and disposed of in accordance with security policies and procedures as outlined in the SSP.

b. Verifying the implementation of delegated aspects of the IS security program.

c. Ensuring all proper account management documentation is completed prior to adding/deleting IS accounts.

d. Verifying all IS security-related documentation is current and accessible to properly authorized individuals.

e. Conducting periodic assessments of authorized ISs and providing corrective actions for all identified findings and vulnerabilities to the ISSM.

f. Ensuring audit records are collected and analyzed in accordance with the SSP.

g. Reporting all security-related incidents to the ISSM.

h. Monitoring system recovery processes to ensure security features and procedures are properly restored and functioning correctly.

i. Formally notifying the ISSM of any changes to an IS that could affect authorization.

j. Serving as a member of the CCB (Configuration Control Board), if designated by the ISSM.

k. Possessing sufficient experience and technical competence commensurate with the complexity of the ISs.

l. Completing the required training identified in the ISSM Required Training Table within one year of appointment.

m. Ensuring user activity monitoring data is analyzed, stored and protected in accordance with the ITPSO policies and procedures.

3.8 Facility Security Officer (FSO)

The cleared contractor will appoint an employee as the FSO. The FSO must be a U.S. citizen and employee of the cleared contractor. In addition, the FSO must be cleared as part of the facility clearance (FCL). The FSO is responsible for supervising and directing security measures necessary for implementing applicable requirements of the NISPOM and related requirements for classified information. They should be fully integrated into every aspect of the RMF process. Responsibilities of the FSO include, but are not limited to:

a. Supporting the ISSM in their efforts to implement the IS's security program and policies for their assigned area of responsibility.

b. Advising all cleared employees of their individual responsibility for safeguarding classified information.

c. Providing security training to cleared employees as appropriate, according to NISPOM Chapter 3, through initial briefings, refresher briefings, and debriefings.

d. Developing/Maintaining a Standard Practice Procedures (SPP) document that implements the applicable requirements of the NISPOM for the cleared contractor's operations and involvement with classified information at the cleared contractor's facility.

e. Ensuring insider threat awareness is addressed within the cleared contractor's security program.

f. Coordinating/Conducting periodic self-inspections related to the activity, information, IS, and conditions of the overall security program, to include the insider threat program.

g. Reviewing and approving the organization's Contingency Plan.

h. Coordinating and planning investigation/cleanup procedures when there is a loss, compromise, or suspected compromise of classified information.

i. Reviewing IS audit record findings related to inappropriate or unusual activity.

j. Enforcing physical access authorizations at entry/exit points to the facility.

k. Employing a formal sanctions process for individuals failing to comply with established security policies and procedures.

l. Completing all security training specified in the NISPOM Chapter 3.

3.9 Privileged User

A privileged user is an individual who is authorized to perform security relevant functions, such as system control, monitoring, data transfer, or administration functions that general users are not authorized to perform. A privileged user is subordinate to the ISSM or ISSO on all matters related to IS security. Privileged user accounts perform security-relevant functions (e.g., Auditors, Data Transfer Agents (DTA), Network Administrators, and System Administrators). Responsibilities of the privileged user include, but are not limited to:

a. Complying with the IS security program requirements as part of their responsibilities for the protection of ISs and classified information.

b. Complying with all policies and procedures issued by the IO (e.g., AFT Procedures, Media Protection Procedures, SCG, etc.).

c. Completing, at a minimum, annual IS general user training and privileged user training.

d. Accessing only the specific data, control information, software, hardware, and firmware for which they are authorized access and have a need-to-know, and assume only those roles and privileges for which they are authorized.

e. Utilizing special accesses or permissions to perform only authorized tasks and functions.

f. Utilizing a separate general user account to perform routine, non-administrative daily tasks (such as web browsing or reading electronic mail) as these activities may unintentionally damage or expose the system to attacks that are delivered via everyday applications.

g. Refraining from using their privileged user accesses to alter, change or destroy information (e.g., audit logs, security-related objects and directories) without approval from the appropriate legal authority.

h. Protecting all privileged authenticators (e.g., root, super user, Domain Administrator, Local Administrator, Auditor, etc.) at the highest classification level of the data processed on the IS.

i. Taking necessary precautions to protect the CIA (Confidentiality, Integrity, Availability) of information encountered while performing privileged duties.

j. Reporting and documenting all system security configuration changes and detected/suspected security-related IS problems that might adversely impact IS security to the ISSM.

3.10 General User

A general user is an individual who can receive information from, input information to, or modify information on an IS. A general user does not have access to system controls, monitoring, and/or administration functions. Responsibilities of the general user include, but are not limited to:

a. Complying with the IS security program requirements as part of their responsibilities for the protection of ISs and classified information.

b. Complying with all policies and procedures issued by the IO (e.g., AFT Procedures, Media Protection Procedures, SCG, etc.).

c. Completing, at a minimum, annual IS training.

d. Accessing only that data, system information, software, hardware, and firmware for which they are authorized access and have a need-to-know, and assume only those roles and privileges for which they are authorized.

e. Being accountable for all their actions on an IS.

f. Protecting IS and IS peripherals from unauthorized access.

g. Protecting authentication mechanisms at the highest classification level and most restrictive classification category for information to which the mechanisms permit access.

h. Being subjected to monitoring of their activity on any classified network; the results of such monitoring could be used against them in a criminal, security, or administrative proceeding.

i. Reporting all actual or suspected security incidents and potential threats and vulnerabilities involving an IS and/or network to the appropriate ISSM/ISSO via secure means.

j. Ensuring all system media and output products are properly classified, marked, controlled, stored, transported, and destroyed.

k. Safeguarding and reporting the receipt of any media received through any channel to the ISSM/ISSO for subsequent virus inspection and inclusion into the media control procedures.

l. Informing the ISSM/ISSO when access to a particular IS is no longer required (e.g., completion of project, transfer, retirement, resignation).

4 SECURITY TRAINING

All IS users will receive initial and annual General User Training. IS users assigned to positions requiring privileged access will also receive Privileged User Training (Related Control: AT-3).

4.1 Privileged User Training

Privileged User training will include, but is not limited to, the following:

a. Completion of General User training.

b. Rules of behavior applicable to the privileged user.

c. The organization's policy for protecting information and IS, including change management and roles and responsibilities of various organizational units.

d. The organization's policy regarding appropriate privileged use of IS resources and the possible repercussions of misuse or abuse.

e. Protection of the IS (e.g., maintenance and backup, care of system media, protection and retention of audit logs, endpoint security).

f. Instructions on protecting passwords or other authentication devices/mechanisms.

g. Operating system security features and technical safeguards of the IS.

h. Processes for recognizing and reporting potential security vulnerabilities, threats, security violations, or incidents.

i. Incident response actions.

4.2 General User Training

General User training will include, but is not limited to, the following:

a. The organization's policy for protecting information and IS.

b. Rules of behavior specifying acceptable user actions to include explicit restrictions on the use of social networking sites, posting information on commercial websites, and sharing information system account information.

c. The organization's policy regarding appropriate use of IS resources as specified in the User Agreement, and the possible repercussions of misuse or abuse.

d. Guidance on protecting the physical area, media, and equipment (e.g., door access, alarms, care of hard drives, Compact Disks (CDs)).

e. Instructions on protecting authenticators and operating the applicable system security features (e.g., setting access control rights to files created by the user).

f. Processes for recognizing and reporting suspected security violations and incidents.

g. Classification and control marking compliance.

h. Incident response actions.

i. Actions requiring Two Person Integrity (TPI).

4.3 Data Transfer Agent (DTA) Training

An individual performing data transfers is commonly referred to as a DTA. The DTA is performing a security-relevant function in providing endpoint security during a data transfer. DTAs must be identified in writing. AFT training for DTAs will include, but is not limited to the following:

a. Data review and sanitization tools (automated and manual).

b. SCG.

c. Permissible AFT file formats.

d. Authorized media formats and marking requirements.

e. AFT logging procedures.

5 RISK MANAGEMENT FRAMEWORK

CNSS has developed a common information security framework for the Federal government and its cleared contractors. The intent of this common framework is to improve information security, strengthen risk management processes, and encourage reciprocity among Federal agencies.

The RMF and associated RMF tasks apply to both ISSMs and CCPs. In addition to supporting the authorization of ISs, the RMF process supports maintaining the security posture of the IS, and facilitating senior leader decisions related to operational risk. Execution of the RMF tasks by CCPs, both internal and external to the organization, helps to ensure that the security capabilities provided by the common controls can be inherited by IS owners with a degree of assurance appropriate for their information protection needs. This approach recognizes the importance of security control effectiveness within ISs and the infrastructure supporting those systems.

The RMF is a life cycle based approach. Therefore, ISSMs will need to revisit various tasks over time to manage their ISs and the environment in which those systems operate. Managing information security related risks for an IS is viewed as part of a larger organization wide risk management activity. The RMF provides a disciplined and structured approach to mitigating risks in a highly dynamic environment of operation.

5.1 Introduction to the Risk Management Framework (RMF)

The Joint Task Force (JTF) Transformation Initiative Working Group developed NIST SP 800-37 to replace the traditional C&A process with the six-step RMF process. Figure 2 depicts the Six-Step RMF Process. The revised process emphasizes:

a. Building information security capabilities into ISs processing classified information through the application of best practices for management, operational, and technical security controls.

b. Maintaining awareness of the security state of ISs on an ongoing basis through enhanced monitoring processes.

c. Providing essential information to senior leaders to facilitate decisions regarding the acceptance of risk to organizational operations and assets, individuals, other organizations, and national security arising from the operation and use of IS.

The objectives of the RMF process include:

a. Incorporating cybersecurity early and robustly in the acquisition and system development life cycle.

b. Implementing a three-tiered approach to risk management that addresses risk-related concerns at the enterprise level, the mission and business process level, and the information system level.

c. Providing a risk management methodology that gives organizations a true picture of vulnerabilities caused by non-compliant controls as it relates to other risk factors (e.g. likelihood, threat, and impact).

d. Codifying system authorization reciprocity to enable organizations to accept approvals by other organizations for interconnection or reuse of IT without retesting.

e. Emphasizing information security continuous monitoring and timely correction of deficiencies, including active management of vulnerabilities and incidents.

The RMF steps include:

1. **Categorize** the IS and the information processed, stored, and transmitted by the system based on an analysis of the impact due to a loss of confidentiality, integrity and availability.

2. **Select** an initial set of baseline security controls for the IS based on the security categorization, tailoring and supplementing the security control baseline as needed based on an organizational assessment of risk and local conditions.

3. **Implement** the security controls and describe how the controls are employed within the IS and its environment of operation.

4. **Assess** the security controls using appropriate assessment procedures 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.

5. **Authorize** IS operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and national security resulting from the operation of the IS and the decision that the risk is acceptable.

6. **Monitor** the security controls in the IS on an ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.

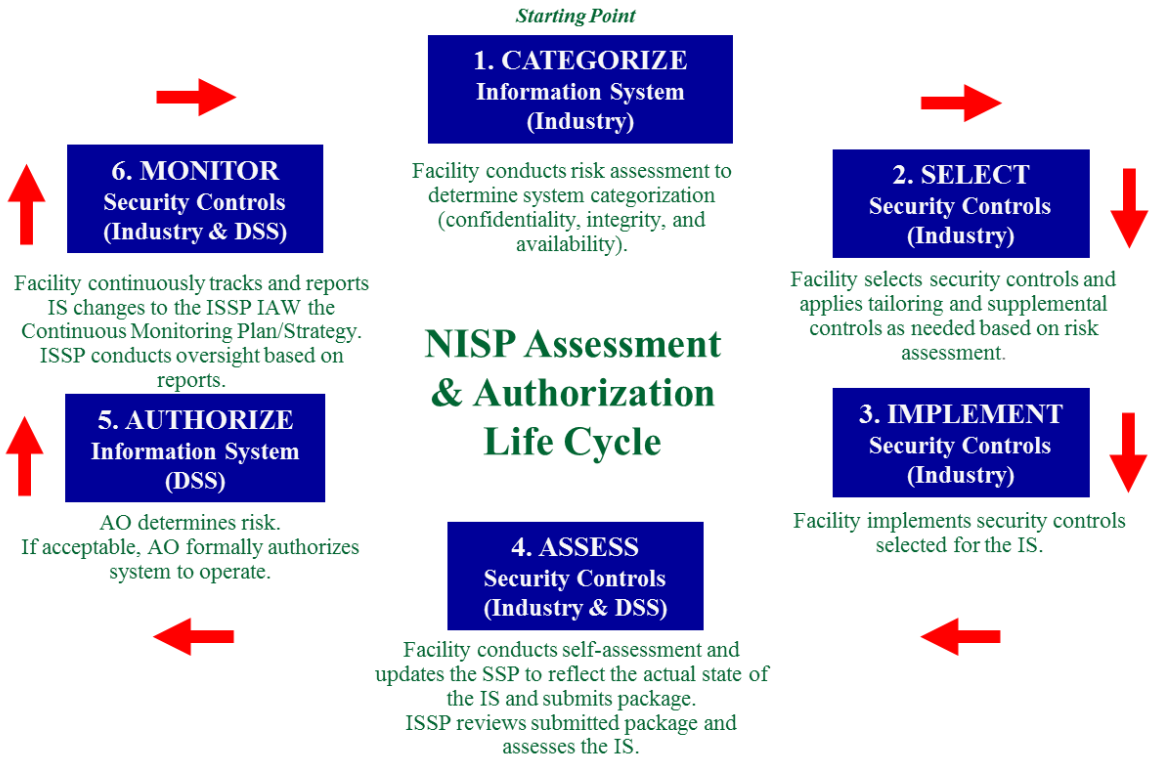

Figure 2 The Six-Step RMF Process

For additional information regarding the RMF, see NIST SP 800-37.

5.2 Fundamentals of the RMF

Managing IS-related security risks is a complex, multifaceted undertaking that requires the involvement of the entire organization from senior leaders providing the strategic vision and top-level goals and objectives for the organization, to mid-level leaders planning and managing projects, to individuals on the front lines developing, implementing, and operating the systems supporting the organization's core missions and business processes. Risk management can be viewed as a holistic activity that is fully integrated into every aspect of the organization.

6 ASSESSMENT AND AUTHORIZATION IMPLEMENTATION GUIDANCE

DSS highly recommends SSP submission for RMF packages at least 90 days before required need, whether re-authorization or new IS. This timeframe will allow for complete SSP review and interaction between the ISSM and ISSP on any potential updates or changes to the SSP.

6.1 RMF Step 1: Categorize

Step 1 of the RMF focuses on categorizing the IS. ISs will be categorized based on the impact due to a loss of CIA of the information or IS.

Security impact levels are defined as Low, Moderate, or High for each of the three IS security objectives: Confidentiality, Integrity, and Availability (CIA). For example, an IS may have a Confidentiality impact level of Moderate, an Integrity impact level of Moderate, and an Availability impact level of Low. The DSS baseline identifies security control specifications needed to safeguard classified information that is stored, processed, or transmitted and adopts a minimum baseline of Moderate-Low-Low (M-L-L).

The impact values will be documented in the SSP along with the research, key decisions, approvals, and supporting rationale. The following paragraphs provide guidance in defining impact levels for all ISs under the purview of DSS.

Confidentiality

The confidentiality impact level for all NISP systems will be Moderate or High.

a. **Moderate**: The unauthorized disclosure of any information processed, stored, and transmitted by the IS 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.

b. **High**: The unauthorized disclosure of any information processed, stored and transmitted by the IS 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.

Integrity

The Integrity Impact Level will be Low, Moderate, or High.

a. **Low**: The unauthorized modification or destruction of any information processed, stored and transmitted by the IS could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States.

b. **Moderate**: The unauthorized modification or destruction of any information processed, stored and transmitted by the IS 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.

c. **High**: The unauthorized modification or destruction of any information processed, stored and transmitted by the IS 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.

Availability

The Availability Impact Level will be Low, Moderate, or High.

a. **Low**: The disruption of access to or use of any information processed, stored and transmitted by the IS could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States (e.g., more than 24 hours).

b. **Moderate**: The disruption of access to or use of any information processed, stored and transmitted by the IS 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 (e.g., less than 24 hours).

c. **High**: The disruption of access to or use of any information processed, stored and transmitted by the IS 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 (e.g., minutes).

The following provides amplification of terms used in determining impact levels.

1. A **limited** adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:

    a. 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 the functions is noticeably reduced.

    b. Result in minor damage to organizational assets.

    c. Result in minor financial loss.

d. Result in minor harm to individuals.

2. A **serious** adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:

   a. 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 the functions is significantly reduced.

   b. Result in significant damage to organizational assets.

   c. Result in significant financial loss.

   d. Result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

3. A **severe or catastrophic** adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:

   a. 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.

   b. Result in major damage to organizational assets.

   c. Result in major financial loss.

   d. Result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.

The ISSM/ISSO, along with assistance from the ISO, is responsible for the following tasks:

Task 1-1: Categorize the IS and document the results in the SSP. Industry will perform a risk assessment for specific concerns for their facility/program. The purpose of the risk assessment is to inform decision makers and support risk responses by identifying:

a. Relevant threats.

b. Vulnerabilities both internal and external to the organization.

c. Impact to the organization that may occur given the potential for threats exploiting vulnerabilities.

d. Likelihood that harm will occur.

Risk assessment outcomes should be reviewed to examine the facility's threat picture and determine if tailoring controls are required. The results are documented in the RAR. The ISSM will review applicable SCGs and verify classification level of RAR results.

Task 1-2: Establish IS boundaries (Reference Information System Boundaries Section).

Task 1-3: The IS is categorized based on the impact due to a loss of confidentiality (moderate/high), integrity (low/moderate/high), and availability (low/moderate/high) of the information according to information provided by the IO.

Task 1-4: Assign qualified personnel to RMF roles and document team member assignments in the SSP.

Task 1-5: Document the system description, including the system/IS boundary, in the initial SSP.

Outputs: RAR, Initial System Security Plan

References: NIST SP 800-30 Revision 1.0, NIST FIPS-199, NIST SP 800-60, CNSSI 1253

6.2 RMF Step 2: Select

The ISSM/ISSO, along with assistance from the ISO, is responsible for the following tasks:

Task 2-1: Identify the security controls that are provided by the organization as common controls for all or multiple IS under the organization's control and document the controls in the SSP. Control implementation can be characterized as:

System Specific – Security controls specific to an IS and the responsibility of the ISO/ISSM.

Common – Security controls that are inheritable by one or more organizational IS and are typically provided by the organization or the infrastructure (Examples: Physical and environmental security controls, Network boundary defense security controls, Organization policies or procedures, etc.). The benefits of common security controls include:

a. Supporting multiple ISs efficiently and effectively as a common capability.

b. Promoting more cost-effective and consistent security across the organization and simplifying risk management activities.

c. Significantly reducing the number of discrete security controls that have to be documented and tested at the IS level which in turn eliminates redundancy, gains resource efficiencies, and promotes reciprocity.

Hybrid – Security controls that are implemented in an IS in part as a common control and in part as a system specific control. If any of the IS components need system-specific infrastructure protections, in addition to common controls that apply to the IS, the control is implemented as a hybrid control (Example: Emergency power may be implemented as a common control for the facility in which the system resides, but the specific IS requires additional availability protection based on the criticality of the information in the system to the organization's mission resulting in the implementation of a separate uninterrupted emergency power source for the IS).

Task 2-2: Select the security controls for the IS and document the controls in the SSP. The selection is based upon the results of the categorization (Security Impact Levels determined

during RMF Step 1). The DSS baseline identifies security control specifications needed to safeguard classified information that is stored, processed, or transmitted and adopts a baseline of Moderate-Low-Low (M-L-L). Apply any DSS Overlay identified as applicable during security categorization. Document the initial security control set and the rationale for adding or removing security controls from the baseline by referencing the applicable overlay in the SSP.

