Defense Counterintelligence and Security Agency Assessment and Authorization Process Manual

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

National Industrial Security Program Authorization Office

Version 2.2

31 August 2020

EXECUTIVE SUMMARY

U.S. Government policy is that all classified information must be appropriately safeguarded to assure the confidentiality and integrity of that information, as well as its availability when required by contract. This Defense Counterintelligence and Security Agency (DCSA) Assessment and Authorization Process Manual (DAAPM) is intended for use by cleared contractors participating in the National Industrial Security Program (NISP).

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 (A&A) process, formerly known as Certification and Accreditation (C&A). The DAAPM transitions the DCSA 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 following publications: National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations – A System Life Cycle Approach for Security and Privacy*; NIST SP 800-53, Version 4, *Security and Privacy Controls for Federal Information Systems and Organizations*; NIST SP 800-53A, Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organization;* the Committee on National Security Systems Instruction (CNSSI) 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 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 by 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 insure and verify unauthorized access to classified information is effectively denied and that performance of classified contracts is not adversely affected.

This DAAPM supersedes all previous versions of the DAAPM and Office of the Designated Approving Authority (ODAA) Process Manuals.

TABLE OF CONTENTS

1 INTRODUCTION

1.1 BACKGROUND

Federal agencies have adopted the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) as a common set of guidelines for the Assessment and Authorization (A&A) of Information Systems (IS). The Defense Counterintelligence and Security Agency (DCSA) adopted these standards in an effort to streamline and build reciprocity across all federal agencies and to ensure all cleared contractor systems that process classified information as part of the National Industrial Security Program (NISP) are authorized under the RMF A&A process. The RMF focuses on a more holistic and strategic process for the risk management of systems, 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 IS.

To enable information sharing within the Federal Government, NIST has a statutory responsibility to develop minimum requirements for the secure operation of systems processing classified information, to include A&A processes. DCSA's policies and procedures comply with these standards and align with the Federal Government's approach to system 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 DCSA will follow the guidance contained within this manual to complete the RMF process and obtain system authorization. DCSA will assess and authorize Special Access Program (SAP) systems in accordance with the DoD Joint SAP Implementation Guide (JSIG) Revision 4, located on the DCSA Webpage, when directed by contractual requirements. If contractual guidance is not provided, DCSA will apply the DAAPM. Industry must coordinate a SAP security plan submission with their assigned Information System Security Professional (ISSP), now called ISSP/Security Control Assessor (SCA) under the RMF.

Reciprocity, as defined in Committee on National Security Systems Instruction (CNSSI) No. 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 system 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 systems under DCSA cognizance include:

- DoD 5220.22-M, *National Industrial Security Program Operating Manual* (NISPOM), Incorporating Change 2

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

  - NIST SP 800-30, Revision 1, *Guide for Conducting Risk Assessments*

  - NIST SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations – A System Life Cycle Approach for Security and Privacy*

  - NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*

  - NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*

  - NIST SP 800-53A, Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations – Building Effective Security Assessment Plans*

- Committee on National Security Systems Instruction (CNSSI) 1253, *Security Categorization and Control Selection for National Security Systems*

- Committee on National Security Systems Directive (CNSSD) 504, *Directive on Protecting National Security Systems from Insider Threat*

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

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 DCSA NISP Authorization Office (NAO) has overall responsibility for content management of the DAAPM. However, this is accomplished through a change management process involving the NISP Information Systems Authorization (NISA) Working Group. Together, the DCSA NAO and NISA Working Group are 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 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 DCSA 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 assessment and 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. CMT members may request ad-hoc meetings as required to address high priority issues and items recognized by all parties as administrative in nature. 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 system are those identified in the authorized security plan. DCSA personnel use the security plan to evaluate the system requirements during system A&A efforts and Security Vulnerability Assessments (SVAs). Figure 1 shows the flow of changes into the DAAPM.

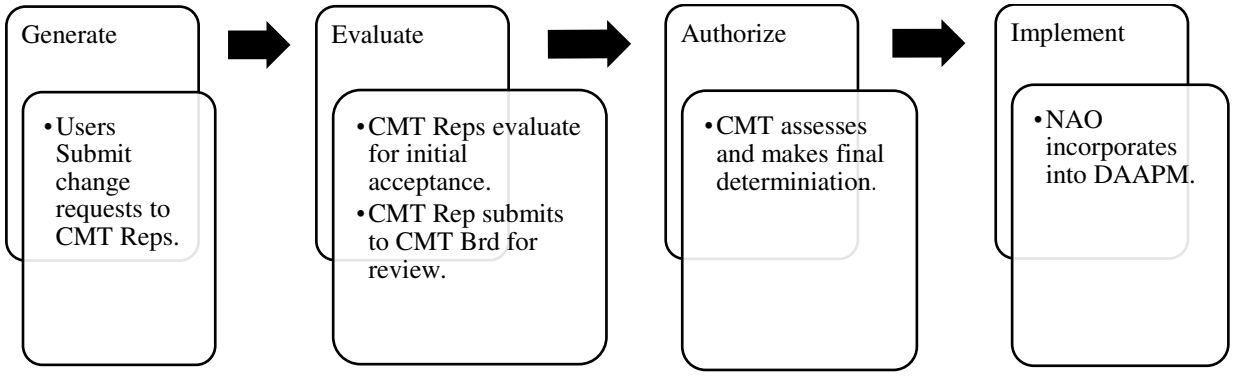


Figure 1 DAAPM Change Management Flow

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

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

c. Issuing security authorization decisions.

d. Verifying records are maintained for all system authorizations under AO purview.

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

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

g. Coordinating cyber incident responses related to classified systems.

h. Reviewing and approving Interconnection Security Agreement (ISA)/Memorandum of Understanding or Agreements (MOU/A) associated with systems 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' systems 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 a systems to determine the overall effectiveness of the controls.

b. Reviewing Risk Assessment Report(s) (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 system 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 systems to ascertain the need for additional safeguards.

f. Ensuring security assessments are completed for each system.

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&M) to ensure weaknesses are identified, effective/acceptable mitigation strategies are planned, and timelines are acceptable and on track.

i. Providing risk-based recommendations to the AO.

j. Assessing proposed changes to systems, 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 systems). The CCP may be an entity in the organization other than the assigned ISO/ISSM for a system that maintains these controls under a larger umbrella. Responsibilities of the CCP include, but are not limited to:

a. Documenting the common controls.

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

c. Documenting assessment vulnerabilities.

d. Providing system security documentation associated with common controls to the ISSMs inheriting those controls.

3.4 INFORMATION OWNER (IO)

An Information Owner (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 system 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, Department of Defense Contract Security Classification Specification, and Security Classification Guide (SCG)) and retaining 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 (C-I-A) Security Impact Levels associated with the IO's data when contractual requirements differ from the DCSA baseline or if concern is raised based on RAR.

f. Providing concurrence when the categorization deviates from the DCSA 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, and 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 a system. Responsibilities of the ISO include:

a. Ensuring 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 system.

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

d. Assisting the ISSM with performing risk assessments and documenting results in a RAR and keeping the risk assessment current throughout the acquisition/development portion of the system life cycle.

e. Providing the ISSM with updates to the POA&M, including identifying correction actions, determining resources required, documenting milestone completion dates, and addressing any residual findings.

f. Overseeing the development, maintenance, and tracking of the system security plan.

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

h. Appointing system users and determining access rights.

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

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

3.6 INFORMATION SYSTEM SECURITY MANAGER (ISSM)

The cleared contractor will appoint, in writing, an employee as the ISSM anytime classified processing involves information systems. 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 is accountable for the implementation of the RMF. The ISSM serves as the principal advisor on all matters, technical and otherwise, involving the security of systems under their purview. Each site is required to have an ISSM capable of effectively handling day-to-day operations and responding to security instances. Responsibilities of an ISSM include, but are not limited to:

a. Developing, maintaining, and overseeing the system 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 a new system.

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

d. Developing and implementing an effective system 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 system security program.

g. Completing training identified in ISSM Required Training Table within 6 months 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 system security program in accordance with Cognizant Security Activity (CSA) 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 system life cycle.

k. Developing, maintaining, and updating, in coordination with all system stakeholders, POA&Ms in order to identify system weaknesses, mitigating actions, resources, and timelines for corrective actions. Entries in the POA&M will be based on vulnerabilities and recommendations identified during assessments.

l. Certifying to the AO, in writing, that the requirements and implementation procedures listed within the security plan are in accordance with the NISPOM, NIST SP 800-53, and DAAPM.

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

n. Ensuring all system security documentation is current and accessible to properly authorized individuals.

o. Implementing security controls to protect the system, in coordination with system stakeholders.

p. Maintaining the system in accordance with the security plan and Authorization to Operate (ATO).

q. Ensuring audit records are collected and analyzed in accordance with the security plan.

r. Coordinating system authorizations with the ISSP and AO.

s. Obtaining and maintaining NISP Enterprise Mission Assurance Support Service (eMASS) access in order to effectively manage all security authorizations for systems under their purview.

t. Managing, maintaining, and executing the continuous monitoring strategy.

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

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

w. Ensuring configuration management policies and procedures are followed.

x. Assessing changes to a system that could affect the authorization.

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

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

aa. Ensuring proper measures are taken when a system incident or vulnerability affecting classified systems or information is discovered.

bb. Reporting all security-related incidents.

cc. Ensuring all users have the requisite security clearances, authorization, and Need-to-Know (NTK).

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

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

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

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

hh. 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 system security programs.