Task 2-3: Tailor the initial security control. Tailoring encompasses:

a. Identifying/designating common controls in initial baselines.

b. Making risk based decisions on remaining baseline controls.

c. Selecting compensating controls.

d. Supplementing baselines with additional controls and control enhancement, if applicable.

The security controls listed in the initial baselines are not a minimum, but rather a proposed starting point from which controls may be removed or added based on tailoring guidance. Document in the SSP the relevant decisions made during the tailoring process, providing a sound rationale for those decisions. Tailor the controls as needed: tailor in controls to supplement the set of selected controls, and tailor out, or modify, the controls as applicable based on the system risk assessment. If a security control identified in the baseline set of controls is tailored out, an explanation must be provided in the SSP, describing the rationale as to why the control does not apply or how it is satisfied by other mitigating factors. Security controls may also be added (e.g., tailored in) as necessary depending upon the IS and/or its environment of operation.

Task 2-4: Develop a strategy for continuous monitoring of security control effectiveness. The implementation of a robust Continuous Monitoring Strategy allows an organization to understand the security state of the IS over time and maintain the initial security authorization in a highly dynamic environment of operation with changing threats, vulnerabilities, technologies, and missions/business functions. Ongoing monitoring of the security controls is a critical part of risk management. Effective monitoring includes, but is not limited to, configuration management and control, security impact analyses on proposed changes, assessment of selected security controls, and security status reporting. This information will be documented within the SSP. This information is used to determine whether the planned security implementation is acceptable in accordance with the RMF.

To pass OBMS validation, the ISSM or designee must upload a blank Certification Statement and add the “Profile” extension for the RAR. For more information on utilizing OBMS, please reference the job aids located here: http://www.dss.mil/is/obms.html.

Outputs: Initial SSP with identified security controls, Continuous Monitoring Strategy, and RAR

References: CNSSI 1253, NIST SP 800-53, DAAPM (Security Controls (M-L-L) and DSS Overlays).

6.3 RMF Step 3: Implement

The ISSM/ISSO is responsible for the following tasks:

Task 3-1: Implementing the security controls specified in the SSP. The ISSM will assess the security controls as documented in the SSP. **Note:** In Step 4, the ISSP will conduct the security controls assessment utilizing the Defense Information Systems Agency (DISA) Security Content Automation Protocol (SCAP) Compliance Checker (SCC) for automated checks and all appropriate baseline/benchmark Security Technical Implementation Guides (STIGs) as documented in the SSP. Additional automated tools can be found at the following link: https://nvd.nist.gov/scap/validated-tools. Any issues/vulnerabilities/weaknesses will be identified and remediated via tailoring and/or POA&M documentation.

Task 3-2: Documenting the security control implementation in the SSP and providing a functional description of the control implementation (including planned inputs, expected behavior, and expected outputs). The documentation will include any additional information necessary to describe how the security capability is achieved at the level of detail sufficient to support control assessment.

Outputs: Updated SSP with a functional description of security control implementation, Supporting Artifacts

References: CNSSI 1253, NIST SP 800-53, NIST SP 800-53A, NIST SP 800-30 Rev 1.0, NIST FIPS 199, DAAPM (Security Controls (M-L-L) and DSS Overlays)

6.4 RMF Step 4: Assess

Step 4 of the RMF focuses on assessing the security controls applicable to the IS and includes the following tasks:

Part 1 – Industry

The ISSM/ISSO is responsible for the following tasks:

Task 4-1: The ISSM will conduct an assessment of the security controls in accordance with the security procedures defined in the SSP. This process is conducted to ensure the security controls are implemented correctly, operating as intended, and meet the security requirements for the IS. In preparation for the ISSP assessment, the SCAP, STIG Viewer, and applicable STIG and/or SCC content must be installed on the IS. If the IS cannot be assessed utilizing the specified scanning tools, the assessment will be conducted in accordance with the SSP.

Task 4-2: The ISSM will review applicable SCG and verify classification level of all SSP artifacts. If supporting artifacts are deemed classified, contact assigned ISSP for guidance. The ISSM will finalize the SSP to reflect the actual state of the security controls, as required, based on the vulnerabilities of the security control assessment, reassessment, and completion of any remediation actions taken. The ISSM will submit the final SSP, Certification Statement, RAR, POA&M (if applicable), and supporting artifacts to DSS for review and authorization

consideration via OBMS. Submit artifacts in accordance with Table 3 below. **Note:** OBMS will only accept PDF documents.

Table 3 OBMS Artifacts

Examples of Unclassified Submission Artifacts	OBMS Document Types
SSP	SSP
Certification Statement	Certification Statement
Risk Assessment Report	Profile
Security Assessment Report (SAR)	Comments
POA&M (if applicable)	Other
Provide any other Supporting Contractual Requirements (DD254, Request for Proposals etc.)	Other
SSP Appendices and any artifacts that support SSP implementation strategy (Standard Operating Procedures (SOPs), ISA/MOU/A, etc.)	Other

Part 2 – DSS

The ISSP is responsible for the following tasks:

Task 4-3: The ISSP receives and reviews the final SSP, Certification Statement, RAR, POA&M (if applicable), and supporting artifacts via OBMS. The initial review will include:

a. Ensuring an adequate system description is provided.

b. Assessing security controls based upon implementation responses. **Note:** Implementation responses must provide sufficient data to describe how the security control is met.

c. Validating justification for tailored-out controls.

d. Ensuring mitigated security controls have comparable safeguarding. **Note:** The ISSM must provide supporting rationale for how the compensating control delivers an equivalent security capability and why the related baseline security control could not be employed.

e. Validating inherited controls via supporting documentation.

The ISSP makes risk-based decisions regarding compliance conditions. In order to facilitate the assessment, the following supporting documents are reviewed:

a. RAR

b. POA&M

c. Configuration Management (Hardware and Software Baselines)

d. System Diagram and/or Network Topology

e. Sponsorship (Department of Defense (DD) Form 254, Request for Proposal (RFP), Framework Agreement)

f. Physical Security (DSS Form 147)

g. Interconnection (ISA/MOU/A - if applicable)

h. Media Protection (AFT/Data Transfer Procedures)

i. Sanitization Procedures (if applicable)

j. Incident Response Plan (IRP)

k. Continuous Monitoring Strategy

l. SPP

m. Additional Supporting Artifacts Requested by the AO

Any weaknesses and/or deficiencies will be documented in the SAR. If the SSP is not acceptable and the documentation is insufficient, the ISSP may recommend a Denial of Authorization to Operate (DATO).

If the SSP is acceptable and the documentation fully addresses all system security controls and security configurations, an on-site assessment may be scheduled. In rare circumstances, an on-site assessment may be waived.

Task 4-4: The ISSP conducts an on-site assessment. The on-site assessment will include:

a. Assessing the applicable technical security controls and system configuration using the applicable DISA compliance scanning tools (e.g., SCC, STIGs, and associated benchmarks).

b. Assessing the supporting operational and managerial security controls.

c. Identifying any necessary remediation/mitigation actions for the POA&M.

Any weaknesses and/or deficiencies will be documented in the SAR. Based on the results of the assessment, the ISSP will prepare the security authorization package, which includes a risk based recommendation.

Part 3 – Industry

The ISSM/ISSO is responsible for the following tasks:

Task 4-5: Develop/Update POA&M based on findings and recommendations from the SAR. The ISSM is responsible for updating the POA&M, to include identifying corrective actions,

determining resources required, documenting milestone completion dates, and addressing any residual findings. The POA&M will identify:

a. Tasks to be accomplished.

b. Resources required to accomplish the tasks.

c. Any milestones in meeting the tasks, to include percentage completed.

d. Scheduled completion dates for the milestones.

e. Mitigating Actions.

Outputs: Final SSP, POA&M, RAR, Supporting Artifacts, and SAR

References: NIST SP 800-53A

6.5 RMF Step 5: Authorize

Step 5 of the RMF focuses on formally authorizing the IS for operation.

Authorization Decisions are based on submission timeliness, NIST security control implementation, ISSM experience, and other factors. The DSS AOs may issue ATOs of shorter duration or ATO with Conditions (ATO-C) which describe conditions needed to be met while validating an SSP package submission.

DSS

The ISSP is responsible for the following tasks:

Task 5-1: The ISSP assembles and submits the security authorization package to the AO. At a minimum, the security authorization package will contain the Authorization Decision Letter, RAR, SAR, and POA&M (as applicable). Additional bodies of evidence may be required, as directed by the AO. The ISSP is responsible for verifying that the security authorization package is complete and is submitted for final review to the AO. For ISs inheriting common controls for specific security capabilities, the security authorization package for the common controls or a reference to such documentation must also be included in the security authorization package. When security controls are provided to an organization by an external provider (e.g., through contracts interagency agreements lines of business arrangements, licensing agreements, supply chain arrangement, etc.), the ISSP will ensure the information needed by the AO to make a risk-based decision is included in the authorization package.

The AO is responsible for the following tasks:

Task 5-2: The explicit acceptance of risk is the responsibility of the AO. The AO will issue an authorization decision for the IS and the common controls inherited by the system after reviewing all of the relevant information, and where appropriate, consulting with other organizational officials.

The authorization decision document (e.g., Authorization to Operate (ATO) and Denial of Authorization to Operate (DATO)) conveys the security authorization decision from the AO to the ISSM, and other organizational officials, as appropriate. The authorization decision document contains the following information:

a. Authorization decision

b. Terms and conditions for the authorization

c. Authorization Termination Date (ATD) – Processing beyond this date is unauthorized

Outputs: Security Authorization Package, Authorization Letter

References: NIST SP 800-53A

6.6 RMF Step 6: Monitor

The Continuous Monitoring Strategy is required to determine if the set of deployed security controls continue to be effective. Continuous monitoring activities support the concept of near real-time risk management through ongoing security assessments and risk analysis, and recording results in IS security documentation (SSP, POA&M, and RAR). Continuous monitoring requires both automated and manual processes. The Continuous Monitoring Strategy includes:

a. Maintaining and executing configuration management processes for ISs.

b. Determining the security impact of proposed or actual changes to the IS and its operating environment (Related Controls: CM-4, CM-3(4), CA-7).

c. Assessing selected security controls (including system-specific, hybrid, and common controls) based on the approved Continuous Monitoring Strategy.

d. Ensuring security documentation, including the SSP, RAR, and POA&M, is updated and maintained based on the results of continuous monitoring activities.

e. Providing security status reports on the security posture of the ISs to appropriate officials in accordance with the Continuous Monitoring Strategy.

f. Supporting risk management decisions to help maintain organizational risk tolerance at acceptable levels.

Part 1 – Industry

The ISSM/ISSO is responsible for the following tasks:

Task 6-1: The ISSM, along with assistance from the ISO, FSO and other IS stakeholders, will assess all technical, management, and operational security controls employed within and inherited by ISs in accordance with the organization's Continuous Monitoring Strategy. The frequency of monitoring is based on the Continuous Monitoring Strategy developed by the

ISO/ISSM or Common Control Provider (CCP) and approved by the AO. To satisfy this requirement, organizations can evaluate the results from any of the following sources, including but not limited to:

a. Security control assessments conducted as part of an IS authorization, ongoing authorization, or reauthorization.

b. Continuous monitoring activities.

c. Testing and evaluation of the IS as part of the acquisition and system development life cycle process or audit.

Task 6-2: The ISSM, along with assistance from the ISO, FSO, and other IS stakeholders, will conduct remediation/mitigation actions based on the results of ongoing monitoring activities, assessment of risk, and outstanding items in the POA&M (if applicable).

The ISO and CCP initiate remediation actions on outstanding items listed in the POA&M and findings produced during the continuous monitoring of security controls. An assessment of risk (either formal or informal) informs organizational decisions with regard to conducting ongoing remediation/mitigation actions.

Task 6-3: The ISSM will ensure the IS security documentation (SSP, POA&M, and RAR) is updated and maintained based on the results of continuous monitoring. The updated SSP will reflect any modifications to security controls based on risk mitigation activities carried out by the ISSM. Continuous monitoring status reports will reflect additional assessment activities carried out to determine security control effectiveness based on modifications to the SSP and deployed controls. Updates to the POA&M will report progress made to outstanding items, address vulnerabilities, and describe mitigation actions. When updating critical information in the POA&M, organizations will ensure that the original information needed for oversight, management, and auditing purposes is not modified or destroyed.

Task 6-4: The results of continuous monitoring activities will be reported to the ISSP as defined in the authorized SSP. Any anomalies or issues (e.g., security control deviations, threat environment changes, incidents impacting IS risk level, security relevant changes, etc.) must be reported immediately to the ISSP.

The ISSM is required to maintain a log of continuous monitoring activities on-site. Continuous monitoring documentation will be assessed during the SVA and other engagement activities (e.g., Advise & Assist visits, periodic communications, etc.). All appropriate administrative and security relevant documentation will be submitted to DSS using OBMS. Security status reporting can be event driven, time driven, or both. The goal is ongoing communication with DSS to convey the current security state of the IS and its environment of operation. Security status reports will be appropriately marked, protected, and handled in accordance with Federal and organizational policies.

Task 6-5: The ISSM will implement an IS decommissioning strategy (referred to as *disposal* in the NIST documentation), which executes required actions when a system is removed from service. Organizations will ensure that all security controls addressing IS removal and

decommissioning (e.g., media sanitization, configuration management, and control) are implemented. Users and application owners hosted on decommissioned IS will be notified as appropriate, and any security control inheritance relationships will be reviewed and assessed for impact.

A cybersecurity risk assessment for an IS undergoing decommissioning should be conducted to identify the level of risk associated with decommissioning activities. The results of the risk assessment drive decisions on the appropriate actions taken during decommissioning. Those actions include:

a. Ensuring that no classified, sensitive, or privacy information will be exposed during the decommissioning process.

b. Ensuring control inheritance relationships are reviewed and assessed for impact; if the system undergoing decommissioning provides inherited controls, ensure "disinherited" controls are implemented elsewhere if they are still required.

c. Ensuring artifacts and supporting documentation are disposed of according to their sensitivity or classification in accordance with the approved SSP.

In certain cases, a system that is being decommissioned encompasses processes, workflows, logic, or data that must be migrated to a receiving/target system. For this reason, it is important that the system that will be decommissioned is first adequately migrated in terms of its functionality and data. Where a migration to a receiving/target system is scheduled, each system should have a migration plan that is developed and approved by the project manager responsible for the decommissioning, the ISO for the legacy system, and the AOs for the respective systems. The migration plan should be established and approved prior to conducting migration activities.

The ISSM will immediately notify the ISSP of the need to decommission an authorized IS. All storage media and memory associated with the IS must be sanitized in accordance with the procedures outlined in the SSP. Provided the IO does not advise to the contrary, material associated with the IS may be retained for up to two years, as outlined in NISPOM, Section 5-701. Records associated with the IS must be retained for one assessment cycle. For more information on implementing a decommissioning/disposal strategy, please reference NIST SP 800-64 Revision 2.0 (Section 3.5).

Part 2 – DSS

The ISSP is responsible for the following tasks:

Task 6-6: The ISSP will review the reported security status of ISs under his/her purview, including the effectiveness of security controls employed within and inherited by the systems, in accordance with the approved Continuous Monitoring Strategy. This review will determine whether the risk to organizational operations, organizational assets, individuals, other organizations, or national security remains acceptable. The ISSP may provide recommendations as to appropriate remediation actions. Security controls that are modified, enhanced, or added during continuous monitoring are reassessed by the ISSP to ensure appropriate corrective actions are taken to eliminate weaknesses or deficiencies or to mitigate the identified risk. The

assessment information received by the ISSP during continuous monitoring activities is provided to the AO. The AO uses the continuous monitoring documentation to determine if the authorization decision needs to be changed from an ATO to a DATO or if reauthorization action is necessary.

Task 6-7: Upon receipt of a decommissioning request, the ISSP will review and forward the request to the AO. Once the ISSM requests decommission, the system is considered decommissioned. The AO will formally decommission the IS by issuing an IS Removal and Decommissioning letter. During the next DSS SVA or contact/engagement, the ISSP will verify that all security controls addressing IS removal and decommissioning were implemented and that storage media, memory, peripherals, etc. associated with the IS were properly sanitized in accordance with the procedures outlined in the authorized SSP and DAAPM.

Outputs: Updated IS Security Documentation (SSP, POA&M, and RAR), Continuous Monitoring Strategy Deliverables (Status Reports), IS Decommissioning Strategy (as necessary), Updated Security Authorization Package (as appropriate)

References: NIST SP 800-30 Revision 1.0, NIST SP 800-37, NIST 800-137, NIST SP 800-64 Revision 2.0 (Section 3.5), NISPOM

7 INFORMATION SYSTEM BOUNDARIES

Security architecture plays a key part in the security control selection and allocation process for an IS. Well-defined boundaries establish the scope of protection for organizational ISs (e.g., what the organization agrees to protect under its direct management control or within the scope of its responsibilities), and include the people, processes, and information technologies that are part of the systems supporting the organization's missions and business processes. IS boundaries are established in coordination with the security categorization process and before the development of the SSP. IS boundaries that are too expansive (e.g., too many system components and/or unnecessary architectural complexity) make the risk management process extremely unwieldy and complex. Boundaries that are too limited increase the number of ISs that must be separately managed, and as a consequence, unnecessarily inflate the total information security costs for the organization.

Establishing IS Boundaries

Organizations have significant flexibility in determining what constitutes an IS and its associated boundary. In addition to consideration of direct management control, organizations may also consider whether the information resources being identified as an IS:

a. Support the same mission/business objectives or functions and essentially the same operating characteristics and information security requirements.

b. Reside in the same general operating environment (or in the case of a distributed IS, reside in various locations with similar operating environments).

c. Reside in the same geographic area (e.g., a site).

Since commonality can change over time, the determination of the IS boundary should be revisited periodically as part of the continuous monitoring process. ISOs will consult with key participants (e.g., AO, ISSP, ISSM and other individuals with a vested interest when establishing or changing system boundaries). The process of establishing IS boundaries and the associated risk management implications is an organization-wide activity that takes into account mission and business requirements, technical considerations with respect to information security, and programmatic costs to the organization.

Once an IS boundary is set, any interconnections with systems outside of that boundary that are approved by a different AO are governed by an ISA. Interconnections include monitoring and controlling communications at key internal boundaries among subsystems, and providing system-wide common controls that meet or exceed the requirements of the constituent subsystems inheriting those system-wide common controls. For additional information regarding ISAs, reference NIST SP 800-47.

Security controls for the interconnection of subsystems are employed when the subsystems implement different security policies or are administered by different authorities. The extent to which the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the IS, can be determined by combining security control assessments at the subsystem level and adding system-level considerations addressing interface issues among subsystems. This approach facilitates a more targeted and cost-effective risk management process by scaling the level of effort of the assessment in accordance with the subsystem security categorization and allowing for reuse of assessment results at the IS level.

8 TYPES OF INFORMATION SYSTEMS

There are many IS types and system configurations that operate within cleared contractor facilities. The predominant IS types are Standalone Information Systems, Local Area Networks (LANs), Unified Networks, Interconnected Systems, and Wide Area Networks (WANs). The information below identifies the particular types of IS seen in cleared Industry.

8.1 Standalone Information Systems

Multi-User Standalone (MUSA) systems serve multiple users, but only one user at a time, and do not sanitize between users. Single-User Standalone (SUSA) systems support one general user. Privileged users (systems administrators) should not be included when determining the number of users on the system. The ISSM or designee will utilize the DSS Overlays (see Appendix) to assist with tailoring control selection.

8.2 Local Area Network (LAN)

A LAN consists of two or more connected workstations for the purpose of sharing information. A LAN can be as simple as two interconnected laptops through a category 5 cross-over cable in a Peer-To-Peer (P2P) configuration, and as complex as a thousand desktops connected by multiple switches and routers traversing several buildings using Active Directory to push security group policies throughout the domain (e.g., client/server (C/S) based). The physical security parameters

within SSPs vary between closed areas and various configurations of restricted areas for LAN implementations. LANs that reside in a closed area can be approved for unattended processing.

8.3 Wide Area Networks (WAN)

A WAN is a computer network that covers a broad geographical area (e.g., any network comprised of communications links traversing metropolitan, regional, or national boundaries), or, more formally, a network that uses routers and public communications links. WANs are used to connect LANs and other types of networks together, so that users and computers in one location can communicate with users and computers in other locations. Many WANs are built for one particular organization and are private; whereas, other WANs can be publicly accessible and have specific requirements for access and interconnection.

8.4 Interconnected Systems

An interconnected network consists of two or more separately authorized systems connected together. The predominant interconnected networks are contractor-to-contractor or government-to-contractor connections, or a combination of both. In rare cases, international connections may need to be established.

Contractor-to-Contractor Connections

If DSS is the AO for both authorized ISs, an ISA is required to establish an interconnection between two or more separately authorized ISs. An ISA is not required when the interconnection involves two or more systems owned by the same IO at the same facility or campus (a Commercial or Government Entity with a single CAGE Code). **Note:** In this circumstance, the SSP will be updated to reflect the interconnection (Network Topology) and coordination will be conducted via the CCB.

The ISA is submitted and managed by the designated host ISSM. The assigned AO is responsible for authorizing the interconnected system. For additional information regarding ISAs, reference NIST SP 800-47.

Government-to-Contractor Connections

For the purposes of this manual, ISA, MOU, and MOA are used interchangeably. An ISA between DSS and the IO is required for all government-to-contractor connections. The purpose of an ISA is to adjudicate the differences in requirements of different AOs and to establish roles and responsibilities. Many IOs and program offices have standard ISA formats that are routinely utilized for all ISAs. The IO may use their format if they would like. However, DSS may levy additional requirements in order to be NISPOM compliant.

All ISA/MOU/MOAs must be sent to NAO for coordination and signature. NAO requires a minimum of 30 days to coordinate and properly staff all ISAs for signature. ISAs are valid until:

a. The agreement is terminated by one or more signatories.

b. A security relevant change occurs on an authorized system covered by the agreement.

c. Changes are made to the connection process.

d. The terms of the ISA/MOU/MOA are violated.

e. The agreement may be rescinded by DSS or the IO at any time.

ISA/MOU/MOA Content

It is highly recommended that the DSS approved ISA format be used. If an ISA is submitted in a format other than the DSS approved format, additional DSS internal reviews may be required. The template can be found in the ODAA Bulletin Board within OBMS, under "Headquarters Bulletin Board".

All ISA/MOU/MOA must contain the following minimum information:

a. Date of the ISA/MOU/MOA.

b. Names and signatures of AOs.

c. Name of Network ISSM/ISSO and responsibilities.

d. High-level description of and usage of the network, to include a Network Topology Diagram.

e. Contract or program name.

f. Name and location of facilities involved.

g. Security points of contact and phone numbers.

h. Names, numbers, or system identifiers for systems involved.

i. Highest classification of data.

j. ISA/MOU/A expiration date or review frequency (if applicable).

k. Categorization/Security Impact Level.

l. Minimum clearance level required of users.

m. Network type: Unified or Interconnected (usually interconnected).

n. Documentation of any existing connections to Defense Information System Network (DISN) circuits.

o. A statement that there is no further connection to any DISN network not outlined in the ISA/MOU/A and none will be added in the future (Secure Internet Protocol Router

Network (SIPRNet), Secret Defense Research Engineering Network (SDREN) and DISN Leading Edge Services (DISN-LES), etc.).

p. Encryption method.

q. A statement regarding required authorization status for interconnected sites and informing Network ISSO about any changes in authorization status.

r. A start and end date.

s. Signatures from all required parties.

ISA/MOU/MOA Submission Process

a. Select the "ISA/(MOU/A) Module" within OBMS.

b. Submit a ISA/(MOU/A) Document.

c. Navigate through the ISA/(MOU/A), Supporting Documents, and Review/Submission tabs and complete all required fields. In the Supporting Documents tab, upload the completed ISA along with any required supporting artifacts (e.g., contractual requirements, network diagram, etc.).

d. Submit for Review.

e. The assigned ISSP will conduct a quality assurance review for accuracy. If satisfactory, the ISSP will submit the ISA package to NAO for further coordination and signature. If the request is inaccurate or missing information, the ISSP will return to the submitter for corrections.

f. Once signed by DSS, the NAO will upload the signed ISA within OBMS and email the responsible POCs.

ISA/MOU/MOA Changes and Invalidations

Certain ISA/MOU/MOAs specify a pre-determined review frequency. During the review, security parameters, the accuracy of the ISA, POC information, and AO signatory information should be verified. If updates to POCs or AOs occur without termination of the current agreement, the facility may submit an administrative addendum to the agreement identifying the personnel changes without requiring the submission of a new agreement for signature. If personnel changes result in recension of or changes to the terms of the current agreement, a new ISA should be drafted and coordinated for signature.

ISA/MOU/MOAs may become invalid if the security posture of a node or the WAN itself changes. Changes must be evaluated by the signing AOs. The AOs will determine the impact (if any) on the authorization of the WAN and/or the validity of the ISA. Changes that may affect the security posture of the WAN or a node should be approved by the AOs prior to implementation.

8.5 Unified Networks

A unified network applies when all involved AOs concur that there will be a single security policy for the entire WAN. For WANs where all the nodes are authorized by DSS, the AO of the host node will authorize the network.

8.6 International Interconnections

Requests to establish international secure communications links between U.S. cleared contractors and foreign governments or foreign cleared contractors require additional supporting artifacts. When submitting the SSP within OBMS, the ISSM will select "International" as a special category for the IS/Unique Identification (UID). The SSP format can be used to support the official Secure Communications Plan (SCP) for approval. If a separate SCP is approved by the Designated Security Authorities (DSAs) or as part of a Program Security Instruction (PSI), the SCP will become an attachment to the SSP. Industry will include the following as supporting documentation with the SSP:

a. Export Authorization

b. Export Procedures

c. PSI (if applicable)

Specific Requirements

The following security requirements must be met for each communication node for the transmission of classified information:

a. The FSO/ISSM will appoint a cleared contractor employee as the designated representative of the communication node. The designated representative may be the ISSM, ISSO or another designee.

b. The FSO will appoint one or more Releasing Officers (RO) and Designated System Operators (DSO) for the communication node that will be appropriately trained. The ROs and DSOs must possess a security clearance at least to the highest classification level of the accessible classified information, and be a cleared contractor employee and citizen of the nation in which the communication node is located. The RO will be designated in writing as an empowered official to act on behalf of their respective companies. Each RO will have the authority to ensure any aspect of a proposed export or temporary import and verify the legality of the transaction and the accuracy of the information to be transferred. The RO may refuse to sign any request for release without prejudice or other adverse recourse.

c. The ISR will brief the FSOs, who will in turn brief the relevant staff, RO, and DSO on what information and technology is releasable under the contract. The employees will acknowledge the briefing in writing. The boundaries of what information is releasable will be carefully defined, particularly in cases where associated technology or information is not releasable. The briefing record will include the date, the identity of the

persons conducting and receiving the briefing, and specific acknowledgment by the person being briefed that they:

i. Understand the extent of the information and technology approved for release.

ii. Are familiar with the security procedures and record keeping requirements pertinent to these transmissions.

iii. Are aware of the criminal penalties that attach to violations of the export statutes.

iv. Have been given a Government POC who can clarify the nature and extent of the material that may be released or the applicable security procedures.

d. Only DSOs will be authorized to place and receive calls and/or to operate equipment.

e. The DSO will be thoroughly familiar with the technical data to be transferred, the project related technology export licenses, and the specific description of material that is authorized for disclosure.

f. The DSO will be responsible for notifying the FSO/ISSM of any required maintenance or repair to the net hardware.

g. The ISSM or designee and the DSOs will be responsible for the secure operation of the communication node in accordance with these instructions and Local Operating Procedures (LOPs).

h. The FSO or ISSM for the system will prepare LOPs for the communication node for the AO as an attachment to the SSP.

Authority to Communicate – Authority to activate the secure dedicated communications link will be granted by the AO after concurrences are received from the DSAs from the United States and the Foreign Government.

8.7 Federal Information Systems

Federal ISs are owned and authorized by a U.S. Federal Agency. The operation of Federal ISs in cleared contractor facilities under DSS cognizance may occur in the following circumstances:

1. A formal agreement between the IO and the cleared contractor has been established. The agreement outlines:

   a. The need for the Federal IS to be in a designated area of the cleared contractor facility.

   b. Security oversight will be provided by the government customer or applicable IO.

   c. DSS no longer has oversight of the designated government space.

   d. Physical security and AO responsibilities belong to the government customer or applicable IO.

The IO will:

a. Establish a formal agreement with the cleared contractor facility which spells out security requirements for the government dedicated space.

b. Oversee the physical security of the physically separated space (e.g. office, room, or building) designated by the cleared contractor.

c. Assess, authorize, and maintain the IS in accordance with established government procedures.

d. Maintain accountability of system hardware and software in accordance with government procedures.

The ISSP will:

a. Ensure that a formal agreement from the cleared contractor is readily available, and review the agreement to validate the approved location of the Federal IS. Example: If DSS security oversight responsibilities are removed within the contract (DD254) for a specific room and corresponding program, the government customer or applicable IO will approve the space and the system/network within.

b. Verify the space is clearly identified as designated government space and that it is physically separated (e.g., office, room, or building) from other cleared contractor operations.

2. A formal agreement is NOT in place between the IO and the cleared contractor for a designated area within the cleared contractor facility, but the Federal IS directly supports a program or contract already functioning in a formally approved area under DSS security oversight (e.g., Closed Area, Special Access Program Facility (SAPF)). Note: DSS will not approve a Closed Area for the sole purpose of safeguarding a Federal IS. Under this circumstance, the following criteria must be met:

a. The government customer or applicable IO maintains accountability for the Federal IS and serves as the AO.

b. The Federal IS is fully accounted for by the owning Agency; associated Federal Agency property labels will be affixed accordingly.

c. There are no connections between the Federal IS and any IS authorized by DSS.

d. There are no unapproved backside connections between the Federal IS and the DISN/DoDIN (e.g., SIPRNet).

e. The inclusion of a Federal IS in an area under DSS cognizance will not require physical security requirements beyond those established by the NISP and approved by DSS for classified processing.

The IO will:

a. Submit a memorandum to the DSS AO requesting approval for a Federal IS to process at the cleared contractor facility.

b. Maintain accountability and serve as the AO for the Federal IS.

c. Provide the cleared contractor guidance related to the secure operation and maintenance of the Federal IS.

d. Ensure that the inclusion of a Federal IS in an area under DSS security oversight will not require physical security requirements beyond those established by the NISP and approved by DSS for classified processing.

The ISSP will:

a. Verify that the Federal IS directly supports a program or contract already functioning in the closed area.

b. Ensure there are no connections between the Federal IS and any IS authorized by DSS.

c. Ensure there are no unapproved backside connections between the Federal IS and the DISN/DoDIN (e.g., SIPRNet).

d. Identify any unlabeled IT equipment in the space and determine its status.

e. Provide recommendation to the DSS AO for the IO request memorandum to acknowledge or deny the request to operate the Federal IS in the approved area.

f. Ensure the Federal IS will be operating in a formally approved area under DSS security oversight cognizance (e.g., Closed Area, SAPF, General Services Administration (GSA) safe, etc.).

The IO request to operate the Federal IS must include the following information:

Non-SAP Facilities – The Federal IS authorization letter, IO contact information, attestation to the above Federal IS requirements/responsibilities, and any additional information deemed necessary by the DSS AO.

SAP Facility (SAPF) in which DSS has oversight of the SAP – The responsible government Program Security Officer (PSO) must provide a letter to the DSS SAP office identifying the Federal IS, IO, ATO date, and PSO contact information.

If the Federal IS requirements/responsibilities are in place, the DSS AO will provide acknowledgment to the cleared contractor facility. The DSS acknowledgement, memorandum request, and any accompanying information will be maintained in the area with the Federal IS. The Federal IS and all associated media must be properly marked and protected in accordance

with applicable governing policies and program SCG(s). If obvious security concerns associated with the Federal IS are identified during routine DSS assessment activities, DSS will coordinate with the facility ISSM and contact the IO.

8.8 Special Categories

Special category systems, as described in NISPOM, Chapter 8, Section 304, will follow the same authorization process as all other ISs. However, it is expected they will implement a tailored set of security controls and make use of compensating controls (when necessary) to provide the acceptable level of protection. Specific application of security measures to protect the IS will be addressed in the SSP.

The cleared contractor will select and implement the appropriate baseline of security controls, and when necessary, apply compensating controls to provide adequate security of the IS. The ISSM will provide the AO with complete rationale and justification for how the compensating controls provide an equivalent security capability or level of protection for the ISs.

The AO assesses the risk of operating the Special Categories ISs with the cleared contractor's recommended set of compensating security controls. If the AO determines the risk is too high, the AO may require additional justification from the IO. The IO may recommend alternate or additional compensating security controls, or recommend that the AO not authorize the system in its present security configuration.

8.8.1 Tactical, Embedded, Data-Acquisition, Legacy, and Special-Purpose Systems

Tactical, embedded, data-acquisition, legacy, and special-purpose systems are Special Categories of systems requiring alternative set of controls not readily available in typical systems. Some ISs are incapable of being modified by users and are designed and implemented to provide a very limited set of predetermined functions. These systems are considered members of a special category, as are data-acquisition systems and other special-purpose test type systems. If an IS meets the criteria of a legacy IS (e.g., incapable of meeting the baseline security control requirements), authorization for continued use of a legacy IS may be authorized by the AO.

8.8.2 Mobile Systems

Mobile systems may be periodically relocated to another cleared contractor facility or government site. A mobile system may be a complete system or components of a larger, more complex system. Special procedures are required to document applicability and control, and to account for the movement, operations, and security of systems that are relocated to alternative locations. The mobile processing procedures will include details regarding the site's physical environment. If a mobile system is in place for 120 days or more, the cleared contractor must submit a SSP so that DSS can conduct the appropriate risk management evaluation. When a mobile system requires relocation, the cleared contractor must provide the ISSP with a notice of seven working days before the date of relocation. The cleared contractor must submit to the ISSP a mobile processing plan that addresses all aspects of security, to include secure movement, physical security, and operations at the new location before relocation. Please refer to the Mobility System Plan (Appendix G).

8.8.3 Diskless Workstation

A diskless workstation is a system that boots either from a CD or the local network and lacks the ability to store data locally to the machine. These types of systems require authorization. The established baseline security controls can be tailored to address the specifics of that system.

The ISSM will submit an SSP package with the proposed tailored security control set for review by the ISSP, as they do with other systems. The ISSP will evaluate the SSP package to determine if the management, operational, and technical controls identified in the plan are adequate to protect the classified information residing on the IS, with the understanding that several categories of systems can be adequately secured without implementation of the complete security control set.

8.8.4 Multifunction Devices

Multifunction Devices (MFDs) combine a PC, printer, and scanner into one container. These devices typically have non-volatile memory, hard drives, an operating system, and networking capability. Some utilize Radio Frequency Identification (RFID) technology for device inventory or status management. If the device has the capability to retain data upon a reboot, clearing procedures are required. Devices with data retention capabilities may require authorization.

Separate authorization is not required for devices when connected to an IS as a peripheral device. In these instances, the multifunction device should be included in the connected system's authorization plan. In particular, area upgrade and monitoring may be necessary to ensure physical security is applicable to these systems.

8.8.5 Virtualization

For systems that employ virtualization, there may be one or more virtual systems on one or more redundant sets of hardware. In cases where the virtual machine operates solely within the boundary of the host machine (e.g. no networked communication with other hosts or external connections), technical protection measures are required to be configured on the host machine and the individual virtual machine images residing on the host system. If virtual machines are configured to communicate with other systems on a LAN/WAN via a shared network interface on the host system (e.g., bridged, NAT), technical protection measures commensurate with the system type and purpose are required to be configured on the virtual machine images. The ISSM will document the use and purpose of each OS used in a virtual environment within the SSP as well as the technical protection measures in place to filter network communication external to the host.

8.8.6 Test Equipment

Test equipment with non-volatile memory that is going to process or retain classified information requires authorization. In cases where there are no technical security features associated with the test equipment, abbreviated procedures may be used in lieu of the standard SSP to identify areas such as clearing/sanitization procedures and physical security. Sanitization procedures (e.g., Certificate of Volatility from the manufacturer) for all test equipment, classified or unclassified (volatile memory included), should be included in the SSP. The cleared contractor must have some type of clearance or sanitization procedure in order to use the equipment for other

unclassified processing. Test equipment manufacturers have published clearing and sanitization procedures for their test equipment. The ISSP will ensure these documents meet the requirements for sanitization. In situations where user accessible or configurable data is contained in EEPROM or Flash EPROM, the only approved procedures are those provided by the manufacturer. Additional requirements in the clearing and sanitization matrix also apply. The ISSP will verify sanitization procedures are properly implemented to ensure the equipment is properly sanitized. In some cases, additional requirements may be applied if the sanitization procedure does not address all the memory on the system.

8.8.7 Peripherals

As technology advances, more and more devices are becoming network capable. Devices such as MFDs, security cameras, Smart TVs, and Uninterruptable Power Supply (UPS) systems frequently come with an Ethernet interface for network connectivity. These devices are designed to work with minimal configuration necessary in order to ensure ease of use. Unfortunately, with this ease of use often comes increased risk to the network.

The following cyber security configurations will be implemented and verified for peripheral devices:

a. Only network protocol that is enabled is Transmission Control Protocol/Internet Protocol (TCP/IP) unless approved by the AO.

b. All management protocols are disabled unless approved by the AO.

c. A firewall or router rule exists to block all ingress and egress traffic from the enclave perimeter to the peripheral.

d. Upgraded to the most current firmware available.

e. Configured to use the most current firmware available.

f. Default passwords and Simple Network Management Protocol (SNMP) community strings have been replaced with complex passwords.

g. Configuration state (passwords, service settings, etc.) is maintained after a power down or reboot.

h. Remote management only by the system administrator from specific IP addresses or from system administrator workstations using latest secure protocols (e.g., SSH, HTTPS, etc.).

i. Have auditing fully enabled for those devices that can generate audits.

j. Unauthorized access is prevented; repair procedures do not result in unauthorized dissemination of or access to classified information.

k. Equipment parts are replaced and destroyed in the appropriate manner when classified information cannot be removed.

l. Appropriately knowledgeable, cleared personnel inspect equipment and associated media used to process classified information before the equipment is removed from protected areas to ensure there is no retained classified information.

m. File shares have the appropriate discretionary access control list in place.

n. Configured to prevent non-administrators from altering the global configuration of the device.

9 TYPES OF SECURITY PLANS

In order to accommodate timely reviews, it is recommended that plans be submitted using the applicable DSS-provided SSP and artifact templates. The templates are located on the DSS RMF Website: http://www.dss.mil/rmf/. Completed plans and supporting artifacts should be kept from public disclosure.