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

Table 1 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
Note: All **contractually required** training and/or technical certifications must be completed within specified time requirements. Completion of training will be evaluated during the SVA.	
ISSM Training Link: https://www.cdse.edu/toolkits/issm/overview.html	

3.7 INFORMATION SYSTEM SECURITY OFFICER (ISSO)

An ISSO is an individual responsible for ensuring the appropriate operational security posture is maintained for a system. The ISSO will be assigned by the ISSM and appointed in writing. The ISSO must be an U.S. citizen and employed by the cleared contractor or its subcontractor. The ISSO assists the ISSM 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 security plan.

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

c. Ensuring all proper account management documentation is completed prior to adding and deleting system accounts.

d. Verifying all system security documentation is current and accessible to properly authorized individuals.

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

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

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 a system that could affect authorization.

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

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

l. Completing the required training identified in the ISSM Required Training Table within 6 months of appointment.

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

n. Executing the continuous monitoring strategy.

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 level (FCL). The FSO is responsible for supervising and directing security measures necessary for implementing

applicable 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 ISSM efforts to implement the system's security program and policies for assigned areas of responsibility.

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

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

d. Developing and 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 and conducting periodic self-inspections related to the activity, information, system, 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 and cleanup procedures when there is a loss, compromise, or suspected compromise of classified information.

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

j. Enforcing physical access authorizations at entry and 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 administrative functions that general users are not authorized to perform. A privileged user is subordinate to the ISSM or ISSO on all matters related to system security. Privileged user accounts perform security-relevant functions (e.g., auditors, Data Transfer Agents (DTA), network administrators, and system administrators). Responsibilities of privileged users include, but are not limited to:

a. Complying with the system security program requirements as part of their responsibilities for the protection of systems 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 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 NTK, and assuming only those roles and privileges for which they are authorized.

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

f. Using a separate general user account to perform routine and non-administrative daily tasks.

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 system.

i. Taking necessary precautions to protect the C-I-A of information encountered while performing privileged duties.

j. Documenting and reporting to the ISSM all system security configuration changes and detected or suspected security-related system problems that might adversely impact system security.

3.10 GENERAL USER

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

a. Complying with the system security program requirements as part of their responsibilities for the protection of systems 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 General User Training.

d. Accessing only the data, system information, software, hardware, and firmware for which they have authorized access and a NTK, and assuming only those roles and privileges for which they are authorized.

e. Being accountable for all their actions on a system.

f. Protecting the system and associated 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 a system 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 to the ISSM/ISSO the receipt of any media received through any channel for subsequent virus inspection and inclusion into the media control procedures.

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

4 SECURITY TRAINING

All system users will receive initial and annual General User Training. System users assigned to positions requiring privileged access will also receive Privileged User Training.

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. Privileged users will not use their general user account to perform administrative activities, and privileged accounts will not be used for general user activities.

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

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

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

g. Instructions on protecting passwords or other authentication devices or mechanisms.

h. Operating system security features and system technical safeguard.

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

j. 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.

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 system account information.

c. The organization's policy regarding appropriate use of system 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, and 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 performs a security-relevant function in providing endpoint security during a data transfer. DTAs must be identified in writing. Training for DTAs will include, but is not limited to the following:

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

b. SCG.

c. Authorized AFT procedures and file formats.

d. Authorized media formats and marking requirements.

e. Data transfer logging procedures.

f. Incident handling procedures.

5 RISK MANAGEMENT FRAMEWORK

CNSS has developed a common information security framework for the Federal Government and its cleared contractors. This common framework aims 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 system authorization, the RMF process supports maintaining the system's security posture and facilitating senior leader decisions related to operational risk. CCPs' execution of the RMF, both internal and external, helps ensure security capabilities provided by the common controls can be inherited by system owners with a degree of assurance appropriate for their information protection needs. This approach recognizes the importance of security control effectiveness within systems 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 systems and the environment in which those systems operate. Managing information security related risks for a system 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, Revision 2, to replace the traditional C&A process with the seven-step RMF process: a preparatory step and six main steps. Figure 2 depicts the seven-step RMF process. The process emphasizes:

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

b. Maintaining awareness of the security state of systems 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 the system.

The objectives of the RMF process include:

a. Incorporating cybersecurity early 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 system level.

c. Providing a risk management methodology that gives organizations an accurate 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 Information Technology (IT) without retesting.

e. Emphasizing information security continuous monitoring and timely correcting deficiencies, including actively managing vulnerabilities and incidents.

The RMF steps include:

1. Prepare to execute the RMF from an organization and system level perspective. Establish a context and priority for managing security and privacy risk.
2. Categorize the system 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.
3. Select an initial set of baseline security controls for the system based on the security categorization, tailoring, and supplementing the security control baseline, as needed, based on an organizational assessment of risk and local conditions.
4. Implement the security controls and describe how the controls are employed within the system and its environment of operation.
5. Assess 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.
6. Authorize system 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 system and the decision that the risk is acceptable.
7. Monitor the system and associated security controls on an ongoing basis to include 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.

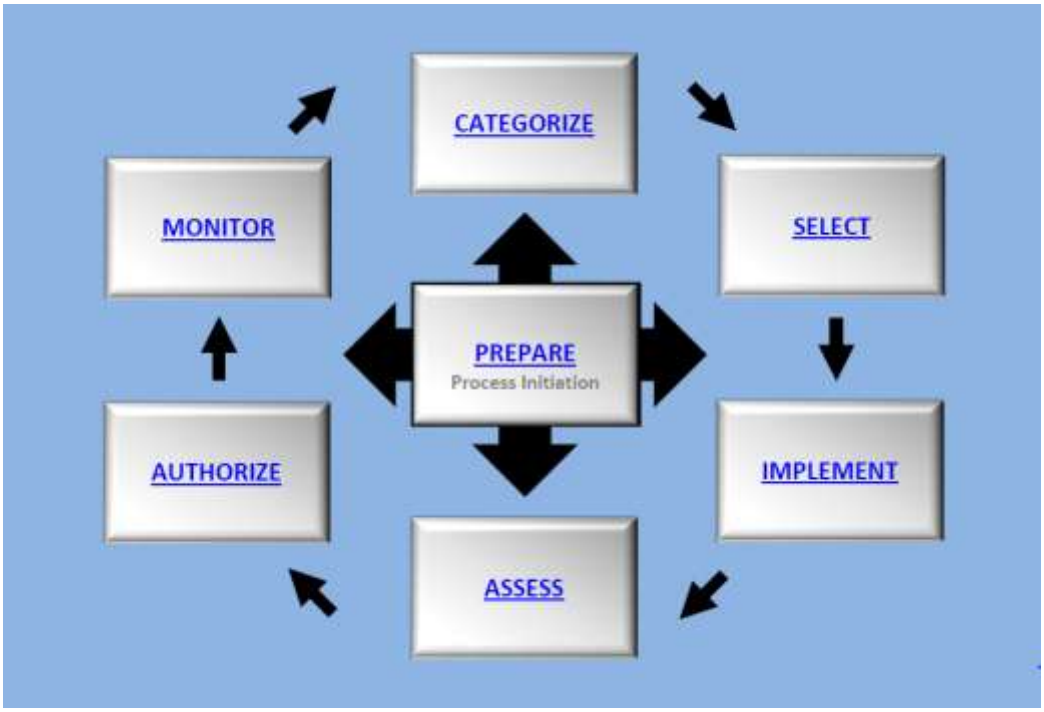


Figure 1 RMF Process

5.2 FUNDAMENTALS OF THE RMF

Managing system-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. Each step in the RMF has a defined set of tasks designed to achieve specific outcomes. Each task contains inputs needed to execute the task and expected outputs generated from successful task execution.

6 ENTERPRISE MISSION ASSURANCE SUPPORT SERVICE (eMASS)

The Enterprise Mission Assurance Support Service (eMASS) is a government-owned, web-based application with a broad range of services for comprehensive fully integrated cybersecurity management. Features include dashboard reporting, controls scorecard measuring, and generating a security plan. eMASS provides an integrated suite of authorization capabilities and prevents cyber attacks by establishing strict process control mechanisms to obtain authorization decisions.

Defense Information Systems Agency (DISA) manages eMASS's core functionality. DISA established an instance of eMASS for Industry. The Industry eMASS instance will be referred to as the NISP eMASS instance. DCSA SSP templates will no longer be submitted through the Office of the Designated Approving Authority (ODAA) Business Management System (OBMS) when requesting assessment and authorization

of a classified system. The security plan is built in eMASS and may be exported in numerous formats, if desired, by eMASS users. **All security plans must be submitted via the NISP eMASS instance:** https://nisp.emass.apps.mil/.

Reference the NISP eMASS Information and Resource Center located on the DCSA Webpage.

Warning: The NISP eMASS instance is **NOT APPROVED** for the storage of **classified information.**

6.1 EMASS WORKFLOW

The NISP eMASS instance supports the RMF A&A process. The overarching NISP eMASS workflow is represented in Figure 3 as a conceptual workflow with the embedded eMASS approval chains.

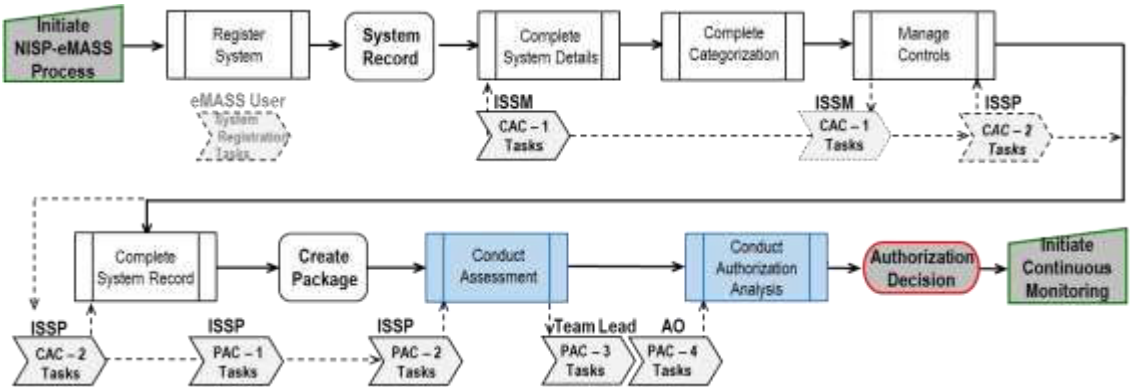


Figure 3 eMASS Workflow

6.2 EMASS APPROVAL CHAIN

An approval chain is a series of users or user groups who must approve content before the deliverable can be finalized. When the last person in the chain approves the content, the deliverable is complete. The approval chain replicates the RMF process.

The core approval chains in eMASS are:

a. **Control Approval Chain (CAC):** Primary vehicle through which the system security controls are approved and validated. The eMASS privileges are aligned with the system roles. As a standard, Industry users are assigned to the CAC – 1 role. ISSPs are assigned to the CAC – 2 role.

b. **Package Approval Chain (PAC):** Primary vehicle through which the system is assessed and authorized.

Figure 4 provides an overview of the NISP eMASS approval chains from the system record creation through the authorization decision. The DAAPM roles are identified across the top.

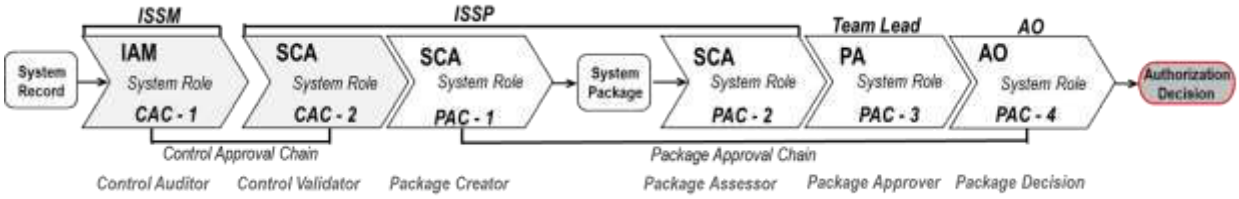


Figure 4 eMASS Approval Chain

Note: The diagram depicts a continuous workflow. However, the CAC and PAC are separate approval chains.

7 ASSESSMENT AND AUTHORIZATION IMPLEMENTATION GUIDANCE

A timely assessment and authorization decision is contingent upon Industry submitting a complete and accurate security plan. DCSA highly recommends submitting security plans, initial or a reauthorization, at least 90 days before the need date. A complete security plan has all the required system details, supporting artifacts, and security control information (including test results) needed to support authorization activities. This timeframe will allow for a complete plan review to include the on-site assessment, interaction between the ISSM and ISSP, and the opportunity to address any potential updates or changes to the security plan. If sufficient time is not allotted for a complete review prior to the Authorization Termination Date (ATD), Industry must cease processing until an ATO is issued.

This document describes the RMF efforts using the following content structure:

- Step Information
- Step Tasks
- Step Outputs
- Supporting Information
- Step References

7.1 PREPARE

The Prepare Step focuses on executing the organization's essential activities, mission and business processes, and system levels to help the organization manage its security and privacy risks using the RMF.

7.1.1 PREPARE STEP TASKS

The Prepare Step tasks are divided into the following categories:

- Organization Level
- System Level

The Prepare Step Tasks will have an alpha designator of **"P"** preceding the task number. For example, the first Prepare task will be Task P-1.

7.1.1.1 ORGANIZATION LEVEL TASKS

The organization requesting an authorization is responsible for the following tasks:

Task P-1: Identifying and assigning individuals to key roles in the execution of the RMF.

Task P-2: Establishing a risk management strategy for the organization that includes a determination and expression of organizational risk tolerance.

Task P-3: Completing an organization-wide risk assessment or updating an existing risk assessment.

Task P-4: Establishing and making available organizationally-tailored control baselines and/or cybersecurity framework profiles (optional).

Task P-5: Identifying, documenting, and publishing common controls available for inheritance.

Task P-6: Prioritizing organizational systems with the same impact level (optional).

Task P-7: Developing and implementing an organization-wide strategy for monitoring control effectiveness.

7.1.1.2 SYSTEM LEVEL TASKS

The ISSM/ISSO, with assistance from the ISO and Key Management Personnel (KMP), is responsible for the following tasks:

Task P-8: Identifying business functions and mission/business processes that the system is intended to support.

Task P-9: Identifying system stakeholders.

Task P-10: Identifying and prioritizing stakeholder assets.

Task P-11: Determining authorization boundaries.

Reference Authorization Boundaries – Section 8.0.

Task P-12: Identifying the types of information processed, stored, and transmitted by the system.

The ISSM should use the CNSSI 1253 reference to determine the data type.

Task P-13: Identifying and understanding all stages of the information life cycle for each information type processed, stored, or transmitted by the system.

Task P-14: Performing a system level risk assessment or updating an existing risk assessment.

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. Impacts 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 to determine if tailoring controls are required. The results are documented in the RAR. **The ISSM will review applicable SCGs and verify the classification level of RAR results**.

Task P-15: Defining and prioritizing security requirements.

Task P-16: Determining the placement of the system within the enterprise architecture.

Task P-17: Allocating security requirements to the system and to the environment in which the system operates.

Task P-18: Registering the system in the NISP eMASS instance.

During new system registration, the following details will be documented:

a. System Information.
b. Authorization Information.
c. Roles.

Follow instructions in the *NISP eMASS Industry Operation Guide* and reference the NISP eMASS Information and Resource Center located on the DCSA Webpage.

7.1.2 PREPARE STEP SUPPORTING INFORMATION

The eMASS has replaced OBMS as the system of record. The following applies:

a. All security plans must be submitted via the NISP eMASS instance located at: https://nisp.emass.apps.mil/.

b. Industry must have a DCSA sponsor and take the DISA eMASS training to establish a NISP eMASS account. Reference the NISP eMASS Training Access and Procedures for Cleared Industry.

c. Industry eMASS users will be assigned to the CAC – 1 role.

7.1.3 PREPARE STEP OUTPUTS

The process outputs for the Prepare Step are as follows:

- RMF Role Assignments
- Business Functions

- Risk Management Strategy
- Statement of Risk Tolerance
- RAR
- List of CCPs
- Common Controls Available via Inheritance
- Organizational Continuous Monitoring Strategy
- Supported Missions
- Mission/Business Processes
- System Information Type(s)
- System Stakeholder List
- Asset List
- Documented Authorization Boundary
- Security Requirements
- Security Architecture
- NISP eMASS System Record
- Documentation of the stages through which information passes in the system such as:
  - Data Flow Diagrams
  - Data Dictionaries
  - Database Schemas
  - Other Designated Deliverables

7.1.4 PREPARE STEP REFERENCES AND RESOURCES

This step is directly supported by the following:

REFERENCES

Short Title	Description
CNSSI 1253	Security Categorization and Control Selection for National Security Systems
NIST SP 800-30	Guide for Conducting Risk Assessments
NIST SP 800-37	Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy
NIST SP 800-39	Managing Information Security Risk: Organization, Mission, and Information System View
NIST SP 800-60	Guide for Mapping Types of Information and Information Systems to Security Categories

RESOURCES

Description	Location
DISA eMASS User Guide	Click “Help” on the eMASS screen
NISP eMASS Industry Operation Guide	https://www.dcsa.mil/mc/ctp/tools/
DCSA Webpage	https://www.dcsa.mil/mc/ctp/tools/

7.2 CATEGORIZE

The Categorize Step focuses on categorizing the system. Security impact levels are defined as Low, Moderate, or High for each of the three system security objectives: C-I-A. Systems will be categorized based on the impact due to a loss of C-I-A of the information or system. For example, a system may have a Confidentiality impact level of Moderate, an Integrity impact level of Low, and an Availability impact level of Low. The DCSA baseline identifies security control specifications needed to safeguard classified information that is stored, processed, or transmitted and adopts a baseline of M-L-L.

When contractual requirements differ from the DCSA baseline or if concern is raised based on the RAR, the IO will provide C-I-A security impact levels to the ISO and ISSM. The impact values will be documented in the security plan along with the research, key decisions, approvals, and supporting rationale. The

following paragraphs provide guidance in defining impact levels for all systems under the purview of DCSA.

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 system 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 system 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 system 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 system 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 system 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 system 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 system 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 system 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.

7.2.1 CATEGORIZE STEP TASKS

The Categorize Step Tasks will have an alpha designator of "C" preceding the task number. For example, the first Categorize task will be Task C-1.

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

Task C-1: Describing and documenting the characteristics of the system.
The System Description is the result of this task.

Task C-2: Categorizing the system.
The system 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 system, including the information processed by the system represented by the identified information types. Effective data type determination, using CNSSI 1253, will assist with categorization. Security categorization results must be documented, consistent with the enterprise architecture, to reflect the commitment to protecting organizational missions, business functions, and mission/business processes, and represent the organization's risk management strategy.

Task C-3: Reviewing security categorization results.
The categorization of the data and system must be coordinated with the IO. The IO is the authority for determining categorization and must be involved in the process.

Task C-4: Populating information not entered during new system registration and documenting categorization results in eMASS.
During the Categorize Step, Industry eMASS users will begin building the security plan.

Follow instructions in the *NISP eMASS Industry Operation Guide* and reference the NISP eMASS Information and Resource Center located on the DCSA Webpage.