There are two types of plans that can be submitted to the AO:

a. System Security Plan (SSP)

b. Master System Security Plan (MSSP)

9.1 System Security Plan

The SSP is a formal document that provides an overview of the security requirements for an IS and describes the security controls in place or planned for meeting those requirements. The process flow for submitting SSP packages is explained on the OBMS external site: http://www.dss.mil/is/obms.html.

9.2 Master System Security Plan (MSSP) - Type Authorization

The term “Master” is associated with an SSP that grants type authorization. Type authorization is an official authorization decision to employ identical copies of an IS or subsystem in specified environments of operation. This form of authorization allows a single MSSP to be developed for an archetype (common) version of an IS that is deployed within a specified facility (under a single CAGE code), resulting in a single ATO. Type authorization will only be granted if the AO/ISSP has determined that the ISSM has the requisite knowledge and skills. Type authorization is used in conjunction with the authorization of site-specific controls (e.g., physical and environmental protection controls, personnel security controls) inherited by the IS.

The exception to type authorization are SIPRNet systems. The NISP SIPRNet Circuit Approval Process, in conjunction with the DISA DISN Connection Process Guide (CPG), must be followed for design, implementation, operation, and decommissioning (disposal) of SIPRNet systems.

The facility is not authorized to utilize a combination of conditions from multiple authorized MSSPs. The IS must be an exact copy. For example, a type authorized IS must be:

a. Operating under the same security categorization (low, moderate, or high).

b. Possessing the same technical configuration.

c. Possessing operating characteristics and security needs that are essentially the same (e.g., configuration, operating system (OS), hardware, risk profile, network policy, security suite, physical controls, etc.).

d. Residing in the same general operating environments.

e. Inheriting common security controls.

For additional identical systems, the ISSM is required to submit the updated SSP and associated supporting artifacts associated with the type authorized system via OBMS utilizing the Self-Certification tab. Identical systems must be acknowledged in OBMS by the ISSP prior to conducting classified processing. If the MSSP associated with type authorization is issued a DATO, all systems authorized under that MSSP are no longer permitted to process classified information.

APPENDIX A: SECURITY CONTROLS (MODERATE-LOW-LOW)

The DSS Moderate-Low-Low (M-L-L) Security Control baseline is available in spreadsheet form on the DSS RMF information resource Webpage, located at http://www.dss.mil/rmf/.The spreadsheet details the requirements for implementation of selected security controls and supplemental guidance, as well as DSS-specific implementation guidelines.

APPENDIX B: DSS OVERLAYS

DSS Overlay

The DSS overlay identifies security control specifications needed to safeguard classified information that is stored, processed, or transmitted. The DSS overlay adopts a minimum baseline of Moderate-Low-Low (M-L-L). This overlay applies to the following types of systems:

- Standalone Systems
  - Single User Standalone (SUSA)
  - Multi User Standalone (MUSA)
- Isolated LAN (ISOL)/Peer-to-Peer (P2P)

References

- CNSSI 1253, Security Categorization and Control Selection for National Security Systems
- NIST SP 800-53, Rev. 4, Recommended Security Controls for Federal Information Systems and Organizations

Characteristics and Assumptions of Standalone Systems

Due to complexity and/or resource constraints, specific security controls may not be applicable to standalone Information Systems (IS). This overlay provides guidance on the security controls required to be implemented on standalone ISs. A standalone system is a single desktop or similar component with no network cards activated or connected. It is not connected to any other system or network and has no Protected Distribution System (PDS) in place.

Characteristics and Assumptions of Isolated LANs (ISOL)/Peer-to-Peer (P2P)

A LAN/P2P is defined as a group of computers and network devices connected together over a relatively small geographic area. A LAN may be isolated – system boundary is completely contained to within the Facility/Building. It is not an Interconnected System to an external network.

An isolated LAN typically has none of the following:

- Connectivity to any other LAN
- Voice over Internet Protocol (VoIP)
- Collaborative Computing

DSS Overlay – Table of Security Controls

The table below summarizes the security control specifications as they apply to the DSS overlay. The symbols used in the table are as follows:

- One dash "-" indicates the control **should not be** selected.
- The letter "G" indicates there is supplemental guidance, including specific tailoring guidance if applicable, for the control.

Tailoring Considerations

Additional tailoring of the DSS Overlay is permitted with the approval of the Authorizing Official (AO). Tailoring may be needed if additional overlays apply to the information system or to address unique circumstances in the system's environment.

Security Controls

Ctrl No	Ctrl Name	SUSA	MUSA	ISOL/P2P
AC-1	Access Control Policy and Procedures			
AC-2	Account Management			
AC-2 (1)	Account Management | Automated System Account Management	-	-	-
AC-2 (2)	Account Management | Removal of Temporary / Emergency Accounts	-	-	-
AC-2 (3)	Account Management | Disable Inactive Accounts	-	-	-
AC-2 (4)	Account Management | Automated Audit Actions			
AC-2 (5)	Account Management | Inactivity Logout			
AC-2 (7)	Account Management | Role Based Schemes	-		
AC-2 (9)	Account Management | Restrictions On Use Of Shared Groups / Accounts	-		
AC-2 (10)	Account Management | Shared / Group Account Credential Termination	-		
AC-2 (12)	Account Management | Account Monitoring / Atypical Usage	-		
AC-2 (13)	Account Management | Disable Accounts For High-Risk Individuals	-		
AC-3	Access Enforcement	-		
AC-3 (2)	Access Enforcement | Dual Authorization	-		
AC-3 (4)	Access Enforcement | Discretionary Access Control	-		

Ctrl No	Ctrl Name	SUSA	MUSA	ISOL/P2P
AC-4	Information Flow Enforcement			
AC-5	Separation Of Duties			
AC-6	Least Privilege			
AC-6 (1)	Least Privilege | Authorize Access To Security Functions			
AC-6 (2)	Least Privilege | Nonprivileged Access For Nonsecurity Functions			
AC-6 (5)	Least Privilege | Privileged Accounts			
AC-6 (7)	Least Privilege | Review Of User Privileges	-		
AC-6 (8)	Least Privilege | Privilege Levels For Code Execution			
AC-6 (9)	Least Privilege | Auditing Use Of Privileged Functions			
AC-6 (10)	Least Privilege | Prohibit Non-Privileged Users From Executing Privileged Functions			
AC-7	Unsuccessful Login Attempts	G		
AC-8	System Use Notification			
AC-10	Concurrent Session Control	-	-	
AC-11	Session Lock			
AC-11 (1)	Session Lock: Pattern Hiding Displays			
AC-12	Session Termination			
AC-12 (1)	Session Termination | User-Initiated Logouts/ Message Displays			
AC-14	Permitted Actions Without Identification Or Authentication			
AC-16	Security Attributes			
AC-16 (5)	Security Attributes | Attribute Displays For Output Devices			
AC-16 (6)	Security Attributes | Maintenance Of Attribute Association By Organization			
AC-16 (7)	Security Attributes | Consistent Attribute Interpretation	-	-	-
AC-17	Remote Access	-	-	-
AC-17 (1)	Remote Access | Automated Monitoring/Control	-	-	-

Ctrl No	Ctrl Name	SUSA	MUSA	ISOL/P2P
AC-17 (2)	Remote Access | Protection Of Confidentiality/Integrity Using Encryption	-	-	-
AC-17 (3)	Remote Access | Managed Access Control Points	-	-	-
AC-17 (4)	Remote Access | Privileged Commands/Access	-	-	-
AC-17 (6)	Remote Access | Protection Of Information	-	-	-
AC-17 (9)	Remote Access | Disconnect/ Disable Access	-	-	-
AC-18	Wireless Access			
AC-18 (1)	Wireless Access | Authentication & Encryption	-	-	
AC-18 (3)	Wireless Access | Disable Wireless Networking			
AC-18 (4)	Wireless Access | Restrict Configurations By Users	-	-	
AC-19	Access Control For Mobile Devices			
AC-19 (5)	Access Control For Mobile Devices | Full Device/ Container-Based Encryption			
AC-20	Use Of External Information Systems			
AC-20 (1)	Use Of External Information Systems | Limits On Authorized Use	-	-	
AC-20 (2)	Use Of External Information Systems |Portable Storage Devices			
AC-20 (3)	Use Of External Information Systems | Non-Organizationally Owned Systems / Components / Devices			
AC-20 (4)	Use Of External Information Systems | Network Accessible Storage Devices	-	-	
AC-21	Information Sharing			
AC-23	Data Mining Protection	-	-	
AT-1	Security Awareness & Training Policy And Procedures			
AT-2	Security Awareness Training			
AT-2 (2)	Security Awareness | Insider Threat			
AT-3	Role-Based Security Training			
AT-3 (2)	Security Training | Physical Security Controls			
AT-3 (4)	Security Training | Suspicious Communications And Anomalous System Behavior			

Ctrl No	Ctrl Name	SUSA	MUSA	ISOL/P2P
AT-4	Security Training Records			
AU-1	Audit And Accountability Policy And Procedures			
AU-2	Audit Events			
AU-2 (3)	Audit Events | Reviews And Updates			
AU-3	Content Of Audit Records			
AU-3 (1)	Content Of Audit Records | Additional Audit Information	-	-	
AU-4	Audit Storage Capacity			
AU-4 (1)	Audit Storage Capacity | Transfer To Alternate Storage	-	-	
AU-5	Response To Audit Processing Failures	G		
AU-5 (1)	Response To Audit Processing Failures | Audit Storage Capacity			
AU-6	Audit Review, Analysis, And Reporting	G		
AU-6 (1)	Audit Review, Analysis, And Reporting | Process Integration	-	-	-
AU-6 (3)	Audit Review, Analysis, And Reporting | Correlate Audit Repositories	-	-	-
AU-6 (4)	Audit Review, Analysis, And Reporting | Central Review And Analysis	-	-	-
AU-6 (5)	Audit Review, Analysis, And Reporting | Integration / Scanning And Monitoring Capabilities			
AU-6 (8)	Audit Review, Analysis, And Reporting | Full Text Analysis Of Privileged Commands	-	-	
AU-6 (9)	Audit Review, Analysis, And Reporting | Correlation With Information From Nontechnical Source			
AU-6 (10)	Audit Review, Analysis, And Reporting | Audit Level Adjustment			
AU-7	Audit Reduction And Report Generation	-		
AU-7 (1)	Audit Reduction And Report Generation | Automatic Processing	-	-	
AU-8	Time Stamps			
AU-8 (1)	Time Stamps | Synchronization With Authoritative Time Source	-	-	-
AU-9	Protection Of Audit Information			

Ctrl No	Ctrl Name	SUSA	MUSA	ISOL/P2P
AU-9 (4)	Protection Of Audit Information | Access By Subset Of Privileged Users	-		
AU-11	Audit Record Retention			
AU-11 (1)	Audit Record Retention | Long-Term Retrieval Capability			
AU-12	Audit Generation			
AU-12 (1)	Audit Generation | System-Wide / Time- Correlated Audit Trail			
AU-12 (3)	Audit Generation | Changes By Authorized Individuals			
AU-16	Cross-Organizational Auditing	-	-	-
AU-16 (1)	Cross-Organizational Auditing | Identity Preservation	-	-	-
AU-16 (2)	Cross-Organizational Auditing | Sharing of Audit Information	-	-	-
CA-1	Security Assessment And Authorization Policies & Procedures			
CA-2	Security Assessments			
CA-2 (1)	Security Assessments | Independent Assessors			
CA-3	System Interconnections	-	-	-
CA-3 (2)	System Interconnections | Classified National Security System Connections	-	-	-
CA-3 (5)	System Interconnections | Restrictions On External System Connections	-	-	
CA-5	Plan Of Action And Milestones			
CA-6	Security Authorization			
CA-7	Continuous Monitoring			
CA-7 (1)	Continuous Monitoring | Independent Assessment			
CA-9	Internal System Connections	-	-	
CM-1	Configuration Management Policy And Procedures			
CM-2	Baseline Configuration			
CM-2 (1)	Baseline Configuration | Reviews & Updates			
CM-2 (2)	Baseline Configuration | Automation Support For Accuracy / Currency			

Ctrl No	Ctrl Name	SUSA	MUSA	ISOL/P2P
CM-3	Configuration Change Control			
CM-3 (4)	Configuration Change Control | Security Representative			
CM-3 (6)	Configuration Change Control | Cryptography Management			
CM-4	Security Impact Analysis			
CM-5	Access Restrictions For Change			
CM-5 (5)	Access Restrictions For Change | Limit Production/Operational Privileges	-		
CM-5 (6)	Access Restrictions For Change | Limit Library Privileges	-		
CM-6	Configuration Settings			
CM-7	Least Functionality			
CM-7 (1)	Least Functionality | Periodic Review			
CM-7 (2)	Least Functionality | Prevent Program Execution	-	-	
CM-7 (3)	Least Functionality | Registration Compliance	-	-	-
CM-7 (5)	Least Functionality | Authorized Software / Whitelisting			
CM-8	Information System Component Inventory			
CM-8 (2)	Information System Component Inventory | Automated Maintenance	-	-	-
CM-8 (3)	Information System Component Inventory | Automated Unauthorized Component Detection	-	-	-
CM-9	Configuration Management Plan			
CM-10	Software Usage Restrictions			
CM-10 (1)	Software Usage Restrictions | Open Source Software			
CM-11	User-Installed Software			
CM-11 (2)	User-Installed Software | Prohibit Installation Without Privileged Status			
CP-1	Contingency Planning Policy And Procedures			
CP-2	Contingency Plan			
CP-3	Contingency Training			
CP-4	Contingency Plan Testing			

Ctrl No	Ctrl Name	SUSA	MUSA	ISOL/P2P
CP-7	Alternate Processing Site	-	-	
CP-9	Information System Backup			
CP-10	Information System Recovery And Reconstitution			
IA-1	Identification And Authentication Policy And Procedures			
IA-2	Identification And Authentication (Organizational Users)			
IA-2 (3)	Identification And Authentication | Local Access To Privileged Accounts	-	-	-
IA-2 (4)	Identification And Authentication | Local Access To Nonprivileged Accounts	-	-	-
IA-2 (5)	Identification And Authentication | Group Authentication	-		
IA-2 (8)	Identification And Authentication | Network Access To Privileged Accounts Replay Resistant	-	-	-
IA-2 (9)	Identification And Authentication | Network Access To Nonprivileged Accounts Replay Resistant	-	-	-
IA-2 (11)	Identification And Authentication | Remote Access - Separate Device	-	-	-
IA-3	Device Identification And Authentication	-	-	
IA-3 (1)	Device Identification And Authentication Cryptographic Bidirectional Authentication	-	-	
IA-4	Identifier Management			
IA-4 (4)	Identifier Management | Identify User Status	-	-	-
IA-5	Authenticator Management			
IA-5 (1)	Authenticator Management | Password- Based Authentication			
IA-5 (2)	Authenticator Management | PKI-Based Authentication	-	-	-
IA-5 (4)	Authenticator Management | Automated Support For Password Strength Determination			
IA-5 (7)	Authenticator Management | No Embedded Unencrypted Static Authenticators			
IA-5 (8)	Authenticator Management | Multiple Information System Accounts			
IA-5 (11)	Authenticator Management | Hardware Token-Based Authentication	-	-	-

Ctrl No	Ctrl Name	SUSA	MUSA	ISOL/P2P
IA-5 (13)	Authenticator Management | Expiration Of Cached Authenticators	-	-	
IA-5 (14)	Authenticator Management | Managing Content Of PKI Trust Stores	-	-	-
IA-6	Authenticator Feedback			
IA-7	Cryptographic Module Authentication			
IA-8	Identification And Authentication (Non-Organizational Users)	-		
IA-8 (1)	Identification And Authentication | Acceptance Of PIV Credentials From Other Agencies	-	-	-
IA-8 (2)	Identification And Authentication | Acceptance Of Third-Party Credentials	-	-	-
IA-8 (3)	Identification And Authentication | Use Of FICAM-Approved Products	-	-	-
IA-8 (4)	Identification And Authentication | Use Of FICAM-Issued Profiles	-	-	-
IR-1	Incident Response Policy And Procedures			
IR-2	Incident Response Training			
IR-3	Incident Response Testing			
IR-3 (2)	Incident Response Testing | Coordination With Related Plans			
IR-4	Incident Handling			
IR-4 (1)	Incident Handling | Automated Incident Handling Processes	G	G	
IR-4 (3)	Incident Handling | Continuity Of Operations			
IR-4 (4)	Incident Handling | Information Correlation			
IR-4 (6)	Incident Handling | Insider Threats - Specific Capabilities			
IR-4 (7)	Incident Handling | Insider Threats-Intra-Organization Coordination			
IR-4 (8)	Incident Handling | Correlation With External Organizations			
IR-5	Incident Monitoring			
IR-6	Incident Reporting			
IR-6 (1)	Incident Reporting | Automated Reporting	G	G	

Ctrl No	Ctrl Name	SUSA	MUSA	ISOL/P2P
IR-6 (2)	Incident Reporting | Vulnerabilities Related To Incidents			
IR-7	Incident Response Assistance			
IR-7 (1)	Incident Response Assistance | Automation Support For Availability Of Information / Support	G	G	
IR-7 (2)	Incident Response Assistance | Coordination With External Providers			
IR-8	Incident Response			
IR-9	Information Spillage Response			
IR-9 (1)	Information Spillage Response | Responsible Personnel			
IR-9 (2)	Information Spillage Response | Training			
IR-9 (4)	Information Spillage Response | Exposure To Unauthorized Personnel			
IR-10	Integrated Information Security Analysis Team	G	G	
MA-1	System Maintenance Policy And Procedures			
MA-2	Controlled Maintenance			
MA-3	Maintenance Tools			
MA-3 (2)	Maintenance Tools | Inspect Media			
MA-3 (3)	Maintenance Tools | Prevent Unauthorized Removal			
MA-4	Nonlocal Maintenance	-	-	
MA-4 (3)	Nonlocal Maintenance | Comparable Security/Sanitization	-	-	
MA-4 (6)	Nonlocal Maintenance | Cryptographic Protection	-	-	
MA-4 (7)	Nonlocal Maintenance | Remote Disconnect Verification	-	-	
MA-5	Maintenance Personnel			
MA-5(1)	Maintenance Personnel | Individuals Without Appropriate Access			
MP-1	Media Protection Policy And Procedures			
MP-2	Media Access			
MP-3	Media Marking			
MP-4	Media Storage			

Ctrl No	Ctrl Name	SUSA	MUSA	ISOL/P2P
MP-5	Media Transport			
MP-5 (3)	Media Transport | Custodians			
MP-5 (4)	Media Transport | Cryptographic Protection			
MP-6	Media Sanitization			
MP-6 (1)	Media Sanitization | Review/Approve/Track/Document/Verify			
MP-6 (2)	Media Sanitization | Equipment Testing			
MP-6 (3)	Media Sanitization | Nondestructive Techniques			
MP-7	Media Use			
MP-7 (1)	Media Use | Prohibit Use Without Owner			
MP-8	Media Downgrading			
MP-8 (1)	Media Downgrading | Documentation Of Process			
MP-8 (2)	Media Downgrading | Equipment Testing			
MP-8 (4)	Media Downgrading | Classified Information			
PE-1	Physical And Environmental Protection Policy And Procedures			
PE-2	Physical Access Authorizations			
PE-2 (3)	Physical Access Authorizations | Restrict Unescorted Access			
PE-3	Physical Access Control			
PE-3 (1)	Physical Access Control | Information System Access			
PE-3 (2)	Physical Access Control | Facility/Information System Boundaries			
PE-3 (3)	Physical Access Control | Continuous Guards/Alarms/Monitoring			
PE-4	Access Control For Transmission Medium	-	-	
PE-5	Access Control For Output Devices			
PE-5 (3)	Access Control For Output Devices | Marking Output Devices			
PE-6	Monitoring Physical Access			
PE-6 (1)	Monitoring Physical Access | Intrusion Alarms / Surveillance Equipment			