7.2.2 CATEGORIZE STEP OUTPUTS

The process outputs for the Categorize Step are as follows:

- System Description
- Security Categorization
- Updated eMASS System Record

7.2.3 CATEGORIZE STEP REFERENCES AND RESOURCES

This step is directly supported by the following:

REFERENCES

Short Title	Description
CNSSI 1253	Security Categorization and Control Selection for National Security Systems
NIST SP 800-30	Guide for Conducting Risk Assessments

NIST SP 800-37	Risk Management Framework for Information Systems and Organizations – A System Life Cycle Approach for Security and Privacy
NIST SP 800-39	Managing Information Security Risk: Organization, Mission, and Information System View
NIST SP 800-60	Guide for Mapping Types of Information and Information Systems to Security Categories

RESOURCES

Description	Location
DISA eMASS User Guide	Click "Help" on the eMASS screen
NISP eMASS Industry Operation Guide	https://www.dcsa.mil/mc/ctp/tools/
DCSA Webpage	https://www.dcsa.mil/mc/ctp/tools/

7.3 SELECT

The Select Step focuses on selecting, tailoring, and documenting the security controls needed to protect the system and organization commensurate with risk.

7.3.1 SELECT STEP TASKS

The Select Step Tasks will have an alpha designator of **"S"** preceding the task number. For example, the first Select task will be **Task S-1**.

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

Task S-1: Selecting the security controls necessary to protect the system commensurate with risk.

The security control selection is based upon the results of the categorization. The DCSA security baseline identifies security control specifications needed to safeguard classified information that is stored, processed, or transmitted. The security baseline is standardized as M-L-L. Apply DCSA Overlay identified as applicable.

Task S-2: Tailoring the initial security controls.

Security control tailoring encompasses the following activities:

a. Identifying and designating common controls in initial baselines.

b. Making risk-based decisions on remaining baseline controls.

c. Selecting compensating controls.

d. Supplementing baseline with additional controls and control enhancements, if applicable.

The security controls listed in the initial baseline are not a minimum, but rather a proposed starting point from which controls may be removed or added based on tailoring guidance. Document 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 order to describe 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 system and/or its environment of operation.

Task S-3: Designating controls as system-specific, hybrid, or common controls and allocating to the specific system elements.

Control implementation can be characterized in the following terms:

System-Specific – Security controls specific to a system and the responsibility of the ISO/ISSM.

Common – Security controls that are inheritable by one or more organizational systems 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 systems 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 system level which in turn eliminates redundancy, gains resource efficiencies, and promotes reciprocity.

Hybrid – Security controls that are implemented in a system in part as a common control and in part as a system specific control. If any of the system components need system-specific infrastructure protections in addition to common controls that apply to the system, 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. However, the specific system requires additional availability protection based on the criticality of the information in the system resulting in the implementation of a separate uninterrupted emergency power source.

Task S-4: Developing a continuous monitoring strategy for the system that reflects security control effectiveness and the organizational risk management strategy.

The implementation of a robust continuous monitoring strategy allows an organization to understand the security state of the system 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:

a. Configuration management and control.

b. Security impact analyses on proposed changes.

c. Assessment of selected security controls.

d. Security status reporting.

The control selection information will be documented so a determination may be made as to whether the planned security implementation is acceptable to manage system risks.

Task S-5: Documenting security controls to include tailoring actions.

During the Select Step, Industry eMASS users will update the security plan in order to reflect the selection of security controls.

Follow instructions in the *NISP eMASS Industry Operation Guide* and reference the NISP eMASS Information and Resource Center located on the DCSA Webpage.

7.3.2 SELECT STEP OUTPUTS

The process outputs for the Select Step are as follows:

- Security Control Selection
- List of Tailored Controls
- Overlay Selection
- Updated System Details
- Continuous Monitoring Strategy

7.3.3 SELECT STEP REFERENCES AND RESOURCES

This step is directly supported by the following:

REFERENCES

Short Title	Description
CNSSI 1253	Security Categorization and Control Selection for National Security Systems
DAAPM – Appendix A	Security Controls (DCSA Organizational Values)
DAAPM – Appendix B	DCSA Overlays
NIST SP 800-30	Guide for Conducting Risk Assessments
NIST SP 800-37	Risk Management Framework for Information Systems and Organizations – A System Life Cycle Approach for Security and Privacy
NIST SP 800-39	Managing Information Security Risk: Organization, Mission, and Information System View
NIST SP 800-53	Security and Privacy Controls for Federal Information Systems and Organizations
NIST SP 800-53A	Assessing Security and Privacy Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans
NIST SP 800-137	Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations

RESOURCES

Description	Location
DISA eMASS User Guide	Click “Help” on the eMASS screen
NISP eMASS Industry Operation Guide	https://www.dcsa.mil/mc/ctp/tools/

DCSA Webpage	https://www.dcsa.mil/mc/ctp/tools/

7.4 IMPLEMENT

The Implement Step focuses on implementing the security controls for the system and documenting the specific details of the control implementation.

7.4.1 IMPLEMENT TASKS

The Implement Step Tasks will have an alpha designator of "I" preceding the task number. For example, the first Implement task will be Task I-1.

The ISSM/ISSO is responsible for the following tasks:

Task I-1: Implementing the selected security controls.
See the NIST SP 800-53 and Appendix A for additional information.

Task I-2: Documenting the security control implementation and providing a functional description of the control implementation.
The implementation plan will include any additional information necessary to describe how the security capability is achieved such as:

a. Planned inputs
b. Expected Behavior
c. Expected Outputs

Task I-3: Updating the security plan based on information obtained during the implementation of the security controls.
During the Implement Step, Industry eMASS users will continue completing the security plan.

If using an artifact to support the implementation of a control, provide the following: artifact name, description, type, template (if applicable), category (e.g., Implementation Guidance, Evidence, and Other), expiration date, last reviewed date, page number, and artifact owner (if applicable).

Follow instructions in the *NISP eMASS Industry Operation Guide* and reference the NISP eMASS Information and Resource Center located on the DCSA Webpage.

7.4.2 IMPLEMENT STEP OUTPUTS

The process outputs for the Implement Step are as follows:

- Implementation Plan
- System Level Continuous Monitoring (SLCM) Strategy
- Supporting Artifacts

7.4.3 IMPLEMENT STEP REFERENCES AND RESOURCES

This step is directly supported by the following:

REFERENCES

Short Title	Description
CNSSI 1253	Security Categorization and Control Selection for National Security Systems
DAAPM – Appendix A	Security Controls (DCSA Organizational Values)
DAAPM – Appendix B	DCSA Overlays
NIST SP 800-30	Guide for Conducting Risk Assessments
NIST SP 800-37	Risk Management Framework for Information Systems and Organizations
NIST SP 800-39	Managing Information Security Risk: Organization, Mission, and Information System View
NIST SP 800-53	Security and Privacy Controls for Federal Information Systems and Organizations
NIST SP 800-53A	Assessing Security and Privacy Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans

RESOURCES

Description	Location
DISA eMASS User Guide	Click "Help" on the eMASS screen
NISP eMASS Industry Operation Guide	https://www.dcsa.mil/mc/ctp/tools/
DCSA Webpage	https://www.dcsa.mil/mc/ctp/tools/

7.5 ASSESS

The Assess Step focuses on assessing the security controls applicable to the system and determining if the controls selected for implementation are implemented correctly, operating as intended, and producing the desired outcome.

7.5.1 ASSESS STEP TASKS

The Assess Step Tasks will have an alpha designator of "A" preceding the task number. For example the first Assess task will be Task A-1. The complexity of the Assess Step requires the tasks to be organized as follows:

- Part I - Industry (Tasks A–1 through A–8)
- Part II - ISSP (Tasks A–9 through A–11)
- Part III - Industry (Task A–12)

7.5.1.1 PART I – INDUSTRY

The ISSM/ISSO is responsible for the following tasks:

Task A-1: Conducting a self-assessment of the security controls.

The self-assessment process is conducted to ensure the security controls are implemented as organizationally intended to meet the security requirements for the system.

The ISSM/ISSO will conduct the security controls self-assessment utilizing the DISA Security Content Automation Protocol (SCAP) Compliance Checker (SCC) for automated checks and all appropriate baseline/benchmark Security Technical Implementation Guides (STIGs). Additional automated tools can be found at the following link: https://nvd.nist.gov/scap/validated-tools. **If the system cannot be assessed utilizing the specified scanning tools, Industry must document the justification and process for assessing the system in the security plan.** The self-assessment will then be conducted in accordance with the defined process.

In preparation for the ISSP assessment, the SCAP, STIG Viewer, and applicable STIG and/or SCC content must be installed on all supported systems. If the system cannot be assessed utilizing the specified scanning tools, the assessment will be conducted in accordance with the process detailed in the security plan.

Note: If not contractually mandated, systems are not required to be configured for compliance to STIG requirements. However, Industry is still required to harden systems in order to appropriately manage risk.

Task A-2: Conducting remediation actions to address deficiencies identified during assessment.

Task A-3: Developing a POA&M for unacceptable risks identified in assessment.

Task A-4: Reviewing the applicable SCG and verifying classification level of all security plan artifacts.

If supporting artifacts are deemed classified, contact assigned ISSP for guidance.

Task A-5: Finalizing the security plan for review and authorization consideration in eMASS.

In order to provide a complete security plan and facilitate the assessment and authorization process, the following supporting artifacts should be included:

a. RAR (Appendix C)
b. POA&M – A POA&M template is available via the NISP eMASS and RMF Knowledge Service.
c. Continuous Monitoring Strategy (will also be addressed in the SLCM section of eMASS)
d. Interconnection (ISA/MOU/A – if applicable)
e. RMF Security Plan Submission and Certification Statement (Appendix D)
f. ISSM/ISSO Appointment Letter (Appendix E)
g. ISSM Training Records
h. Sponsorship (Department of Defense (DD) Form 254, Request for Proposal (RFP), Framework Agreement)
i. Configuration Management (Hardware and Software Lists) (Appendix F and G)
j. System Diagram and/or Network Topology (Appendix H)
k. Facility/System Layout

l. Record of Controlled Area/Physical Security (Signed and legible DSS Form 147) (Appendix I)
m. IS Access Authorization and Briefing Form (Appendix J)
n. IS Privileged Access Authorization and Briefing Form (Appendix K)
o. Upgrade/Downgrade Procedures Record (Appendix L)
p. IS Security Seal Log (if applicable) (Appendix M)
q. Maintenance, Operating System, and Security Software Change Log (Appendix N)
r. Media Protection (AFT/Data Transfer Procedures) (Appendix O)
s. Contingency Plan (if applicable) (Appendix P)
t. Incident Response Plan (IRP) (Appendix Q)
u. Sanitization Procedures (Appendix S)
v. Mobility System Plan (if applicable) (Appendix T)
w. SPP (if applicable)
x. Artifacts (Standard Operating Procedures (SOPs), policies, etc.) demonstrating proper control implementation and/or requested by the AO.

Notes: The artifacts above are not an all-inclusive list. Templates are available in the DAAPM Appendices and available for download on the DCSA Webpage.

The eMASS requires a POA&M for non-compliant controls. If annotating the vulnerability is determined to be classified as per the SCG, indicate in eMASS that details will be maintained on-site.

Task A-6: Documenting self-assessment results and determining if all aspects of the security controls, including the Control Correlation Identifiers (CCIs), are compliant, non-compliant, or not applicable.

During the Assess Step, Industry eMASS users will finalize the security plan.

Follow instructions in the *NISP eMASS Industry Operation Guide* and reference the NISP eMASS Information and Resource Center located on the DCSA Webpage.

Task A-7: Verifying that all information is populated in eMASS.

Industry eMASS users will ensure the following is complete:

a. Required system details are populated.
a. Implementation Plan and SLCM is completed for all security controls.
b. Risk Assessment is addressed for all non-compliant security controls.
c. All Artifacts needed to support authorization activities are added.
d. Assessment Procedures (APs)/CCIs assigned to a security control are tested and the test results applied for all security controls.
e. POA&M is accurate and addresses all non-compliant controls.

Task A-8: Moving the security plan to the next stage of the CAC for validation.

Industry eMASS users will confirm that the security plan reflects 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. Once the security plan is complete, the security controls are ready to move to the next stage of the CAC (CAC – 2 role/ISSP). The ISSP will complete the control validation/assessment. Use the Bulk Processing feature in eMASS to submit all controls to the ISSP for validation.

Follow instructions in the *NISP eMASS Industry Operation Guide* and reference the NISP eMASS Information and Resource Center located on the DCSA Webpage.

7.5.1.2 PART II – ISSP

The ISSP is responsible for the following tasks:

Task A-9: Reviewing the final security plan and supporting artifacts.

The initial review will include:

a. Ensuring an adequate system description is provided.
b. Assessing security controls based upon implementation responses and test results. *Implementation responses and test results must provide sufficient data to describe how the security control is implemented and met.*
c. Validating justification for tailored-out controls.
d. Ensuring mitigated security controls have comparable safeguarding. *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.
f. Making a risk-based decision regarding compliance conditions.

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

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

Task A-10: Conducting the on-site assessment.

The on-site assessment will include:

a. Assessing the applicable technical security controls, system configuration, manual and not reviewed (NR) checks using the most up-to-date 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 make a risk-based recommendation.

Task A-11: Validating the controls.

The ISSP will validate the controls and record the results in eMASS.

7.5.1.3 PART III – INDUSTRY

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

Task A-12: Developing/Updating 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.

7.5.2 ASSESS STEP OUTPUTS

The process outputs for the Assessment Step are as follows:

- Assessment of Security Controls
- Remediation Actions
- Finalized Security Plan
- Review and Validation of Security Controls
- POA&M
- SAR

7.5.3 ASSESS STEP REFERENCES AND RESOURCES

This step is directly supported by the following:

REFERENCES

Short Title	Description
DAAPM – Appendix A	Security Controls (DCSA Organizational Values)
DAAPM – Appendix B	DCSA Overlays
NIST SP 800-30	Guide for Conducting Risk Assessments
NIST SP 800-37	Risk Management Framework for Information Systems and Organizations
NIST SP 800-53A	Assessing Security and Privacy Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans

RESOURCES

Description	Location
DISA eMASS User Guide	Click “Help” on the eMASS screen
NISP eMASS Industry Operation Guide	https://www.dcsa.mil/mc/ctp/tools/
DCSA Webpage	https://www.dcsa.mil/mc/ctp/tools/

7.6 AUTHORIZE

The Authorize Step focuses on formally authorizing the system for operation. Authorization decisions are based on an assessment of the application of the RMF and residual risk to loss/compromise of data.

7.6.1 AUTHORIZE STEP TASKS

The Authorize Step Tasks will have an alpha designator of **"R"** preceding the task number. For example, the first Authorize task will be **Task R-1**. The tasks will be divided into the following parts:

- Part I – ISSP
- Part II – AO

7.6.1.1 PART I – ISSP

The ISSP is responsible for the following tasks:

Task R-1: Verifying the finalized security plan.

The ISSP is responsible for verifying the security plan is complete and ready for final review by the AO. For systems inheriting common controls for specific security capabilities, the security plan for the common controls or a reference to such documentation must also be included.

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 arrangements, etc.), the ISSP will ensure the information needed by the AO to make a risk-based decision is included in the system security authorization package.

Task R-2: Submitting the system security authorization package via the PAC.

Once the CAC – 2 role (ISSP) has validated all security controls in eMASS, the ISSP will initiate the appropriate workflow and submit the finalized system security authorization package via the PAC for review and approval.

Task R-3: Applying an assessment decision.

As a PAC user within eMASS, the ISSP will apply an assessment decision. The ISSP will assess the package and provide a complete SAR containing the "Security Controls Assessor Executive Summary", the overall system cybersecurity risk, and the "Assessment Date". Additionally, the ISSP will recommend an ATD to the AO. When complete, the ISSP will submit the package to the next role in the approval chain.

7.6.1.2 PART II – AO

The AO is responsible for the following tasks:

Task R-4: Providing risk responses for determined risks.

The AO is responsible for determining whether the identified risks need to be mitigated prior to authorization. **The explicit acceptance of risk is the responsibility of the AO.**

Task R-5: Issuing an authorization decision for the system 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 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. ATD – Processing beyond this date is unauthorized.

Note: ATD cannot be greater than 1095 calendar days (3 years) and is determined by the AO.

Task R-6: Applying an authorization decision.

When the package is submitted to the AO role within eMASS, the AO will apply an authorization decision.

The following is a list of authorization decisions:

a. ATO
b. Authorization to Operate with Conditions (ATO-C)
c. Interim Authorization to Test (IATT)
d. DATO
e. Decommissioned

If necessary, the AO can add a residual risk statement as a comment or an artifact. The AO will have up to 30 days after a package has been authorized to update the authorization information.

Warning: An ATO cannot be issued if a non-compliant security control has a HIGH or VERY HIGH residual risk level.

7.6.2 AUTHORIZE STEP SUPPORTING INFORMATION

The package is a static snapshot in time once it enters the approval process. If the live system data is changed while the package is being reviewed, the package will not be updated. The package information cannot be edited or changed except for the following:

a. All POA&M items contained in the package are completely locked except for "severity" during the review process until approved by the AO when an authorization decision is applied.

b. Changes to the "severity" in the package POA&M items will be reflected in the live system.

c. The risk assessment summary contained in the package can be updated during the review process until it is finalized by the ISSP.

d. Changes to the Risk Assessment Summary in the package Risk Assessment will be reflected in the live system.

e. An assessment and authorization decision applied to the package will be reflected in the live data.

7.6.3 AUTHORIZE STEP OUTPUTS

The process outputs for the Authorization Step are as follows:

- Submission of System Security Authorization Package to the PAC
- Application of Approval Status to Security Plan
- SAR Executive Summary
- Authorization Decision

7.6.4 AUTHORIZE STEP REFERENCES AND RESOURCES

This step is directly supported by the following:

REFERENCES

Short Title	Description
DAAPM – Appendix A	Security Controls (DCSA Organizational Values)
DAAPM – Appendix B	DCSA Overlays
NIST SP 800-30	Guide for Conducting Risk Assessments
NIST SP 800-37	Risk Management Framework for Information Systems and Organizations
NIST SP 800-39	Managing Information Security Risk: Organization, Mission, and Information System View
NIST SP 800-53	Security and Privacy Controls for Federal Information Systems and Organizations
NIST SP 800-53A	Assessing Security and Privacy Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans
NIST SP 800-137	Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations

RESOURCES

Description	Location
DISA eMASS User Guide	Click “Help” on the eMASS screen
NISP eMASS Industry Operation Guide	https://www.dcsa.mil/mc/ctp/tools/
DCSA Webpage	https://www.dcsa.mil/mc/ctp/tools/

7.7 MONITOR

The Monitor Step focuses on maintaining an ongoing situational awareness about the security posture of the system and the organization. A continuous monitoring strategy is required to determine if the set of deployed security controls continues to be effective. Continuous monitoring activities support the concept of near real-time risk management through ongoing security assessments and risk analysis, and

by recording results in system security documentation. Continuous monitoring requires both automated and manual processes. A continuous monitoring strategy includes:

a. Maintaining and executing configuration management processes.

b. Determining the security impact of proposed or actual changes to the system and its operating environment.

c. Assessing selected security controls (including system-specific, hybrid, and common controls) based on the approved continuous monitoring strategy.

d. Ensuring security documentation is updated and maintained based on the results of continuous monitoring activities.

e. Providing security status reports on the security posture of the system to appropriate officials in accordance with the continuous monitoring strategy.