Ctrl No	Ctrl Name	SUSA	MUSA	ISOL/P2P
PE-8	Visitor Access Records			
PE-12	Emergency Lighting			
PE-13	Fire Protection			
PE-14	Temperature And Humidity Controls			
PE-15	Water Damage Protection			
PE-16	Delivery And Removal			
PE-17	Alternate Work Site	-	-	
PE-19	Information Leakage			
PE-19 (1)	Information Leakage | National Emissions/TEMPEST Policies and Procedures			
PL-1	Security Planning Policy And Procedures			
PL-2	System Security Plan			
PL-2 (3)	System Security Plan | Plan / Coordinate With Other Organizational Entities			
PL-4	Rules Of Behavior			
PL-4 (1)	Rules Of Behavior | Social Media And Networking Restrictions			
PL-8	Information Security Architecture			
PL-8 (1)	Information Security Architecture | Defense-In-Depth			
PL-8 (2)	Information Security Architecture | Supplier Diversity			
PM-1	Information Security Program Plan			
PM-3	Information Security Resources			
PM-4	Plan Of Action And Milestones Process			
PM-5	Information System Inventory			
PM-6	Information Security Measures Of Performance			
PM-7	Enterprise Architecture			
PM-8	Critical Infrastructure Plan			
PM-9	Risk Management Strategy			
PM-10	Security Authorization Process			

Ctrl No	Ctrl Name	SUSA	MUSA	ISOL/P2P
PM-11	Mission/Business Process Definition			
PM-12	Insider Threat Program			
PM-13	Information Security Workforce			
PM-14	Testing, Training, And Monitoring			
PM-15	Contacts With Security Groups And Associations			
PM-16	Threat Awareness Program			
PS-1	Personnel Security Policy And Procedures			
PS-2	Position Risk Designation			
PS-3	Personnel Screening			
PS-3 (1)	Personnel Screening | Classified Information			
PS-4	Personnel Termination			
PS-4 (1)	Personnel Termination | Post- Employment Requirements			
PS-5	Personnel Transfer			
PS-6	Access Agreements			
PS-6 (2)	Access Agreements | Classified Information Requiring Special Protection			
PS-6 (3)	Access Agreements | Post-Employment Requirements			
PS-7	Third-Party Personnel Security			
PS-8	Personnel Sanctions			
RA-1	Risk Assessment Policy And Procedures			
RA-2	Security Categorization			
RA-3	Risk Assessment			
RA-5	Vulnerability Scanning			
RA-5 (1)	Vulnerability Scanning | Update Tool Capability			
RA-5 (2)	Vulnerability Scanning | Update By Frequency/Prior To New Scan/When Identified			
RA-5 (4)	Vulnerability Scanning | Discoverable Information			
RA-5 (5)	Vulnerability Scanning | Privileged Access			
RA-6	Technical Surveillance Countermeasures Survey			

Ctrl No	Ctrl Name	SUSA	MUSA	ISOL/P2P
SA-1	System And Services Acquisition Policy And Procedures			
SA-2	Allocation Of Resources			
SA-3	System Development Life Cycle			
SA-4	Acquisition Process			
SA-4 (1)	Acquisition Process | Functional Properties Of Security Controls			
SA-4 (2)	Acquisition Process | Design / Implementation Information For Security Controls			
SA-4 (6)	Acquisition Process | Use Of Information Assurance Products			
SA-4 (7)	Acquisition Process | NIAP-Approved Protection Profiles			
SA-4 (9)	Acquisition Process | Functions / Ports / Protocols / Services In Use			
SA-4 (10)	Acquisition Process | Use Of Approved PIV Products	-	-	
SA-5	Information System Documentation			
SA-8	Security Engineering Principles			
SA-9	External Information System Services	-	-	-
SA-9 (1)	External Information System | Risk Assessment/Organizational Approvals	-	-	-
SA-9 (2)	External Information Systems | Identification Of Functions / Ports / Protocols / Services	-	-	-
SA-10	Developer Configuration Management			
SA-10 (1)	Developer Configuration Management | Software/Firmware Integrity Verification			
SA-11	Developer Security Testing And Evaluation			
SA-12	Supply Chain Protection			
SA-15	Development Process, Standards, And Tools			
SA-15 (9)	Development Process, Standards, And Tools | Use Of Live Data			
SA-19	Component Authenticity			
SA-22	Unsupported System Components			

Ctrl No	Ctrl Name	SUSA	MUSA	ISOL/P2P
SC-1	Systems And Communications Protection Policy And Procedures			
SC-2	Application Partitioning			
SC-3	Security Function Isolation			
SC-4	Information In Shared Resources	-		
SC-4 (2)	Information In Shared Resources | Periods Processing	G	G	G
SC-5	Denial Of Service Protection	-	-	-
SC-5 (1)	Denial Of Service Protection | Restrict Internal Users	-	-	-
SC-7	Boundary Protection	-	-	-
SC-7 (3)	Boundary Protection | Access Points	-	-	-
SC-7 (4)	Boundary Protection | External Telecommunications Services	-	-	-
SC-7 (5)	Boundary Protection | Deny By Default/Allow By Exception	-	-	-
SC-7 (7)	Boundary Protection | Prevent Split Tunneling For Remote Devices	-	-	-
SC-7 (8)	Boundary Protection | Route Traffic To Authenticated Proxy Servers	-	-	-
SC-7 (9)	Boundary Protection | Restrict Threatening Outgoing Communications Traffic	-	-	-
SC-7 (10)	Boundary Protection | Prevent Unauthorized Exfiltration	-	-	-
SC-7 (11)	Boundary Protection | Restrict Incoming Communications Traffic	-	-	-
SC-7 (12)	Boundary Protection | Host-Based Protection	-	-	-
SC-7 (13)	Boundary Protection | Isolation Of Security Tools/Mechanisms/Support Components	-	-	-
SC-7 (14)	Boundary Protection | Protects Against Unauthorized Physical Connections	-	-	-
SC-8	Transmission Confidentiality And Integrity	-	-	-
SC-8 (1)	Transmission Confidentiality And Integrity | Cryptographic Or Alternate Physical Protection	-	-	-
SC-8 (2)	Transmission Confidentiality And Integrity | Pre / Post Transmission Handling	-	-	-

Ctrl No	Ctrl Name	SUSA	MUSA	ISOL/P2P
SC-8 (3)	Transmission Confidentiality And Integrity | Cryptographic Protection For Message Externals	-	-	-
SC-8 (4)	Transmission Confidentiality And Integrity | Conceal / Randomize Communications	-	-	-
SC-10	Network Disconnect	-	-	-
SC-12	Cryptographic Key Establishment And Management			
SC-12 (2)	Cryptographic Key Establishment And Management | Symmetric Keys			
SC-12 (3)	Cryptographic Key Establishment And Management | Asymmetric Keys			
SC-13	Cryptographic Protection			
SC-15	Collaborative Computing Devices	-	-	-
SC-15 (3)	Collaborative Computing Devices | Disabling/Removal in Secure Work Areas	-	-	-
SC-17	Public Key Infrastructure Certificates	-	-	
SC-18	Mobile Code			
SC-18 (1)	Mobile Code | Identify Unacceptable Code/Take Corrective Actions			
SC-18 (2)	Mobile Code | Acquisition/Development/Use			
SC-18 (3)	Mobile Code | Prevent Downloading/Execution			
SC-18 (4)	Mobile Code | Prevent Automatic Execution			
SC-19	Voice Over Internet Protocol (VoIP)	-	-	-
SC-20	Secure Name/Address Resolution Service (Authoritative Source)	-	-	-
SC-21	Secure Name/Address Resolution Service (Recursive Or Caching Resolver)	-	-	-
SC-22	Architecture And Provisioning For Name/ Address Resolution Service	-	-	-
SC-23	Session Authenticity	-	-	-
SC-23 (1)	Session Authenticity | Invalidate Session Identifiers At Logout	-	-	-
SC-23 (3)	Session Authenticity | Unique Session Identifiers With Randomization	-	-	-
SC-23 (5)	Session Authenticity | Allowed Certificate Authorities	-	-	-

Ctrl No	Ctrl Name	SUSA	MUSA	ISOL/P2P
SC-28	Protection Of Information At Rest			
SC-28 (1)	Protection Of Information At Rest | Cryptographic Protection			
SC-38	Operations Security			
SC-39	Process Isolation			
SC-42	Sensor Capability And Data	-	-	
SC-42 (3)	Sensor Capability And Data | Prohibit Use Of Devices	-	-	
SI-1	System And Information Integrity Policy And Procedures			
SI-2	Flaw Remediation			
SI-2 (1)	Flaw Remediation | Central Management			
SI-2 (2)	Flaw Remediation | Automated Flaw Remediation Status	-	-	
SI-2 (3)	Flaw Remediation | Time To Remediate Flaws / Benchmarks For Corrective Actions	-	-	
SI-2 (6)	Flaw Remediation | Removal Of Previous Versions Of Software / Firmware			
SI-3	Malicious Code Protection			
SI-3 (1)	Malicious Code Protection | Central Management	-	-	
SI-3 (2)	Malicious Code Protection | Automatic Updates	-	-	
SI-3 (10)	Malicious Code Protection | Malicious Code Analysis	G	G	
SI-4	Information System Monitoring			
SI-4 (1)	Information System Monitoring | System- Wide Intrusion Detection System	-	-	-
SI-4 (2)	Information System Monitoring | Automated Tools For Real-Time Analysis	-	-	-
SI-4 (4)	Information System Monitoring | Inbound And Outbound Communications Traffic	-	-	-
SI-4 (5)	Information System Monitoring | System- Generated Alerts	-	-	-
SI-4 (10)	Information System Monitoring | Visibility Of Encrypted Communications	-	-	-
SI-4 (11)	Information System Monitoring | Analyze Communications Traffic Anomalies	-	-	-

Ctrl No	Ctrl Name	SUSA	MUSA	ISOL/P2P
SI-4 (12)	Information System Monitoring | Automated Alerts	-	-	
SI-4 (14)	Information System Monitoring | Wireless Intrusion Detection	-	-	
SI-4 (15)	Information System Monitoring | Wireless To Wireline Communications	-	-	
SI-4 (16)	Information System Monitoring | Correlate Monitoring Information	-	-	
SI-4 (19)	Information System Monitoring | Individuals Posing Greater Risk			
SI-4 (20)	Information System Monitoring | Privileged User			
SI-4 (21)	Information System Monitoring | Probationary Periods	-	-	
SI-4 (22)	Information System Monitoring | Unauthorized Network Services	-	-	
SI-4 (23)	Information System Monitoring | Host- Based Devices			
SI-5	Security Alerts, Advisories, And Directives			
SI-7 (14)	Software, Firmware, And Information Integrity | Binary Or Machine Executable Code	-	-	
SI-10	Information Input Validation	-	-	
SI-11	Error Handling			
SI-12	Information Handling And Retention			

APPENDIX C: RISK ASSESSMENT REPORT (RAR) TEMPLATE

<ORGANIZATION>
<SYSTEM NAME>
<DATE>

Record of Changes:

Version	Date	Sections Modified	Description of Changes
1.0	DD Mm YY	Initial RAR	

System Description

The <*System Name* and *Unique Identifier*> consists of <*System Description*> processing <*Classification Level*> data. The risk categorization for this Information System (IS) is assessed as <*e.g., Moderate-Low-Low*>.

IS# <*Unique Identifier*> is located <*insert physical environment details*>. The IS <*list all system connections and inter-connections, or state "has no connections, (wired or wireless)*>. This IS is used for <*system purpose/function*>, in support of performance on the <*list all program and/or contract information*>. The IS <*provide any system specific details, such as Mobility*>.

The Information Owner is <*insert POC information, including address and phone number*>.

The ISSM is <*insert POC information, including address and phone number*>.

The ISSO is <*insert POC information, including address and phone number*>.

Scope

The scope of this risk assessment is focused on the system's use of resources and controls to mitigate vulnerabilities exploitable by threat agents (internal and external) identified during the RMF control selection process, based on the system's categorization.

This initial assessment will be a Tier 3 or "information system level" risk assessment. While not entirely comprehensive of all threats and vulnerabilities to the IS, this assessment will include any known risks related to the incomplete or inadequate implementation of the NIST SP 800-53 controls selected for this system. This document will be updated after certification testing to include any vulnerabilities or observations by the independent assessment team. Data collected during this assessment may be used to support higher level risk assessments at the mission/business or organization level.

<Identify assumptions, constraints, timeframe. This section will include the following information:

- *Range or scope of threats considered in the assessment*
- *Summary of tools/methods used to ensure NIST SP 800-53 compliance*
- *Details regarding any instances of non-compliance*
- *Relevant operating conditions and physical security conditions*
- *Timeframe supported by the assessment (Example: security-relevant changes that are anticipated before the authorization, expiration of the existing authorization, etc.).>*

Purpose

<Provide details on why this risk assessment is being conducted, including whether it is an initial or other subsequent assessment, and state the circumstances that prompted the assessment. Example: This initial risk assessment was conducted to document areas where the selection and implementation of RMF controls may have left residual risk. This will provide security control assessors and authorizing officials an upfront risk profile.>

Risk Assessment Approach

This initial risk assessment was conducted using the guidelines outlined in the *NIST SP 800-30, Guide for Conducting Risk Assessments*. A *<SELECT QUALITATIVE / QUANTITATIVE / SEMI-QUANTITATIVE>* approach will be utilized for this assessment. Risk will be determined based on a threat event, the likelihood of that threat event occurring, known system vulnerabilities, mitigating factors, and consequences/impact to mission.

The following table is provided as a list of sample threat sources. Use this table to determine relevant threats to the system.

Table 1: Sample Threat Sources (see NIST SP 800-30 for complete list)

TYPE OF THREAT SOURCE	DESCRIPTION
ADVERSARIAL - Individual (outsider, insider, trusted, privileged) - Group (ad-hoc or established) - Organization (competitor, supplier, partner, customer) - Nation state	Individuals, groups, organizations, or states that seek to exploit the organization's dependence on cyber resources (e.g., information in electronic form, information and communications, and the communications and information-handling capabilities provided by those technologies.
ADVERSARIAL - Standard user - Privileged user/Administrator	Erroneous actions taken by individuals in the course of executing everyday responsibilities.

TYPE OF THREAT SOURCE	DESCRIPTION
STRUCTURAL - IT Equipment (storage, processing, comm., display, sensor, controller) - Environmental conditions • Temperature/humidity controls • Power supply - Software • Operating system • Networking • General-purpose application • Mission-specific application	Failures of equipment, environmental controls, or software due to aging, resource depletion, or other circumstances which exceed expected operating parameters.
ENVIRONMENTAL - Natural or man-made (fire, flood, earthquake, etc.) - Unusual natural event (e.g., sunspots) - Infrastructure failure/outage (electrical, telecomm)	Natural disasters and failures of critical infrastructures on which the organization depends, but is outside the control of the organization. Can be characterized in terms of severity and duration.

The following tables from the NIST SP 800-30 were used to assign values to likelihood, impact, and risk:

Table 2: Assessment Scale – Likelihood of Threat Event Initiation (Adversarial)

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Adversary is **almost certain** to initiate the threat event.
High	80-95	8	Adversary is **highly likely** to initiate the threat event.
Moderate	21-79	5	Adversary is **somewhat likely** to initiate the threat event.
Low	5-20	2	Adversary is **unlikely** to initiate the threat event.
Very Low	0-4	0	Adversary is **highly unlikely** to initiate the threat event

Table 3: Assessment Scale – Likelihood of Threat Event Occurrence (Non-adversarial)

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Error, accident, or act of nature is **almost certain** to occur; or occurs **more than 100 times per year**.
High	80-95	8	Error, accident, or act of nature is **highly likely** to occur; or occurs **between 10-100 times per year**.

Qualitative Values	Semi-Quantitative Values		Description
Moderate	21-79	5	Error, accident, or act of nature is **somewhat likely** to occur; or occurs **between 1-10 times per year**.
Low	5-20	2	Error, accident, or act of nature is **unlikely** to occur; or occurs **less than once a year,** but **more than once every 10 years**.
Very Low	0-4	0	Error, accident, or act of nature is **highly unlikely** to occur; or occurs **less than once every 10 years**.

Table 4: Assessment Scale – Impact of Threat Events

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	80-95	8	The threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. A severe or catastrophic adverse effect means that, for example, the threat event 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 assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.
Moderate	21-79	5	The threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A serious adverse effect means that, for example, the threat event 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 the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

Qualitative Values	Semi-Quantitative Values		Description
Low	5-20	2	The threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A limited adverse effect means that, for example, the threat event 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 the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Very Low	0-4	0	The threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation.

Table 5: Assessment Scale – Level of Risk

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	80-95	8	Threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Moderate	21-79	5	Threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Low	5-20	2	Threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Very Low	0-4	0	Threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.

Table 6: Assessment Scale – Level of Risk (Combination of Likelihood and Impact)

Likelihood (That Occurrence Results in Adverse Impact)	Level of Impact				
	Very Low	Low	Moderate	High	Very High
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

Risk Assessment Approach

Determine relevant threats to the IS. List the risks to the IS in the Risk Assessment Results table below and detail the relevant mitigating factors and controls. Refer to NIST SP 800-30 for further guidance, examples, and suggestions.

Risk Assessment Results

Threat Event	Vulnerabilities / Predisposing Characteristics	Mitigating Factors	Likelihood (Tbl 2 or 3)	Impact (Table 4)	Risk (Tbls 5 & 6)
e.g. Hurricane	*Power Outage*	*Backup generators*	*Moderate*	*Low*	*Low*

* Likelihood / Impact / Risk = Very High, High, Moderate, Low, or Very Low

APPENDIX D: POA&M TEMPLATE

Plan of Action and Milestones (POA&M)

System Name Company/Organization Name		Date of this POA&M Date of Last Update Date of Original POA&M	

ISSM Information

Name Phone Email		IS Type UID	

Item Identifier	Weakness or Deficiency	Security Control	POC	Resources Required	Scheduled Completion Date	Milestones with Completion Dates	Changes to Milestones	Weakness/ Deficiency Identified by	Risk Level (Low/Med/High)	Estimated Cost	Status	Comments

The POA&M job aid can be found at:
http://www.dss.mil/documents/rmf/Plan_of_Action_and_Milestones_POAM_Job_Aid.pdf

APPENDIX E: ISSM CERTIFICATION STATEMENT

To: Defense Security Service (DSS)
27130 Telegraph Road
Quantico, VA 22134

Subject: RMF IS Security Package Submission and Certification Statement

This letter serves as notification of the systems identified in the attached System Security Plan (SSP) as identified in the below National Industrial Security Program (NISP) Authorization Office (NAO) Unique Identifier (UID).

Facility Name:	CAGE Code:
Address:	
ISSM Name:	
ISSM Phone:	
NAO Unique Identifier:	

By submitting this security package, I am providing formal certification that the requirements and implementation procedures listed within the attached System Security Plan (SSP) are in accordance with National Industrial Security Process Manual (NISPOM), National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, and the DSS Assessment and Authorization Manual (DAAPM). I certify that all security controls and protection measures as described in the attached SSP and supporting artifacts have been implemented. I understand that failure to comply with the above conditions could result in the withdrawal of authorization. Any items that do not meet all NISPOM and DAAPM requirements will be addressed in a Plan of Action and Milestone (POA&M).

By signing below, I certify that the information provided in the attached SSP is true and correct. I understand that the United States Code (Title 18, section 1001) provides that making willful false official statements or concealing a material fact is a felony which may be punished by fine or imprisonment or both.