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

7.7.1 MONITOR STEP TASKS

The Monitor Step Tasks will have an alpha designator of **"M"** preceding the task number. For example, the first Monitor task will be **Task M-1**. The tasks will be divided into the following parts:

- **Part I – Industry**
- **Part II – ISSP**
- **Part III – AO**

7.7.1.1 PART I – INDUSTRY

The ISSM/ISSO with assistance from the ISO, FSO, and other system stakeholders is responsible for the following tasks:

Task M-1: Monitoring all technical, management, and operational security controls employed within and inherited by systems in accordance with the continuous monitoring strategy.

The frequency of monitoring is based on the continuous monitoring strategy developed by the ISO/ISSM as part of the security plan, or provided by the CCP and approved by the AO.

Task M-2: Conducting ongoing assessments of control effectiveness in accordance with the continuous monitoring strategy.

Task M-3: Analyzing and responding appropriately to the output of continuous monitoring activities.

This task includes conducting remediation/mitigation actions based on the results of ongoing monitoring activities, assessment of risk, and outstanding items in the POA&M.

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 M-4: Ensuring the system security documentation is updated and maintained based on the results of continuous monitoring.

The updated security plan 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 system security documentation 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 the original information needed for oversight, management, and auditing purposes is not modified or destroyed.

Task M-5: Reporting results of continuous monitoring activities to the ISSP.

Any anomalies or issues (e.g., security control deviations, threat environment changes, incidents impacting system 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.). Actions associated with continuous monitoring activities are a method to meet self-inspection requirements outlined in NISPOM, Chapter 8, Section 101h. The ISSM will be able to demonstrate that all of the weekly, quarterly, and annual activities have taken place as part of their self-inspection.

All appropriate administrative and security relevant documentation will be submitted to DCSA using eMASS. Security status reporting can be event driven, time driven, or both. The goal is ongoing communication with DCSA to convey the current security state of the system and its environment of operation. Security status reports will be appropriately marked, protected, and handled in accordance with Federal and organizational policies.

Task M-6: Implementing a decommission plan.

Note: *Decommission* has the same context as the NIST term, *Disposal*.

A decommission plan addresses the approach used to securely transition the system and system elements into a decommissioned state. The plan determines approaches, schedules, resources, specific considerations of decommission, and the effectiveness and completeness of decommission actions. Organizations will ensure all security controls addressing removal and decommissioning (e.g., media sanitization, configuration management, and control) are implemented. Users and application owners hosted on decommissioned systems will be notified as appropriate, and any security control inheritance relationships will be reviewed and assessed for impact.

A cybersecurity risk assessment for a system 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 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 system security authorization package.

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 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 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.

When requesting the decommission of an authorized system, the ISSM will initiate a Decommission Workflow in eMASS (Reference the *NISP eMASS Industry Operation Guide*). All storage media and memory associated with the system must be sanitized in accordance with the procedures outlined in the security plan. Provided the IO does not advise to the contrary, material associated with the system may be retained for up to two years, as outlined in the NISPOM, Chapter 5, Section 701. Records associated with the system must be retained for one assessment cycle. For more information on implementing a decommission plan/disposal strategy, please reference NIST SP 800-160 Volume 1.

Task M-7: Making updates to the live system.

As a result of continuous monitoring activities, the security plan may require updates within eMASS.

Follow instructions in the *NISP eMASS Industry Operation Guide* and reference the NISP eMASS Information and Resource Center located on the DCSA Webpage.

7.7.1.2 PART II – ISSP

The ISSP is responsible for the following tasks:

Task M-8: Reviewing the reported security status of systems under his/her purview to include the employed security control effectiveness within and inherited by the systems in accordance with the approved continuous monitoring strategy.

The review determines whether the operational risk remains acceptable to the organization, assets, individuals, other organizations, and/or to national security.

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, deficiencies, or to mitigate the identified risk. The information received by the ISSP during continuous monitoring activities is assessed and a risk recommendation is provided to the AO.

Task M-9: Reviewing and submitting decommission requests to the next role in the approval chain.

During the next DCSA SVA or contact/engagement, the ISSP will verify all security controls addressing system removal and decommissioning were implemented and storage media, memory, peripherals, etc. associated with the system were properly sanitized in accordance with the procedures outlined in the security plan and DAAPM.

7.7.1.3 PART III – AO

The AO is responsible for the following tasks:

Task M-10: Conducting ongoing authorizations using the results of continuous monitoring activities and communicating changes in risk determination and acceptance decisions.
The AO uses the information provided by the ISSP to determine if the authorization decision needs to be changed from an ATO to a DATO or if reauthorization action is necessary.

Task M-12: Formally decommissioning systems.

7.7.2 MONITOR STEP OUTPUTS

The process outputs for the Prepare Step are as follows:

- Decommission Plan
- Updated Security Plan
- Updated POA&M Remediation/Mitigation Items
- Technical, Management, and Operational Security Controls are Assessed, Modified and Submitted for Approval according to Continuous Monitoring Strategy

7.7.3 MONITOR STEP REFERENCES AND RESOURCES

This step is directly supported by the following:

REFERENCES

Short Title	Description
NIST SP 800-30	Guide for Conducting Risk Assessments
NIST SP 800-37	Risk Management Framework for Information Systems and Organizations
NIST SP 800-39	Managing Information Security Risk: Organization, Mission, and Information System View
NIST SP 800-53	Security and Privacy Controls for Federal Information Systems and Organizations
NIST SP 800-53A	Assessing Security and Privacy Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans
NIST SP 800-88	Guidelines for Media Sanitization
NIST SP 800-137	Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations

NIST SP 800-160	Systems Security Engineering - Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems

RESOURCES

Description	Location
DISA eMASS User Guide	Click "Help" on the eMASS screen
NISP eMASS Industry Operation Guide	https://www.dcsa.mil/mc/ctp/tools/
DCSA Webpage	https://www.dcsa.mil/mc/ctp/tools/

8 AUTHORIZATION BOUNDARIES

Security architecture plays a key part in the security control selection and allocation process for a system. Well-defined boundaries establish the scope of protection for organizational systems (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. Authorization boundaries are established in coordination with the security categorization process. 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 systems that must be separately managed, and as a consequence, unnecessarily inflate the total information security costs for the organization.

Establishing Authorization Boundaries

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

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

b. Process, store, and transmit similar types of information (e.g., same categorization impact levels).

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

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

Since commonality can change over time, the determination of the authorization boundary should be revisited periodically as part of the continuous monitoring process. ISOs will consult with key participants (e.g., AO, ISSP, ISSM, and system stakeholders) when establishing or changing authorization boundaries. The process of establishing authorization 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 authorization 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 system, 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 system level.

9 TYPES OF SYSTEMS

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

9.1 STANDALONE 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 DCSA Overlays (Appendix B) to assist with tailoring control selection.

9.2 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 based). The physical security parameters 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.

9.3 WIDE AREA NETWORK (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.

9.4 ENTERPRISE WIDE AREA NETWORK (EWAN)

An Enterprise Wide Area Network (eWAN) is a corporately shared physical IT infrastructure that hosts multiple classified NISP programs, distributed across multiple geographic locations (DCSA regions), through one enterprise network topology using an approved design. The NISP eWAN program serves as a high-level review of the personnel, processes, and technology necessary to plan, deploy, assess, and authorize an enterprise network topology that spans two or more DCSA geographic regions. eWANs are centrally managed and are a core function of the organization's classified work.

eWANs are authorized by NAO Headquarters and require approval for inclusion in the program. Facilities desiring to participate in the NISP eWAN Program must meet the requirements outlined in the NISP eWAN Program Job Aid. The job aid and associated resources are located on the DCSA Webpage.

9.5 UNIFIED WIDE AREA NETWORK (WAN)

A unified WAN applies when all involved AOs concur that there will be a single security policy for the entire WAN. For unified WANs where all the nodes are authorized by DCSA, the AO for the host node will authorize the system. The host ISSM is responsible for managing the system and must be notified before any changes are made. Only one security plan is required for a unified network. The security plan must include specific information for each node on the network.

9.6 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

In many cases, there are requirements for Industry to collaborate and share information in support of a contract or multiple contracts through the establishment of a contractor-to-contractor connection. If DCSA is the AO for both authorized systems, an Interconnection Security Agreement (ISA) may be required to establish an interconnection between two or more separately authorized systems. An ISSM at one of the connecting sites is designated as the lead or "Host ISSM." The ISA is submitted and managed by the designated host ISSM. The host DCSA AO will be the first to sign the ISA with coordination to the connecting DCSA AO nodes.

For a template and additional information regarding ISAs, reference NIST SP 800-47.

An ISA is required if one or more of the following is true:

a. The interconnection is between two or more separately authorized systems located at multiple facilities or campuses under multiple Commercial and Government Entity (CAGE) codes.

b. There is more than one IO.

c. The interconnection involves multiple AOs.

The Host ISSM is responsible for the following tasks:

a. Creating and managing the ISA.

b. Submitting the ISA to DCSA via the assigned ISSP.

c. Uploading the signed ISA within the security plan.

The ISSP is responsible for the following tasks:

a. Assessing the ISA and coordinating assessment activities with the connecting nodes' assigned ISSPs.

b. Providing a recommendation and submitting the ISA to all involved DCSA AOs for signature.

c. Distributing the signed ISA to all stakeholders (DCSA AOs, ISSPs, and ISSMs).

The signed ISA will be included as a security plan artifact for all connecting nodes.

An ISA is ***NOT*** required if all of the following are true:

a. The interconnection is between two or more separately authorized systems located at the same facility or campus under a single CAGE Code.

b. There is a single IO for all systems.

The ISSM is responsible for the following tasks:

a. Documenting the interconnection in the security plan.

b. Clearly identifying how user access is achieved.

c. Ensuring the configuration diagram accurately depicts all interconnections and hardware.

d. Conducting coordination via the CCB.

The ISSP is responsible for the following tasks:

a. Validating the interconnection.

b. Assessing the applicable technical system security controls and configuration.

c. Assessing the supporting operational and managerial security controls.

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

Government-to-Contractor Connections

An ISA (i.e., MOU/A) between DCSA and the IO is required for all government-to-contractor connections. The purpose of an ISA is to adjudicate the differences in requirements between AOs, establish roles and responsibilities, and outline technical requirements and connection processes. When specifically required by the IO, ISAs will be executed for contractor facility connections to government systems. These agreements will be coordinated at the Agency level and are outside of the scope of the DAAPM.

DCSA has a standard government-to-contractor ISA template. Although IOs and program offices may have their own standard template, it is highly recommended that the DCSA-approved government-to-contractor ISA template be used. If an ISA is submitted in a format other than the DCSA-approved template, DCSA may levy additional requirements in order to be NISPOM-compliant and further DCSA internal reviews will be required.

All ISAs must be submitted to NAO Headquarters by the IO for coordination and signature on behalf of cleared industry. **NAO will not process ISAs for coordination that are sent directly from the cleared contractor**. Industry must work and communicate with their IO and/or ISO to determine the appropriate AO or AO representative to serve as signatory to the ISA. 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 are violated.

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

Government-to-Contractor ISA Content

As stated above, it is highly recommended that the DCSA-approved government-to-contractor ISA template (Appendix W) be used.

All ISAs must contain the following minimum information:

a. Date of the ISA.

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. Connection approval process.

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 expiration date or review frequency (if applicable).

k. Categorization/security impact level.

l. Minimum clearance level required of users.

m. Network type.

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 and none will be added in the future (Secret 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.

Note: In addition to ISAs, interconnection agreements can also be established via MOU/As. DCSA recommends the use of the DCSA standard Government-to-Contractor ISA template to facilitate government-to-contractor connections.

Government-to-Contractor ISA Changes and Invalidations

Certain ISAs specify a pre-determined review frequency. During the review, security parameters, the accuracy of the ISA, Point of Contact (POC) information, and AO signatory information will 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.

ISAs 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.

9.7 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. The security plan can be used to support the official Secure Communications Plan (SCP) for approval. If a separate SCP is approved by the Designated Security Authorities (DSA) or as part of a Program Security Instruction (PSI), the SCP will be added as a supporting artifact. Industry will include the following as supporting artifacts with the security plan:

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. Employees will acknowledge the briefing in writing. The boundaries of releasable information 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 and 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.

9.8 FEDERAL INFORMATION SYSTEMS

Federal IS are owned and authorized by a U.S. Federal Agency. If a Component or Government Contracting Authority (GCA) needs to locate a federal IS at a cleared contractor facility they must follow the provisions of DoD Manual 5220.22, Volume 2.

Note: Cleared contractors do not have the responsibility to request exceptions or authority to deviate from the above guidance.

9.9 PROPOSAL SYSTEMS

Proposal Systems support pre-contract award activity. Pre-contract award activity involves response to Broad Agency Announcements (BAAs), Request for Proposals (RFPs), Requests for Information (RFIs), Rough Orders of Magnitude (ROMs), white papers, and other solicitations. In order to support Industry in pursuits for new business and an acceptable level of risk management, DCSA established the following expedited process for SUSA and MUSA proposal system authorizations:

a. Proposal systems may be submitted for authorization *PRIOR* to solicitation request.

b. This process will only be used for SUSA and MUSA proposal systems with the applicable overlay applied. By keeping the proposal system as a SUSA/MUSA, the A&A process can be expedited (i.e., less complex, on site may be waived, reduced controls, etc.). Proposal LANs will not be authorized using the expedited process.

c. Include the following SOPs with the security plan:

- Upgrade/Downgrade Procedures – Include clearing/sanitization procedures used between solicitations.

- Hibernation Procedures – A variance/special procedure that specifies how the system will be protected during a dormant state. The procedures will include a process for protecting the system through the use of physical security controls (e.g. seals, locks, alarms, and GSA-approved containers), technical controls (e.g., whole disk encryption, disabled accounts, and audit logs), and immediate patching/updates upon return to service. **Periods of hibernation will not exceed 180 days without AO approval.**

d. Use the NISP Classified Configuration (NCC) Toolkit. For more detailed instructions, reference the job aid located on the DCSA Webpage.

e. Conduct an assessment using the DISA SCAP SCC for automated checks and all appropriate baseline/benchmark STIGs. If the system cannot be assessed utilizing the specified scanning tools, the assessment will be conducted in accordance with the security plan. **Scan results will be provided as an artifact within eMASS *PRIOR* to any classified information being introduced to the system. If annotating a system vulnerability is determined to be classified as per the SCG, contact the assigned ISSP.**

f. Provide continuous monitoring strategies for active system use (solicitation actions) and in hibernation.

g. Identify physical security requirements clearly in the security plan.

h. When solicitation is received, update the security plan by uploading the solicitation request as a supporting artifact.

i. Reassess the current security plan and update upon contract award in accordance with the contractual requirements. DCSA will determine whether or not a reauthorization is required.

j. The ATD will be determined by the AO.

9.10 SPECIAL CATEGORIES

Special category systems, as described in the NISPOM, Chapter 8, Section 304, will follow the same authorization process as all other systems. 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 system will be addressed in the security plan.

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 system. 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 system.

The AO assesses the risk of operating the special categories system 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.

9.10.1 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 systems 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. Industry must coordinate with the IO and provide evidence that this type of system is contractually required. For controls tailored out based on contractual requirements, the AO must be provided with the complete rationale and justification via a Statement of Work (SOW), DD Form 254, or artifact from the IO. In addition, the RAR must detail the specific security controls that cannot be implemented. If a system meets the criteria of a legacy system (e.g., incapable of meeting the baseline security control requirements), authorization for continued use of a legacy system may be authorized by the AO.

9.10.2 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. The mobile system must be operated and maintained by trained personnel and relocation should be temporary. 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 inform their assigned ISSP. The ISSP will conduct the appropriate risk management evaluation and provide a risk-based recommendation to the AO. The AO will determine whether or not the system must return to the originating site and if additional safeguards are required. The mobile processing plan must be updated accordingly. All mobile systems are required to return to the originating site for final disposition with the exception of transfers and/or procedures authorized by the AO.

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 U).

Note: Mobility will not be used for noncontractual purposes and/or to circumvent the submission of a system for RMF assessment and authorization.

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

9.10.4 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 a system as a peripheral device. In these instances, the multifunction device should be included in the security plan. In particular, area upgrade and monitoring may be necessary to ensure physical security is applicable to these systems.

9.10.5 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, Network Address Translation (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 Operating System (OS) used in a virtual environment within the package as well as the technical protection measures in place to filter network communication external to the host.

9.10.6 TEST EQUIPMENT

Test equipment with non-volatile memory used to process or retain classified information requires authorization and must implement all applicable security controls unless component limitations, technical configurations, and/or test conditions render the security controls non-applicable. In these cases, justification must be provided for any controls designated non-applicable due to the aforementioned limitations.

Industry must have sanitization procedures (e.g., Certificate of Volatility from the manufacturer) for all test equipment, classified or unclassified (volatile memory included). Test equipment manufacturers publish clearing and sanitization procedures. In situations where user accessible or configurable data is

contained in Electrically Erasable Programmable Read-Only Memory (EEPROM) or Flash Erasable PROM (EPROM), the only approved procedures are those provided by the manufacturer. Additional requirements in the clearing and sanitization matrix also apply. The ISSP will assess all procedures to ensure implemented procedures meet requirements and 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.

9.10.7 VIDEO TELECONFERENCE (VTC)

VTC systems are used to display, transmit, and receive audio and video signals across a telecommunication medium, and are not considered system peripherals. VTC systems with non-volatile memory and/or network connectivity must be addressed in the security plan as system components and all applicable security controls must be identified, documented, and implemented or mitigated.

9.10.8 VIDEO DISTRIBUTION SYSTEM (VDS)

Video Distribution System (VDS) is the distribution or delivery of digital media content such as audio, video, and software. VDS with non-volatile memory and/or network connectivity must be addressed in the security plan as system components and all applicable security controls must be identified, documented, and implemented or mitigated.

9.10.9 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. The only network protocol that is allowed/authorized is TCP/IP. Other protocols require authorization by the AO.

b. All management protocols will be disabled unless authorized by the AO.

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

d. All peripheral devices will be maintained or upgraded to the most current firmware available.

e. All peripheral devices will be 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 (e.g., passwords, service settings, etc.) is maintained after a power down or reboot.

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

i. Auditing will be fully enabled for those devices that can generate audits.

j. Unauthorized access will be prevented. Repair procedures will not result in unauthorized dissemination of, or access to, classified information.

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

l. Knowledgeable and cleared personnel will 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 will have the appropriate discretionary access control list in place.

n. Devices will be configured to prevent non-administrators from altering the global configuration of the device.