Thank You,

ISSM Signature	Date

APPENDIX F: WARNING BANNER

DSS Authorized Warning Banner
You are accessing a U.S. Government (USG) Information System (IS). Use of this USG IS constitutes: - Consent for authorized monitoring at all times; -- To ensure proper functioning of equipment and systems including security systems and devices, and; -- To prevent, detect, and deter violations of statutes and security regulations and other unauthorized use of the system. This system and related equipment are intended for the communication, transmission, processing, and storage of official USG or other authorized information only. Communications using, or data stored on this system are: - Not private; -- Subject to routine monitoring, interception, and search; and -- May be disclosed or used for any authorized purpose. If monitoring of this USG IS reveals possible evidence of violation of criminal statutes or security regulations (or other unauthorized usage), this evidence and any other related information, including User identification, may be provided to law enforcement officials or may result in appropriate administrative or disciplinary action.

DoD SIPRNet Warning Banner
You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions: - The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations. - At any time, the USG may inspect and seize data stored on this IS. - Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose. - This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy. - Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

APPENDIX G: MOBILITY SYSTEM PLAN

For the Movement of Classified Information Systems (IS):

Facility
Address
City, State Zip Code

Date of Mobility Plan
Revision Number

A. Introduction

This plan outlines the procedures for the transporting of classified IS equipment between [Facility] and various sites as listed in the Mobile Processing Plan attached to the SSP.

B. Description of Equipment

Equipment consists of computers, components, and test equipment to be used in support of field tests, flight test, customer reviews, and meetings. See SSP for list of equipment.

C. Identification of Participating Government and Cleared Contractor Representatives

- [Facility]
- Name of ISSM
- Address
- Contact information
- Local Defense Security Service Representative
- Name of SSP
- Address
- Contact information

D. Movement

Movement of the equipment will originate from [Facility]. Equipment will be transported to various sites listed in the Mobile Processing Procedures attached to the SSP. The Mobile Processing Procedures will include details regarding the site's physical environment. The ISSM will notify the DSS Representative prior to movement of the system to or from any off-site location. All equipment will be shipped either as classified at system approval level or downgraded to an unclassified state, security seals affixed. All remaining classified components will be properly shipped or hand carried.

E. Notification of Transportation

The ISSM will be notified of the upcoming movement as early as possible. The following information must be provided:

- Program name
- Classification
- Will the shipment contain hazardous material? If so, provide a Material Safety Data Sheet (MSDS) or an Intent to Hand Carry letter from the customer
- Size and weight of equipment
- Who owns the equipment, and is it Government Furnished Equipment (GFE)?

F. Hand Carry (Courier)

This must be authorized by the Security Manager. Each courier must be identified by name, title, as well as the name of the program being supported. Flight itinerary and vehicle rental information must be provided. Couriers must be cleared at the appropriate level and be thoroughly briefed on their security responsibilities. Each courier will be issued a "Courier Authorization" and will be provided emergency telephone numbers.

G. Responsibilities of Receiving Facility

- The recipient organization must notify the dispatching organization and [Facility] Security of any security relevant problems that occur.
- The recipient organization must notify the dispatching organization and [Facility] Security of any discrepancies in the documentation or equipment.

Mobility System Form (To be used when releasing IS to government activity or test site.)

CLEARED CONTRACTOR LETTERHEAD

[DATE]

FROM: [ISSM]

TO: [Name of government site ISSO and address]

SUBJECT: Relocation of DSS Authorized Information System [name or number of IS] from [company name] to [user agency site or test-site].

On [authorization date], the information system (IS) identified as [UID] located at [company name and address] was authorized to process classified information at the [level of classified information] level by the Defense Security Service (DSS) in accordance with the National Industrial Security Program Operating Manual (NISPOM). A copy of the authorization letter is attached for your review.

[Company name] has a requirement in conjunction with [contract number] with [name of IO] to relocate the above to [government site or test site] in order to process classified information for [purpose]. During the period when this will be resident at [name of government site, test site, or installation, etc.], your activity must assume cognizance for the security of the system. Any movement of an authorized IS outside of the DSS-approved area changes the original intent of DSS authorization.

Prior to the above system being relocated to your site, an authorized official of [name of site] must sign this letter and return it to the address provided. Your authorized official's signature will represent your organization's concurrence to accept the risk associated with moving an IS and security cognizance for the above-specified IS while it will be located at your site and under your jurisdiction. [Name of contractor] anticipates the IS (or closed area) will be removed from [name of site], and consequently your jurisdiction, by [provide approximate time of removal and location to which the system will be subsequently relocated].

If you have questions or would like to discuss this, please contact [company POC] at [telephone number] or by e-mail at [e-mail].

Sincerely,

[ISSM's Name]

[Title/Company]

Attachments: DSS Authorization Letter

Dated [Date]

Copy to: [Cognizant DSS ISR]

CONCURRENCE:

_____

(Name/Title of Authorized Official)

Authorized Alternate Site Locations

Alternate Site	Point of Contact
A. Location Operating Environment ☐ Restricted Area ☐ Closed Area	Contact Name: Phone: Phone: Fax: Cell: E-mail:
B. Location Operating Environment ☐ Restricted Area ☐ Closed Area	Contact Name: Phone: Phone: Fax: Cell: E-mail:

Authorized Sites for Mobile Processing

Mobile site Information	Point of Contact
A. [Facility] Type of Site: ☐ Contractor ☐ Government	Contact Name: Phone: Phone: Fax: Cell: E-mail: Shipping Method and Instructions:
B. [Facility] Type of Site: ☐ Contractor ☐ Government	Contact Name: Phone: Phone: Fax: Cell: E-mail: Shipping Method and Instructions:
C. [Facility] Type of Site: ☐ Contractor ☐ Government	Contact Name: Phone: Phone: Fax: Cell: E-mail: Shipping Method and Instructions:

System Component Information Form

[Facility Information]	System/Component Information	[System Identification]

To relocate a system approved for Mobile Processing, this form must be completed and submitted by the Information System Security Manager (ISSM) the local DSS Industrial Security Representative (IS Rep) prior to Shipment. The owning ISSM must coordinate the movement through the local IS Rep anytime the system is relocated. The ISSM must receive concurrence from the gaining ISSM/GCA in writing prior to shipment accepting responsibility for the system or components being relocated.

Program:	Contract Number:

Owning Facility Contact Information

ISSO	Telephone	Fax	E-mail
Alternate ISSO	Telephone	Fax	E-mail
ISSM	Telephone	Fax	E-mail

Relocation Site Information

Government Site	Contractor Site	Gaining Facility Name:

Address	City	State	Zip

Specific Processing Location (Bldg/Room)	Cage Code

Security Office Point of Contact (FSO/IO/ISSM)	Telephone	Fax	E-mail

DSS ISR Name	Telephone
Program Point of Contact	Telephone

Duration of Visit – Date from:	Date to:	Shipping Date (mm/dd/yy)

Authorization to process at the relocation site

The following documentation is provided authorizing classified processing at the relocation site.

	Yes	No	Comment
Contractual Relationship	☐	☐	
Technical Instruction	☐	☐	
Statement of Work	☐	☐	
Provisions within Special	☐	☐	
Other	☐	☐	

Relocation Site Activities		
Will the equipment be moving from the contractor facility to a government location?	☐ Yes	☐ No
If so, how will the equipment be handled? Will the equipment leave possession of the contractor?		
Does the equipment return to the contractor facility when not in use?	☐ Yes	☐ No
System Connection Requirements		
If the relocation site is another contractor facility, will the system be connected to the gaining facility's network?	☐ Yes	☐ No
If so, is the connection authorized and approved by DSS? Provide details of approved connection, to include MOU.		
Will the system be connected to the gaining facility's network (if government site)?	☐ Yes	☐ No

Privileged User Information /Relocation Site ISSO			
Users Identified Below have been Briefed/Trained and are Responsible for Conducting Weekly Audits and Antivirus Updates			
Relocation Site ISSO Name	**Privileged Account**	**Briefing/Training Date**	**Briefed by Name**
Relocation Site Alternate ISSO Name	**Privileged Account**	**Briefing/Training Date**	**Briefed by Name**

IS System or List of Components being Moved to the Relocation Site					
Quantity	Make/Model	Serial Number	Memory	Non-volatile?	Method of Sanitization

APPENDIX H: ASSURED FILE TRANSFER (AFT) PROCEDURES

Assured File Transfers (AFT)

There are two types of data transfers: Low-to-High and High-to-Low.

Low-to-High

Low-to-High is defined as a transfer from a lower classification system to a higher classification system, and also includes data transferred between two like security domains.

High-to-Low

High-to-Low is defined as a transfer from a higher classification system to a lower classification system. It also includes a transfer between systems of the same classification with a differing set of programs.

Conducting manual data transfers between security domains can be a time consuming, labor intensive process, and must be done methodically and accurately to assure integrity of the source information, to ensure that only the data identified for transfer is transferred, to prevent introduction of malicious software, and to prevent data spills. Careless methods, shortcuts, and untrained users have compromised sensitive and classified information vital to national security, mission success, and operational processes.

AFT procedures are established to mitigate the risks associated with all aspects of this activity and are conducted by individuals trained in the risks associated with transferring data between disparate security domains. The DTA is responsible for understanding the risks involved in data transfers and following AFT procedures to ensure any potential risk is managed during the download and transfer process. The subject matter expert (SME) is an individual knowledgeable of the program and the classification of information associated with it, and is responsible for ensuring the file is reviewed and sanitized of all program-related data.

Print Hardcopy

Printing eliminates the vulnerabilities associated with electronic media. Printing selected data and performing a comprehensive review by a SME is not considered an AFT. Once media is printed and a comprehensive review is conducted, the NISPOM Chapter 4 marking guidance must be followed.

Data Transfer Tracking

All data transfers (e.g., Low-to-High, High-to-Low) must be tracked to include date, originator making request, filename, file format type, classification level, source, destination systems, number of copies created, DTA performing transfer, SME performing review, and approver. Both types of data transfers can be maintained in one log, as long as the type of data transfer is clearly annotated.

Low-to-High transfer requires:

- Logging transfers from a lower classified system to a higher classified system (e.g., Secret to Top Secret, Unclassified to Secret, etc.).

- Performing two virus/malware scans. The first scan is performed once the files is downloaded to the media on the originating system. The second scan is performed on the media in the target system prior to uploading the file to the system. When possible, use virus/malware scanning products from different vendors.

- Testing of the write-protect mechanism. Once media is introduced on the High side, the capability to write to the media must be tested to ensure the media is write-protected. If the test fails, the media must be classified at the higher classification level.

High-to-Low transfer requires:

- Log for transfers from a higher classified system to a lower classified system (e.g., Secret to Unclassified, Top Secret to Secret, etc.) with a documented mission justification.

- As a community best practice, use of an automated review tool in lieu of a manual transfer process (e.g., checklist).

- AO approved AFT procedures and authorized file types/formats.

- AO approval for use of automated tools or a manual transfer process/checklist, to include any IO requirements, as part of the SSP.

AFT High-To-Low Procedures

For every file type or format, there are countless unique transfer procedures developed by industry and government. DSS has provided the AFT procedures and authorized file types below. Regardless of the file format or procedure used, there are requirements common to all general media and electronic transfers:

- The file types/formats and transfer procedures must be authorized by DSS and documented in the System Security Plan (SSP)

- Target media must be factory fresh

- All new and reused media must be scanned for viruses with the latest definitions prior to starting an AFT

- A comprehensive review must be performed to ascertain the sensitivity and classification level of the data

- Classified path/file embedded links and/or classified path/file names are not used for source or target files

- The compilation of all files on the target media does not cause an increased classification level due to “Aggregation”

- Files are transferred using a known, authorized utility or command
- Target media is verified to contain only intended source files
- Files are verified on target media to contain the correct sensitivity of information and/or level of unclassified or lower classified information
- The target media displays the appropriate security classification label
- An administrative record of the transfer is created and maintained

If the ISSM is unable to implement the DSS File/Type Formats and Authorized Procedures, the SSP must include a description of the file format and/or procedure used. These procedures must be approved by the AO.

DSS Authorized File Type/Formats

Format Type	Explanation	Common File Extensions
ASCII	ASCII-formatted information is essentially raw text like the text in this document. Many applications have the ability to export data in ASCII or text format. Program source code, batch files, macros and scripts are straight text and stored as ASCII files. ASCII files may be read with any standard text editor.	.txt .dat .c .for .fil .asc .bat **Note:** This is not an all-inclusive list. If a file cannot be read with a standard text editor, try changing the extension to .txt. If the file still cannot be read with a text editor, it is most likely not an ASCII file.
Hypertext Markup Language (HTML)	The document format used on the World Wide Web. Web pages are built with HTML tags (codes) embedded in the text. HTML defines the page layout, fonts, and graphic elements, as well as the hypertext links to other documents on the Web.	.html .htm
Joint Photographic Experts Group (JPEG)	JPEG (pronounced jay-peg): An ISO/ITU standard for compressing still images that is very popular due to its high compressibility.	.jpg
Bitmap (BMP)	A Windows and OS/2 bitmapped graphics file format. It is the Windows native bitmap format. Every Windows application has access to the BMP software routines in Windows that support it.	.bmp
Graphics Interchange Format (GIF)	A popular bitmapped graphics file format developed by CompuServe.	.gif

Note: Executable programs may not be transferred. The source code (ASCII text) may be reviewed/transferred to a lower level Information System then re-compiled into executable code.

DSS AFT Procedure (Windows-Based)

1. The target media must be factory fresh.

2. The procedure must be performed by a Data Transfer Agent (DTA).

3. If multiple files are being transferred, create a designated directory for the transfer using the DOS Make Directory command (md [drive:] path) or the new folder command under Windows Explorer. (Rationale: This will establish an empty directory which helps ensure that only intended files are transferred).

4. If multiple files are being transferred, transfer all files into the newly-created directory.

5. As a general rule, files should be converted to one of the acceptable formats first (DSS Authorized File Type/Formats), then reviewed. Drawings and presentation type files (e.g. PowerPoint, Publisher, and Visio) are an exception. These types of files within their native application may have layers of information (e.g., text on top of graphics, or multiple graphics layers). Once exported into one of the authorized graphic formats (e.g. .bmp, .jpg, .gif), the layers will be merged together and will not be editable to remove any higher classified information. To review these files, use the native application used to generate the file. Ensure that every page, chart, slide, drawing etc., of the file is examined. Within each page, chart, slide, drawing, etc., ensure that all layers are reviewed by ungrouping and moving objects around so everything is visible. Some applications may also have information in headers and footers, notes pages, etc. Below is a detailed procedure for reviewing one of the more commonly used presentation/graphic applications (Review of MS Word and MS Excel files can follow the same instructions), but some items will not apply. **Note:** depending on application versions, the menu selections may differ.

   PowerPoint

   - Review headers and footers. Click on Header and Footer under the View menu. Click on and review both the Slide and the Notes and Handouts tab.

   - Review the master design for the file. Click on Master under the View menu. Select and review each of the Masters (Slide, Title, Handout, & Notes).

   - For each slide, click on Edit and Select All. Once all objects are selected, click on Draw (bottom left of screen), and then Ungroup until the Ungroup option is no longer available (grayed out). Press the tab key to outline each object (delineated by a box around a graphic or text) in the slide. If an object is outlined but not visible, move it, bring it forward, or change its color until it is visible, or delete it. Repeat this process for each object in the slide. Use this process to find and delete all higher classified information.

- After the review and edit is complete, save the information in one of the authorized formats. Click on File Save As under the File menu. Select one of the DSS-authorized formats from the drop-down menu of Save As Type.

6. If any files are not in one of the following five formats, ASCII/Text, HTM/HTML, JPEG, BMP, GIF, convert it to one of these formats.

   - Spreadsheet and database files must be exported as an ASCII text files.

   - The graphics files within HTM/HTML files must be saved separately as JPG files. HTML files by themselves are text information and may be treated as a standard ASCII file format.

   - Executable programs may not be transferred. The source code (ASCII text) may be reviewed/transferred to a lower level IS then re-compiled into executable code.

7. Review the files using a compatible application. Review all the files and not just random samples.

   - BMP and JPG files may be reviewed with a graphics file viewer such as MS Photo Editor. **Note:** Since GIF files may contain a 3D/animation/multi-page image, you must use a program that will show all the information stored in GIF files. Internet Explorer or Netscape can be used. MS Photo Editor will not display all the frames (images) and therefore is not adequate to view GIF files.

   - For ASCII text, the preferred application for reviewing is NotePad. However, these applications have file size limitations. If the file cannot be opened with NotePad, use MS Word (see below).

   - After completion of the review, remove all encoded formatting created by previous editing with MS Word. On the File menu, click Save As (Selected Approved Format) then click Save.

   - Review remaining ASCII files not viewable with NotePad with MS Word:

     1) Ensure all hidden text and codes are viewable. Click Options on the Tools menu, click the View tab, then select every option under the Show section and All under the Formatting Marks section.

     2) Verify all Tracked changes (Revisions in MS Word) are viewable. Click on Track Changes then Highlight Changes under the Tools menu. If Enabled, Disable the Track changes while editing. Enable the Highlight changes on screen.

     3) Review the Summary and Contents sections of the file properties. Click Properties on the File menu, and then click on the Summary and Contents tabs.

     4) Review headers and footers. Click on Header and Footer under the View menu. Headers will be displayed at the top of each page; any footers will be displayed at

the bottom of each page. **Note**: If a document has multiple Sections, each Section may have different headers and footers.

5) Review comments. Click on Comments under the View menu. A comments pane will be displayed at the bottom of the screen. If Comments is grayed out under the View menu, this means there are no comments within the document.

6) Review footnotes: Click on Footnotes under the View menu. If footnotes are grayed out under the View menu, this means there are no footnotes within the document. If footnotes are not grayed out, there are footnotes. If you are displaying the document in Normal layout or Web Layout, a footnote pane will appear at the bottom of the screen. If you are displaying the document in Print Layout, footnotes will already be visible at the bottom of each page, or at the end of the document.

7) Review the entire contents of the file including all Sections. All embedded objects except clipart and WordArt must be deleted. When reviewing Clipart and WordArt and text boxes, ensure there is no information hidden behind these objects. **Note**: Embedded objects may be opened and saved separately prior to deletion. Each separately saved object is subject to this procedure prior to transfer.

8) When you are finished reviewing the file, ensure all hidden deleted information from Fast Save operations is removed. On the File menu, click Save As (Selected Approved Format), then click Save. Also, if the file is not yet in one of the acceptable file format types, select one of the DSS-approved formats from the drop-down menu of Save As Type.

- For all file formats, verify the source and target files names are not classified.

8. Use the standard save or transfer command or utility (e.g. drag and drop, copy, etc.) to transfer the files to the target media.

9. Write-protect the media (physical or software) as soon as the transfers are complete.

10. Verify (dir/s [drive]: or Windows Explorer) that only intended files were transferred.

11. Compare the files that were transferred to the originals [fc (pathname/filename) drive: (path/filename)].

12. Apply the appropriate security classification label to the target media.

13. Create an administrative record of the transfer and maintain with your audit records. The record must specify the data being released, the personnel involved, and the date.

DSS AFT Procedure (Unix-Based)

Note: These procedures should be tailored for the local environment. In particular, the Unix commands listed herein are for illustration only and must be modified to account for the Unix version, hardware configuration, and software installation specifics.

1. The target media must be factory fresh.

2. The procedure must be performed by a DTA.

3. If multiple files are being transferred, create a designated source directory for the transfer using the Unix make directory command (mkdir directory_name) (Rationale: This will establish an empty directory which helps ensure that only intended files are transferred).

4. If multiple files are being transferred, transfer all files into the newly created directory.

5. Verify the source and target files names are not classified.

6. View the contents of **all files** in the designated directory, not random samples.

    - For text files use software that displays the entire contents of the file. (e.g., Hex editor) Any unintelligible data is assumed to be classified at the authorized IS level.

    - For graphics or movie files, review the files using an appropriate file viewer. Ensure that the file format does not include internal annotations or other additional data (if present, this information can only be viewed with a specialized viewer, and poses a significant threat of inadvertent disclosure).

    - For non-text files, the sensitivity or classification of non-text and non-graphics files cannot generally be determined without intensive technical analysis. Such files must be assumed to be classified. Files in this category include binary database files, compressed archives, and executable code.

        1) In the case of executable files, review and downgrade the source code and then transfer the source code to a lower-classified machine for re-compilation.

        2) In some cases, the source code will be classified, but the compiled code will be unclassified as specified in the classification guidance document. After compilation, the executable should be reviewed with HEX editor software to ensure that no classified information has escaped the compilation process.

        3) In the case of binary database files, export the data to ASCII text format, then review and downgrade the text file for media migration.

        4) Compressed archives should be reviewed and transferred uncompressed.

7. Use the Tar utility to create and write an archive of the source directory to the target media. The Unix command sequence will be as shown below (the exact command may vary depending on the Unix version, machine configuration, and the media used):

8. mt -f /dev/rst0 rew.

9. Ensure tape is rewound (not required if using floppy).

10. tar cvf /dev/rst0 /directory_name.

11. Create Tar file on tape.

12. Write-protect the media as soon as the transfers are complete.

13. Verify that the media contains the expected data by printing a directory of the Tar file:

    - mt -f /dev/rst0 rew.

        1) Ensure tape is rewound (not required for floppy) tar tvf /dev/rst0 | lpr.

        2) Print directory of file (| lpr may be omitted for on-screen review).

14. The output of the above command should match the contents of the source directory. To verify that they match, compare the output of the above command with the directory printed by the following command:

    - ls -alR /source-directory | lpr (| lpr may be omitted for on-screen review).

15. Ensure the date, time, and file sizes are as expected. If any unintended data was copied, the target media must be considered classified and cannot be used for a trusted down load again.

16. Apply the appropriate security classification label to the target media.

17. Create an administrative record of the transfer and maintain with your audit records. The record must specify the data being released, the personnel involved, and the date.

Data Transfer Agent (DTA) Authorization Form

Printed Name:	Applicable UID(s)/Contract(s):

Manager Request	
I request the above named individual be authorized to perform Assured File Transfers (AFT). I understand this process involves both knowledge of classification issues and attention to detail in reviewing information and following the process for performing a transfer of data. I also understand that transferring information from a classified environment to an unclassified environment increases the risk of compromising classified information and will instruct authorized employees under my supervision to perform these actions only when absolutely necessary.	
Printed Name:	
Signature:	Date:

Acceptance of Responsibility	
I have attended training and understand both the risks associated with performing an AFT and the mechanisms associated with the AFT process. I understand that all media generated from a classified system must be labeled and handled at the highest level of data on the system unless an AFT High-To-Low Procedure is performed. I understand it is my responsibility to perform this process as outlined in the AFT Procedure.	
Signature:	Date:

ISSM or ISSO Authorization	
I certify that the individual identified above has been briefed in the vulnerabilities associated with transferring unclassified or lower classified information from an authorized Information System. Additionally, he/she has demonstrated extensive knowledge of all appropriate security classification guides and authorized procedures associated with the information downloaded.	
Authorized File Formats: ASCII/Text, HTM/HTML, JPEG, BMP, GIF Specify:	
Printed Name:	
Signature:	Date:

APPENDIX I: CLASSIFIED SPILL CLEANUP PROCEDURES

Classified Spills (also known as contaminations) occur when classified data is introduced to an unclassified computer system or a system authorized at a lower classification. Any classified spill will involve an Administrative Inquiry (AI) for the facility concerned (Related Controls: IR-9 and IR-9(1)).

Wiping Utility

Hard drives involved in a classified spill should be wiped using a National Security Agency (NSA) or National Information Assurance Program (NIAP) approved product. If one is unavailable, any commercially available wiping utility that meets the following requirements may be used:

a. If wiping whole disks, it must be able to wipe the entire drive (e.g., partition tables, user data, operating systems and boot records).

b. If wiping whole disks, it must be able to wipe Device Configuration Overlay (DCO) hidden sectors if Advanced Technology Attachment (ATA-6) disks are being used.

c. If wiping whole disks, it must be able to wipe a Host Protected Area (HPA).

d. Must be able to sanitize by overwriting with a pattern, and then its complement, and finally with another unclassified pattern (e.g., “00110101” followed by “11001010” and then followed by “10010111” [considered three cycles]). Sanitization is not complete until three cycles are successfully completed.

e. Must be able to verify the overwrite procedure by randomly re-reading (recommend 10% if possible) from the drive to confirm that only the overwrite character can be recovered. If not, the use of an additional utility to accomplish this is acceptable.

f. Must be able to print the results of the overwriting operation showing any bad sectors or areas of the disk that could not be written to (if there are any bad sectors or blocks the disk must be destroyed or degaussed).

Cost Analysis

It is suggested that the company perform a cost analysis before using the option of wiping hard drives. Wiping can take many hours to perform and it may be more cost effective to dispose of hard drives by degaussing or destruction. NIST Special Publication 800-88, Guidelines for Media Sanitization can provide some assistance in this regard.

Additional Precautions

The hard drive may not be the only storage media in a system. Beware of floppy disks left in floppy disk drives, Zip disks in Zip drives, CDs and Digital Versatile Disks (DVDs) in optical drives, tapes in tape backup-units, thumb drives/compact flash drives, BIOS passwords, printing devices and the like. Include relevant documentation when an old system is wiped and then transferred from one department or division within the same company to another. Desktops and

laptops aren't the only systems that need sanitizing. Pocket PCs, PDAs, some multifunction cell phones, and other devices may also contain sensitive information such as passwords or confidential data.

Coordination

Employees or security managers who report the discovery of classified information on unclassified or lower classified information systems are not to delete the classified data, but to isolate the systems and contact the cognizant FSO, ISSM or ISSO immediately. Caution should be taken when discussing such incidents over unsecured telephones so as not to further endanger any classified information that may be at risk on unclassified systems.

The initial report should include the following (if known):

a. Origination of data/message: Facility, location, point of contact

b. Other facilities involved: Facility, location, point of contact

c. Method of transmission

d. All equipment involved: Servers (Redundant Array of Independent Disks (RAID) or single), workstations, notebooks, e-mail servers, Blackberries, etc

e. Specify: Remote dial-in or network connection

f. Location of all equipment

g. All Operating Systems involved

h. Number of people involved (Identify the employee(s) and include clearance level)

i. Status of backup tapes (if applicable)

j. Availability of audit logs to determine access

k. Current status of all equipment involved

l. Data owner notification

m. Customer information:

- Name
- Point of Contact
- Phone numbers
- Email address

n. IRP

Appropriately Cleared Team

It is essential that all persons who participate in the cleanup have the appropriate clearance/access to account for unexpected exposure to classified information. Uncleared personnel involved in a data spill will be required to sign a standard non-disclosure agreement.

Protection of Classified Data and Hardware

The cognizant ISSM will interview all appropriate persons to determine the extent of the contamination and to recover any hardcopy or media copies of the classified information. Any contaminated systems such as printers or other peripherals with memory that cannot be readily sanitized will be moved into a controlled area until they can be cleaned. Backup tapes that are determined to contain potential classified material must be identified and secured appropriately until they can be sanitized.

Transitory Devices

Data that is transmitted through transitory network devices such as mail hubs, routers, etc., is constantly overwritten through normal network operations. Therefore, sanitization procedures are applicable only to the sending and/or receiving network servers and client workstations.

References

The following references will assist with the development of an IRP:

- NIST Special Publication (SP) 800-88, *Guidelines for Media Sanitization*
- NIST Special Publication 800-61, Computer Security Incident Handling
- Committee on National Security System Instruction (CNSSI) no. 1001, *National Instruction on Classified Information Spillage*
- CNSSP No. 18 National Policy on Classified Information Spillage
- CNSSP No. 26 National Policy on Reducing the Risk of Removable Media for National Security Systems

Role	Responsibilities
All Personnel	• Immediately communicate to each other any reports of e-mail security incidents or classified contaminations • Participate in and support security incident meetings and response efforts • Assess the risks of the contamination and follow any special guidelines of the data owner (customer) • Assign appropriately cleared individuals to participate in the cleanup effort

Role	Responsibilities
FSO	• The originating facility FSO of the contamination will act as the incident lead • Notify applicable Government agencies of the security incident • Determine the security classification level of the data and confirm the appropriate cleanup procedures • Identify the sender/receiver(s) of the classified information • Request cleanup assistance by appropriately cleared technicians • Contact the appropriate security official at any distant locations where the contamination was received or from where it originated • Notify company officials of the incident and the planned cleanup effort
ISSM/ ISSO	• Assess the extent of contamination and plan cleanup actions • Conduct cleanup of contaminated systems and any peripherals using cleared personnel. Spills at all classification levels will be cleaned up following IRP procedures authorized in the SSP. IO approval either prior to (preferable) or after the spill occurs (the IO may require destruction) is required. If the IO does not answer within 30 days it will be taken as a concurrence with the procedures and declassification. • Report vulnerabilities, cleanup actions, and any other pertinent information to DSS Representative • Protect and isolate any contaminated systems from further compromise • Coordinate storage/transport of classified material or other evidence • Determine if there was "bcc:" addressing or if the sender copied his/her own account • Determine if the contamination was distributed via other paths such as print, ftp, electronic media, server storage, etc. • Determine if recipient accounts have user-configured rules for auto-forward, auto-save or other special instructions • Investigate possibility of proxy accounts, Blackberry access, remote access and any other possible "feeds" from the contaminated accounts • Isolate any contaminated assets of the sender/receiver

APPENDIX J: MEDIA SANITIZATION

Media Sanitization

The guidance below does not capture all forms of media. Please reference additional NSA resources on NSA's Media Destruction Guidance website: https://www.nsa.gov/ia/mitigation_guidance/media_destruction-guidance/index.

Before storage media is released out of organizational control, becomes obsolete, or is no longer usable or required for an information system, it is a requirement to ensure that residual magnetic, optical, electrical, or other representations of data which have been deleted are not recoverable.

Sanitization is the process of removing information from storage devices or equipment such that data recovery using any known technique or analysis is prevented. Sanitization includes the removal of data from the storage device, as well as the removal of all labels, markings, and activity logs.

Destruction is the process of physically damaging media so that it is not usable and there is no known method of retrieving the data. This may include degaussing, incineration, shredding, grinding, embossing, chemical immersion, etc.

All sanitization and destruction procedures require AO approval. Organizations may also institute additional media sanitization policies and procedures as needed.

Responsibilities

Organizations are responsible for ensuring adequate resources and equipment are available to support media sanitization activities.

The ISSM is responsible for the security of all media assigned to the organization and under his/her purview. To protect these assets, he/she must ensure the security measures and policies contained within this section are followed. Additionally, the ISSM, with AO approval, may publish SOPs for sanitizing, and releasing system memory or media.

Ensure appropriate safeguards are in place so removable media that contains classified, sensitive, or controlled unclassified information are properly sanitized, destroyed, and/or disposed of in accordance with an approved method when no longer needed.

Sanitization of Media

Prior to media disposal, release out of organizational control, or release for reuse, organizations will sanitize all media using sanitization mechanisms with strength and integrity commensurate with the classification or sensitivity of the information.

All media, regardless of classification, will be sanitized in accordance with the procedures outlined in the SSP prior to release, or disposal.

Degaussing Magnetic Media

Degaussers are ineffective in erasing optical and solid state storage devices.

Degaussing (e.g., demagnetizing) is a method of sanitization. Degaussing is a procedure that reduces the magnetic flux on media virtually to zero by applying a reverse magnetizing field. Properly applied, degaussing renders any previously stored data on magnetic media unreadable and may be used in the sanitization process. Degaussing is not an approved method for sanitizing optical media.

It is highly recommended that after degaussing, but prior to disposal, all media is physically damaged to prevent data recovery attempts.

Refer to the NSA's website for media destruction guidance including the current Evaluated Products List – Degausser. This Evaluated Product List (EPL) specifies the model identification of current equipment units that were evaluated against and found to satisfy the requirements for erasure of magnetic storage devices that retain sensitive or classified data.

Sanitizing Optical Media (Destruction)

Optical storage devices include CDs and DVDs. Optical storage devices cannot be sanitized, only destroyed. Refer to Policy Manual NSA Central Security Service (CSS) 9-12 for detailed procedures related to the sanitization of optical media. Equipment approved for use in the destruction of optical media can be found in the NSA/CSS Evaluated Products List for Optical Media Destruction Devices.

Sanitizing Solid State Storage Devices (Destruction)

Solid state storage devices include Random Access Memory (RAM), Read Only Memory (ROM), Field Programmable Gate Array (FPGA), smart cards, and flash memory. Refer to Policy Manual NSA/CSS 9-12 for detailed procedures related to the destruction (e.g., smelting) of solid state storage devices.

Release of Systems and Components

The ISSM/ISSO, in conjunction with the organization's equipment custodian will develop equipment removal procedures for systems and components as approved by in the SSP. When such equipment is no longer needed, it can be released if:

- It is inspected by the ISSM/ISSO. This inspection will assure that all media, including all internal disks and nonvolatile memory components and boards, have been removed or sanitized.

- A record is created of the equipment release indicating the procedure used for sanitization and date of release to the equipment custodian. The record of release will be retained by the ISSM/ISSO for a period of two years.

Release of Memory Components and Boards

A memory component is considered to be the Lowest Replaceable Unit (LRU) in a hardware device. Memory components reside on boards, modules, and subassemblies. A board can be a module, or may consist of several modules and subassemblies. Memory components are specifically handled as either volatile or nonvolatile, as described below.

Volatile Memory Components

Memory components that do not retain data after removal of all electrical power sources, and when reinserted into a similarly configured system, are considered volatile memory components. Volatile components that have contained extremely sensitive or classified information may be released only in accordance with NSA/CSS Policy Manual 9-12.

Nonvolatile Memory Components

Components that do retain data when all power sources are discontinued are nonvolatile memory components. Some nonvolatile memory components (e.g., ROM, Programmable ROM (PROM), or Erasable PROM (EPROM)) and their variants that have been programmed at the vendor's commercial manufacturing facility and are considered to be unalterable in the field may be released. When in doubt, assume the component can be altered. All other nonvolatile components (e.g., removable/non-removable hard disks) may be released after successful completion of the sanitization procedures as defined in the SSP.

Other Nonvolatile Media

Visual Displays

There are many types of video display technologies in use. These technologies are susceptible, to differing degrees, to a phenomenon called "burn-in." Burn-in occurs when the normally volatile components of the display mechanism becomes worn or damaged and retain evidence of the data they were displaying. A visual display may be considered sanitized if no sensitive or classified information remains in the visual display. If this information is visible on any part of the visual display face, the display will be sanitized before it is released from control.

The display technology in common use is liquid crystal display (LCD). When powered for a long period in the rotated position, a liquid crystal may retain some of its twist and will not relax to its normal orientation. This is referred to as burn-in even though it is physically twist-in. This burn-in is not typically a problem for LCD displays that do not display an image for days on end. If LCD burn-in is suspected, the ISSM will uniformly illuminate each pixel of the display then visually search for contrasting areas that reveal information. Vary the intensity across the range of off to saturation for each color (red, green, and blue).

LCDs with compromising burn-in areas identified during assessment can normally be sanitized by leaving the device off for a few days in a warm (<140 degrees Fahrenheit) environment until the liquid crystals relax. If this is insufficient then the display should be alternated between long periods of full white and full black until the liquid crystals relax. If all this is insufficient or the display is strongly suspect, then the liquid crystal medium in the offending area of the display

between the front and rear LCD plates must be disturbed or removed. The liquid crystal medium is non-toxic but messy.

Actual burn-in can occur in legacy cathode ray tube, plasma, and laser phosphor displays. Where bright images are displayed for long period of time in the same location, the screen phosphors overheats and the image is permanently burned-in. The ISSM will inspect the face of the visual display without power applied. If sensitive information is visible (typically as a dark spot), the visual display will be sanitized before releasing it from control. If nothing is visible, the ISSM will apply power to the visual display, then vary the intensity from low to high.

In accordance with NSA/CSS Policy Manual 9-12, cathode ray tubes (CRT) and plasma monitors exhibiting burn-in will be sanitized by destroying the display surface of the monitor into pieces no larger than five centimeters square. Be aware of the hazards associated with physical destruction of monitors.

Light Emitting Diode (LED) displays (not LCDs with LED illumination) use an LED per pixel color and may have burn-in when LEDs overheat and fail. LED displays are typically used in signage and not on desktop displays. Destruction will be sufficient to preclude the derivation of sensitive or classified information from the arrangement of the inoperative LEDs.

Printer Platens and Ribbons

Printer platens and ribbons will be removed from all printers before the equipment is released. One-time ribbons and inked ribbons will be destroyed as sensitive material. The rubber surface of platens will be sanitized by wiping the surface with alcohol.

Laser Printer Drums, Belts, and Cartridges

Laser printer components containing light-sensitive elements (e.g., drums, belts, and complete cartridges) will be sanitized before release from control. Used toner cartridges from properly operating equipment that has completed a full printing cycle (without interruption) may be treated, handled, stored, and disposed of as unclassified and may be recycled. When a laser printer does not complete a printing cycle (e.g., a paper jam or power failure occurs), the toner cartridge may NOT be treated as unclassified. If the toner cartridge is removed without completing a print cycle, the cartridge drum must be inspected by lifting the protective flap and viewing the exposed portion of the drum. If residual toner is present, manually rotating the drum is sufficient to wipe off residual toner material present. Alternatively, a subsequent print cycle may be completed and is sufficient to wipe residual toner from the cartridge drum. After completing sanitization actions, the toner cartridge may be treated, handled, stored, and disposed of as unclassified (to include recycling).

Multifunction Devices (MFDs)

MFDs, including digital copiers and copier or printer centers, have the capability to copy, print, scan, and fax, either in a standalone mode or networked. These devices are computer-based, network-capable devices with processors, memory, hard drives, image retention components, and in some cases, cellular phone transmitters with vendor auto-alert features. When using multifunctional printer/copier equipment, the document image may remain on the imaging

drum/belt, hard drives, and static RAM. All memory resident components of MFDs must be properly sanitized before release.

Destroying Media

Destruction procedures must be detailed in the SSP. Media and memory components that are damaged, malfunction, or become unusable must be destroyed using methods appropriate for the media type.

Media Sanitization Matrix

MEDIA	CLEAR						SANITIZE															
Magnetic Tape																						
Type I	a						b									l						
Type II	a						b									l						
Type III	a						b									l						
Magnetic Disk																						
Bernoulli	a	c					b									l						
Floppy	a	c					b									l						
Non-Removable Rigid Disk		c				a			d							l						
Removable Rigid Disk	a	c				a			d							l						
Optical Disk																						
Read Many, Write Many		c														l						
Read Only																l	m					
Write Once, Read Many (WORM)																l	m					
Memory																						
Dynamic Random Access Memory (DRAM)		c	g					c					g				l						
Electronically Alterable Programmable Read Only Memory (EAPROM)				h											i		l					
Electronically Erasable PROM (EEAPROM)				h							f						l					
Erasable Programmable ROM (EPROM)					j			c								k	l					k then c
Flash EPROM (FEPROM)			h					c						h			l					h then c
Programmable ROM (PROM)		c															l					
Magnetic Bubble Memory		c				a		c									l					
Magnetic Core Memory		c				a			d								l					
Magnetic Plated Wire		c						c			e						l					c and e
Magnetic Resistive Memory		c															l					
Non-volatile RAM (NOVRAM)		c						c									l					
Read Only Memory (ROM)																	l					
Synchronous DRAM (SDRAM)		c	g					c					g				l					
Static Random Access Memory (SRAM)		c	g					c					g				l					

MEDIA	CLEAR						SANITIZE																
Other Media																							
Video Tape																	l						
Film																	l						
Equipment																							
Monitor			g																		p		
Impact Printer			g																	o			o then g
Laser Printer			g																n				n then g

Instructions for reading the matrix:

A letter in black in the above table indicates the procedure is a complete, single option. For example, to sanitize EEPROM: Perform either procedure f or l (refer to indices below) and the media/memory is completely sanitized. Highlighted letters indicate the procedures must be combined for a complete sanitization. For example, to sanitize a Laser Printer: "n" must be performed, followed by "g".

Note: When a combination of two procedures is required, the far right hand column indicates the order of the procedures (e.g., "o then g").

Matrix Index:

a. Degauss with Type I, II, or III degausser.

b. Degauss with same Type (I, II, or III) degausser.

c. Overwrite all addressable locations with a single character utilizing an approved overwrite utility.

d. For spills only, overwrite with a pattern, and then its complement, and finally with another unclassified pattern (e.g., "00110101" followed by "11001010" and then followed by "10010111" [considered three cycles]). Sanitization is not complete until three cycles are successfully completed. Once complete, verify a sample. If any part could not be written to the disk, the disk must be destroyed or degaussed. This option does not apply to disks used on a system accredited for classified processing.

e. Each overwrite must reside in memory for a period longer than the classified data resided.

f. Overwrite all locations with a random pattern, then with binary zeros, and finally with binary ones utilizing an approved overwrite utility.

g. Remove all power (to include battery power).

h. Perform a full chip erase per manufacturer's data sheets.

i. Perform h above, then c above, a total of three times.

j. Perform an ultraviolet erase according to manufacturer's recommendation.

k. Perform j above, but increase time by a factor of three.

l. Destruction.

m. Destruction is required only if the classified information is contained.

n. Run 1 page (font test acceptable) when print cycle not completed (e.g., paper jam or power failure). Dispose of output as unclassified if visual examination does not reveal any classified information.

o. Ribbons must be destroyed. Platens must be cleaned.

p. Inspect and/or test screen surface for evidence of burn-in information. If present, screen must be destroyed.

APPENDIX K: ACRONYMS

A&A	Assessment and Authorization
AC	Access Control
ACAS	Assured Compliance Assessment Solution
AFT	Assured File Transfer
AI	Administrative Inquiry
AO	Authorizing Official
ATA	Advanced Technology Attachment
ATC	Authorization to Connect
ATD	Authorization Termination Date
ATO	Authorization to Operate
AU	Audit and Accountability
BoE	Body of Evidence
CAGE	Commercial and Government Entity
CCP	Common Control Provider
CD	Compact Disk
CDS	Cross Domain Solution
CI	Counterintelligence or Controlled Interface
CIA	Confidentiality, Integrity, and Availability
CM	Configuration Management
CNSS	Committee on National Security Systems
CNSSD	Committee on National Security Systems Directive
CNSSI	Committee on National Security Systems Instruction
CNSSP	Committee on National Security Systems Policy
COMSEC	Communications Security
CONOPS	Concept of Operations
COOP	Continuity of Operations
COTS	Commercial-off-the-Shelf
CP	Contingency Planning
C/S	Client/Server
CSA	Cognizant Security Agency
CSS	Central Security Service
CTTA	Certified TEMPEST Technical Authority
DAR	Data At Rest
DATO	Denied Authorization to Operate
DCO	Device Configuration Overlay
DMZ	Demilitarized Zone
DNS	Domain Name System

DRP	Disaster Recovery Plan
DSA	Designated Security Authority
DTA	Data Transfer Agent
DVD	Digital Versatile Disk
EAP	Extensible Authentication Protocol
EEPROM	Electrically Erasable Programmable Read-only Memory
EPL	Evaluated Products List
EPROM	Erasable Programmable Read-only Memory
FPGA	Field Programmable Gate Array
FRD	Formerly Restricted Data
FSO	Facility Security Officer
FTP	File Transfer Protocol
GCA	Government Contracting Authority
GFE	Government Furnished Equipment
GIG	Global Information Grid
GOTS	Government off-the-shelf
GMT	Greenwich Mean Time
HTTP	Hyper Text Transfer Protocol
I&A	Identification and Authentication
I/O	Input/Output (e.g. I/O Port)
IA	Identification and Authentication or Information Assurance
IDS	Intrusion Detection System
IO	Information Owner
IP	Internet Protocol
IR	Incident Response or Infrared
IS	Information System
ISA	Interconnection Security Agreement
ISCP	Information System Contingency Plan
ISO	Information System Owner
ISOL	Isolated LAN
ISSM	Information System Security Manager
ISSO	Information System Security Officer
ISSP	Information System Security Professional
IT	Information Technology
ITPSO	Insider Threat Program Senior Official
JTF	Joint Task Force
KVM	Keyboard/Video/Mouse
LAN	Local Area Network

LCD	Liquid Crystal Display
LED	Light Emitting Diode
LOP	Local Operating Procedures
LRU	Lowest Replaceable Unit
MA	Maintenance
MAC	Media Access Control
MFD	Multifunction Device
MP	Media Protection
MSSP	Master System Security Plan
NAO	NISP Authorization Office
NAPA	NISP Administration and Policy Analysis
NIC	Network Interface Card
NISP	National Industrial Security Program
NISPOM	National Industrial Security Program Operating Manual
NIST	National Institute of Standards and Technology
NSA	National Security Agency
P2P	Peer to Peer
PAN	Personal Area Network
PCL	Product Compliant List
PDA	Personal Digital Assistant
PDS	Protected Distribution System
PE	Physical and Environmental Protection
PED	Portable Electronic Device
PL	Planning or Protection Level
PM	Program Management or Program Manager
POA&M	Plan of Action and Milestones
POC	Point of Contact
PROM	Programmable Read-Only Memory
PS	Personnel Security
PSI	Personnel Security Investigation or Program Security Instruction
PSO	Program Security Officer
RA	Risk Assessment
RAID	Redundant Array of Independent Disks
RAL	Risk Acknowledgement Letter
RAM	Random Access Memory
RAR	Risk Assessment Report
RD	Restricted Data
RF	Radio Frequency

RFID	Radio Frequency Identification
RMAT	Remote Maintenance and Testing
RMF	Risk Management Framework
RO	Releasing Officer
ROM	Read Only Memory
SA	System and Services Acquisition
SAP	Special Access Program
SAPF	Special Access Program Facility
SCA	Security Control Assessor
SCAP	Security Content Automation Protocol (pronounced S-CAP)
SCC	SCAP Compliance Checker
SCG	Security Classification Guide
SCP	Secure Communications Plan
SI	System and Information Integrity
SOP	Standard Operating Procedures
SP	Special Publications
SSL	Secure Socket Layer
SSP	System Security Plan
STE	Secure Terminal Equipment
STIG	Security Technical Implementation Guide
SUSA	Single User-Standalone
SVA	Security Vulnerability Assessment
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TSCO	Top Secret Control Officer
UAC	User Account Control
UHF/VHF	Ultra-High Frequency/Very High Frequency
USERID	Individual user identifier
USG	U.S. Government
VPL	Validated Products List
VPN	Virtual Private Network
VTC	Video Teleconference
VVoIP	Voice and Video Over IP
WAN	Wide Area Network
WDE	Whole Disk Encryption

APPENDIX L: DEFINITIONS

Authorization	Formal declaration by the AO that an IT system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.
Authorization to Connect	Formal approval granted by a WAN AO allowing the connection of a node to a WAN.
Authorization to Operate	Approval granted by an AO for an IS to process classified information.
Audit Log	A chronological record of system activities. Includes records of system accesses and operations performed in a given period.
Audit Trail	A chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security relevant transaction from inception to final result.
Certification	Comprehensive evaluation of the technical and non-technical security features of an IT system and other safeguards, made in support of the accreditation process, to establish the extent that a particular design and implementation meets a set of specified security requirements by the ISSM.
Classified Information	Official information that has been determined, pursuant to E.O. 12958 or any predecessor order, to require protection against unauthorized disclosure in the interest of national security and which has been so designated. The term includes National Security Information (NSI), Restricted Data (RD), and Formerly Restricted Data (FRD).
Classified Information Spillage	Security incident that occurs whenever classified data is spilled either onto an unclassified information system or to an information system with a lower level of classification.
Compensating Security Control	A management, operational, and/or technical control (e.g., safeguard or countermeasure) employed by an organization in lieu of a recommended security control in the low, moderate, or high baselines described in NIST Special Publication 800-53 or in CNSS Instruction 1253, that provides equivalent or comparable protection for an information system.
Command Cyber Readiness Inspection	A review of an IS connected to the SIPRNet to evaluate enclave and network security, perform network-based vulnerability scans, and assess compliance with applicable policies.
Company	A generic and comprehensive term which may include sole proprietorships, individuals, partnerships, corporations, societies, associations, and organizations usually established and operating to commonly prosecute a commercial, industrial, or other legitimate business, enterprise, or undertaking.

Computer Network Attack (CNA)	Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.
Computer Network Defense (CND)	Defensive measures to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction.
Configuration Control Board (CCB)	Establishment of and charter for a group of qualified people with responsibility for the process of controlling and approving changes throughout the development and operational life cycle of products and systems; may also be referred to as a change control board.
Controlled Interface (CI)	A boundary with a set of mechanisms that enforces the security policies and controls the flow of information between interconnected information systems (CNSSI 4009).
CONFIDENTIAL	This designation will be applied to information or material the unauthorized disclosure of which could be reasonably expected to damage national security.
Cleared contractor	Any industrial, educational, commercial, or other entity that has been granted an FCL by a CSA.
Denial	When a Systems Security plan has been accepted and reviewed by an ISSP and is not granted an approval to operate.
Document	Any recorded information, regardless of its physical form or characteristics, including but not limited to: written or printed matter, tapes, charts, maps, paintings, drawing, engravings, sketches, working notes and papers; reproductions of such things by any means or process; and sound, voice, magnetic, or electronic recordings in any form.
Environment	Aggregate of external procedures, conditions, and objects affecting the development, operation, and maintenance of an IT system.
Executive Order 12829	The NISP was established by E.O. 12829, 6 January 1993, "National Industrial Security Program" for the protection of information classified pursuant to E.O. 12356, April 2, 1982, "National Security Information," or its successor or predecessor orders and the Atomic Energy Act of 1954, as amended.
External System	An information system that is outside of the boundary established by the AO and can be part of an interconnected system (contractor-to-government).
Facility	A plant, laboratory, office, college, university, or commercial structure with associated warehouses, storage areas, utilities, and components, that, when related by function and location, form an operating entity. (A business or educational organization may consist of one or more facilities as defined herein.) For purposes of industrial security, the term does not include Government installations.

Facility (Security) Clearance	An administrative determination that, from a security viewpoint, a facility is eligible for access to classified information of a certain category (and all lower categories).
Field Office Chief (FOC)	Responsible for managing the DSS Mission across an assigned are of responsibility. IS Reps report to the Field Office Chief.
Formal Access Approval	Formal Access Approval is the documented approval by a data owner to allow access to a particular category of information. It can be linked to any caveated information, such as Compartmented, NATO, REL TO, Critical Nuclear Weapon Design Information, Communications Security (COMSEC) or Crypto variable information, FRD, etc.
Government Furnished Equipment (GFE)	Property that is acquired directly by the government and then made available to the cleared contractor for use.
Host	The individual who takes ultimate responsibility for preparation and maintenance of accreditation documentation (NSP) for the WAN. Usually the ISSM for one of the nodes, the Host also determines the requirements that must be met before connection to the WAN is permitted.
Information Owner (IO)	An element of a U.S. government agency designated by the agency head and delegated broad authority regarding acquisition functions.
Information System Boundary	All components of an information system to be authorized for operation by an authorizing official; excludes separately authorized systems, to which the information system is connected.
Information System (IS)	Any telecommunication or computer-related equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of voice or data, and includes software, firmware and hardware.
Information System Security Manager (ISSM)	The cleared contractor employee responsible for the implementation of Automated Information System security, and operational compliance with the documented security measures and controls, at the cleared contractor facility.
Information System Security Officer (ISSO)	The ISSO(s) is assigned by the ISSM when the facility has multiple authorized ISs, is in a multiple facility organization in which the ISSM has oversight responsibility for multiple facilities, or when the technical complexity of the facility's IS program warrants the appointment. The name and phone number of the ISSO(s) must be identified in the SSP(s). During an IS certification visit, the IS Rep or ISSP will determine what duties and responsibilities have been delegated to the ISSO and verify the ISSO understands them. During a Security Review, the IS Rep or ISSP will review those duties and responsibilities and verify the ISSO is carrying them out.

Interconnection Security Agreement (ISA)	Contract between telecommunication organizations for interconnecting their networks and exchanging telecommunication traffic.
Interim Approval to Connect (IATC)	Temporary approval granted by a WAN AO allowing the connection of a node to WAN.
Interconnected System	An interconnected network consists of two or more separately authorized systems connected together. Interconnected networks may be contractor-to-contractor or government-to-contractor connections, or a combination of both.
Internet Protocol	Connectionless protocol used in packet-switched layer networks, such as Ethernet.
Local Area Network	Computer network within a small geographical area such as a home, school, computer laboratory, office building, or group of buildings.
Master System Security Plan (MSSP)	The term "Master" is associated with an SSP that grants type authorization. Type authorization is an official authorization decision to employ identical copies of an information system or subsystem (including hardware, software, firmware, and/or applications) in specified environments of operation (e.g., same classification, contract, and physical environment).
Multiple User Stand-Alone	Systems that have one user at a time, but have a total of more than one user with no sanitization between users.
National Institute of Standards and Technology (NIST)	Organization that promulgates national level standards, including those designed to protect IS.
Network	An IS term meaning a network composed of a communications medium and all components attached to that medium whose responsibility is the transference of information. Such components may include ISs, packet switches, telecommunications controllers, key distribution centers, and technical control devices.
NISP Authorization Office (NAO)	Delegated the responsibility for the DSS mission for cleared contractor IS certification and accreditation oversight.
Node	Any device or collection of devices authorized under a single Systems Security plan connected to a WAN.
Physical Security	The measures used to provide physical protection of resources against deliberate and accidental threats.
Plan of Action and Milestones (POA&M)	Facilitates an agreement between the cleared contractor and DSS identifying items from the baseline configuration requirements cannot be met and the reasons. The POA&M documents deficiencies that can be corrected and defines a timeline for resolving the issues.

Protected Distribution System (PDS)	Secure conduit for protecting classified lines, transmitting data outside of a controlled area.
Radio Frequency ID	Technologies that use wireless communication between an object (also known as a tag) and an interrogating device (also known as a reader), for the purposes of automatically tracking and identifying of such objects.
Re-Authorization	An action taken by DSS when security relevant changes are made to an approved (M)SSP. An action taken by DSS 3 years from the date of the ATO for a (M)SSP.
Regional Director	Responsible for all aspects of operations within the region.
Risk	A combination of the likelihood that a threat will occur, the likelihood that a threat occurrence will result in an adverse impact, and the severity of the resulting impact.
Risk Acknowledgement Letter	Letter from the IO acknowledging the level of risk when an information system cannot be configured to meet requirements of the NISPOM based on customer defined requirements.
Risk Assessment	Process of analyzing threats to, and vulnerabilities of, an IT system, and the potential impact that the loss of information or capabilities of a system would have on national security. The resulting analysis is used as a basis for identifying appropriate and effective measures.
Risk Management	Process concerned with the identification, measurement, control, and minimization of security risks in IT systems to a level commensurate with the value of the assets protected.
SECRET	The designation that will be applied only to information or material the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.
Secure Terminal Equipment	Piece of equipment utilized to enable encrypted/secure voice and/or data communication.
Security Cognizance	The Government office assigned the responsibility for acting for CSAs in the discharge of industrial security responsibilities described in the NISPOM.
Security Content Automation Protocol (SCAP) Compliance Checker	Automated compliance scanning application that utilizes DISA STIG benchmarks and OS-specific baselines to analyze and report on the security configuration of the IS. The application can be run locally on the host system to be scanned, or scans can be conducted across a network.

Security-Relevant Change	A security-relevant change to a system is any change affecting the availability, integrity, authentication, confidentiality, or non-repudiation of an IS or its environment. Examples would include changes to the Identification and Authentication, Auditing, Malicious Code Detection, Sanitization, Operating System, Firewall, Router Tables and Intrusion Detection Systems of a system, or any changes to its location or operating environment.
Security Requirement	Types and levels of protection necessary for equipment, data, information, applications, and facilities to meet security policy.
Security Technical Implementation Guides (STIG)	The configuration standards for IA and IA enabled devices/systems.
STIG Viewer	A tool used in conjunction with the STIGs to view the compliance status of the system's security settings as reported by the compliance checker.
Single User Stand-Alone	Systems assigned to single user and are without network connectivity.
Systems Security Plan (SSP)	Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.
TOP SECRET	The designation that will be applied only to information or material the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.
TEMPEST	The protection of sensitive information being compromised from electronic equipment producing emanations.
User	Person or process authorized to access an IT system.
User Code	Software that allows a user to modify data or functions of an IS. Determining if an IS has user code may be a matter of degree, but as an example: If an IS only has a button that performs a single function when pressed, the system is considered to have no user code on it. If the user can input classified information and save it to the IS, then the IS certainly has user code.
Video Teleconference	Technology that facilitates the communication and interaction of two or more users through a combination of high-quality audio and video over Internet Protocol networks.
Voice Over Internet Protocol (VoIP)	Technology used for delivering different kinds of data from a source to a destination using IP (Internet Protocol).
Wide Area Network (WAN)	Network that exists over a large-scale geographical area.

APPENDIX M: REFERENCES

The following references were used in the creation of the DAAPM. This list is not all inclusive as the security controls reference additional material.

- E.O. 12829, *National Industrial Security Program*, January 6, 1993
- E.O. 13526, *Classified National Security Information*, December 29, 2009
- DoD 5220.22-M, Change 2, *National Industrial Security Program Operating Manual*, May 18, 2016
- CNSSI 1253, *Security Categorization and Control Selection for National Security Systems*, March 27, 2014
- CNSSI 4009,Committee on National Security Systems (CNSS) *Glossary*, April 6, 2015
- CNSSI 7003, *Protected Distribution Systems (PDS)*, September 30, 2015
- NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*, February 2010. (updated June 5, 2014)
- NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*
- NIST SP 800-53, Revision 4, *Recommended Security Controls for Federal Information Systems and Organizations*, April 2013 (Updates as of January 22, 2015)
- NIST SP 800-53A, Revision 4, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans*, December 2014
- NIST SP 800-60, Volume 1, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008
- NIST SP 800-61, Revision 2, *Computer Security Incident Handling Guide*, August 2012
- NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, September 2011
- FIPS 140-2, *Security Requirements for Cryptographic Modules*, May 25, 2001; Change notice December 3, 2002
- CNSSD 504, *Directive on Protecting National Security Systems From Insider Threat*
- E.O. 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing of Classified Information*
- Presidential Memorandum, *National Insider Threat Policy and Minimum Standards for Executive Branch Threat Programs*