10 DEPARTMENT OF DEFENSE INFORMATION NETWORK (DoDIN)

The Department of Defense Information Network (DoDIN) is defined by Joint Publication 3-12, Joint Cyberspace Operation, as "the globally interconnected, end-to-end set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, including owned and leased communications and computing systems and services, software (including applications), data, and security."

In order to connect to the DoDIN, Industry must have a validated requirement approved by a sponsoring government IO and validation of the mission requirement from the DoD CIO in accordance with CJCIS 6211.02D. Obtaining and retaining enclave connections to the DoDIN requires Industry to follow the step-by-step procedures outlined in the applicable Connection Process Guide (CPG). CPGs explain the connection process for DoDIN networks and services.

Examples of DoDIN connected systems are the following: SIPRNet, Missile Defense Agency Classified Network (MDACNet), DREN, DISN Test Evaluation Network (DTEN), DARPA Secure Wide Area Network, (DSWAN), Joint Interoperability Test Command, (JITC), Joint Training and Experimentation Network (JTEN), Multi-Agency Collaboration Environment (MACE), and SDREN.

Table 3 DoDIN Information and Resources

DoDIN Information and Resources	
Defense Information Systems Network (DISN) CPG	https://www.disa.mil/network-services/Enterprise-Connections/Connection-Approval
DoDIN Connection Approval FAQS	https://www.disa.mil/Network-Services/Enterprise-Connections/FAQs/Connection-Approval-FAQs
DoDIN Network Topology Requirements	https://www.disa.mil/Network-Services/Enterprise-Connections/Mission-Partner-Training-Program/DSN-Topology-Requirements
Mission Partner Library for DoDIN Connections and Services	https://www.disa.mil/Network-Services/Enterprise-Connections/Mission-Partner-Training-Program
NISP SIPRNet Circuit Approval Process Guide (NSCAP)	https://www.dcsa.mil/mc/ctp/nao/

11 CROSS DOMAIN SOLUTION (CDS)

DoD Instruction (DoDI) 8540.01, Cross Domain Policy, Section 2.a(2) specifically states the instruction applies to all cross domain capabilities to, from, within, or between DoD systems to include mission partner and cleared defense contractor systems. DoDI 8540.01, Section 3.c specifically states cross domain capability requirement must be met by a CDS listed on the Unified Cross Domain Services Management Office (UCDSMO) – managed CDS baseline list. DoDI 8540.01, Section 8.u.(1) specifically states a Cross Domain Solution Authorization (CDSA) is issued by DoD Information Security Risk Management Committee (ISRMC) or Defense Information Assurance /Security Accreditation Working Group (DSAWG) before allowing a CDS to access or transfer information between different interconnected security domains. A CDSA is required for use of a CDS. The CDSA is issued by ISRMC or DSAWG.

High-level overview training for CDS, DSAWG and the CDS connection approval process is located at the following link:

https://www.disa.mil/Network-Services/Enterprise-Connections/Mission-Partner-Training-Program

12 AUDIT VARIANCE

During periods of system inactivity (e.g., hibernation) or when a facility plans to stop work for an extended period of time (e.g., holiday shutdowns), an audit variance may be authorized. **Periods of hibernation will not exceed 180 days without AO approval.** When requesting an audit variance, Industry must have an SOP that specifies how the system will be protected during a dormant state. The SOP will include a process for protecting the system through the use of physical security controls (e.g., seals, locks, alarms, and GSA-approved containers), technical controls (e.g., whole disk encryption, disabled accounts, and audit logs), and immediate patching/updates upon return to service. The audit variance will be authorized via the security plan (i.e., added as a supporting artifact). Industry is required to maintain a log

of audit variance activities on-site. Audit variance documentation will be assessed during the SVA and other engagement activities (e.g., Advise & Assist visits, periodic communications, etc.).

13 TYPE AUTHORIZATION

Type authorization is an official authorization decision to employ identical copies of a system in specified environments of operation. This form of authorization allows a single security plan to be developed for an archetype (common) version of a system that is deployed within a specified facility (under a single CAGE Code). 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 system. Type authorization is available to all authorized systems unless specified otherwise in the authorization decision.

The facility is not authorized to utilize a combination of conditions from multiple authorized systems. For example, a type authorized system must be:

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

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

c. Residing in the same general operating environments.

d. Inheriting common security controls.

The ATD of the initial type authorized system will apply to all identical copies of the system. If the authorization package associated with type authorization is issued a DATO, all systems authorized under that package are no longer permitted to process classified information.

In order to ensure the successful management and operation of type authorized systems, Industry must follow the instructions detailed in the NISP eMASS Industry Operation Guide. The NISP instance of eMASS is not only the database of record for A&A activities, but it is also used as a tracking tool for all NISP systems, including those that are type authorized.

When a system will be used for type authorization, Industry is required to select [Yes] in the System Information > Type Authorization section. In addition, Industry is responsible for updating the System Information > System Description section and uploading the applicable artifacts (e.g., Test Results, Hardware and Software Baselines, Facility/System Layout, Record of Controlled Area, and artifacts requested by the ISSP/AO).

Type authorization does not apply to expanding an existing authorized system (e.g., adding workstations to a Client/Server LAN). Expanding an existing system is addressed through the implementation of the Configuration Management (CM) security controls (e.g., CM-1, CM-2, CM-2(1), CM-3, etc.). All hardware and software changes to a system must go through a configuration change control process. Configuration change control is the documented process for managing and controlling changes to the configuration of a system. Industry will follow their authorized configuration management policy and associated procedures to implement configuration changes.

The exception to type authorization are DoDIN connected systems. The appropriate CPG must be followed for design, implementation, operation, and decommission (disposal).

APPENDIX A: SECURITY CONTROLS (DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY ORGANIZATIONAL VALUES)

The Defense Counterintelligence and Security Agency (DCSA) Security Controls, including the DCSA Moderate-Low-Low (M-L-L) Security Control Baseline, is available in spreadsheet form on the DCSA Webpage, located at: https://www.dcsa.mil/mc/ctp/tools/. The spreadsheet details the requirements for security control implementation, organizational values, supplemental guidance, as well as DCSA specific guidelines. **The Security Controls spreadsheet must be used for all systems requiring DCSA assessment and authorization.**

APPENDIX B: DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY OVERLAYS

Defense Counterintelligence and Security Agency (DCSA) Overlay

The DCSA overlay identifies security control specifications needed to safeguard classified information that is stored, processed, or transmitted. The DCSA 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 Local Area Network (LAN) (ISOL)/Peer-to-Peer (P2P)

References

- Committee on National Security Systems Instruction (CNSSI) 1253, *Security Categorization and Control Selection for National Security Systems*
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Rev. 4, *Security and Privacy 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 systems. This overlay provides guidance on the security controls required to be implemented on standalone systems. 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)

An ISOL/P2P is defined as a group of computers and network devices connected together over a relatively small geographic area and the constituent systems retain their own local security policy. 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. This overlay does not apply to client/server LANs.

An isolated LAN typically has none of the following:

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

DCSA Overlay – Table of Security Controls

The table below summarizes the security control specifications as they apply to the DCSA 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 DCSA Overlay is permitted with the approval of the Authorizing Official (AO). Tailoring may be needed if additional overlays apply to the 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	-	-	-
AC-17 (2)	Remote Access | Protection Of Confidentiality/Integrity Using Encryption	-	-	-
AC-17 (3)	Remote Access | Managed Access Control Points	-	-	-

Ctrl No	Ctrl Name	SUSA	MUSA	ISOL/P2P
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			
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			

Ctrl No	Ctrl Name	SUSA	MUSA	ISOL/P2P
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			
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			

Ctrl No	Ctrl Name	SUSA	MUSA	ISOL/P2P
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-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			

Ctrl No	Ctrl Name	SUSA	MUSA	ISOL/P2P
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			
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	-	-	-

Ctrl No	Ctrl Name	SUSA	MUSA	ISOL/P2P
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	-	-	-
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	-	-	-

Ctrl No	Ctrl Name	SUSA	MUSA	ISOL/P2P
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	
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			

Ctrl No	Ctrl Name	SUSA	MUSA	ISOL/P2P
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			
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			

Ctrl No	Ctrl Name	SUSA	MUSA	ISOL/P2P
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			
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			

Ctrl No	Ctrl Name	SUSA	MUSA	ISOL/P2P
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-2	Senior Information Security Officer			
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			
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			

Ctrl No	Ctrl Name	SUSA	MUSA	ISOL/P2P
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			
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	-	-	-

Ctrl No	Ctrl Name	SUSA	MUSA	ISOL/P2P
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			
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			

Ctrl No	Ctrl Name	SUSA	MUSA	ISOL/P2P
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	-	-	-
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)	-	-	-

Ctrl No	Ctrl Name	SUSA	MUSA	ISOL/P2P
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	-	-	-
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	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	-	-	-

Ctrl No	Ctrl Name	SUSA	MUSA	ISOL/P2P
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	-	-	-
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 TEMPLATE

RISK ASSESSMENT REPORT (RAR)

<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/Unique Identifier*> consists of <*System Description*> processing <*Classification Level*> data. The risk categorization for this system is assessed as <*e.g., Moderate-Low-Low*>.

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

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

The Information System Security Manager (ISSM) is <*insert Point of Contact (POC) information, including address and phone number*>.

The Information System Security Officer (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 Risk Management Framework (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 system, this assessment will include any known risks related to the incomplete or inadequate implementation of the National Institute of Standards and Technology (NIST) Special Publication (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.)

TYPE OF THREAT SOURCE	DESCRIPTION
ADVERSARIAL - Standard user - Privileged user/Administrator	Erroneous actions taken by individuals in the course of executing everyday responsibilities.
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**.
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.

Qualitative Values	Semi-Quantitative Values		Description
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.
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.

Qualitative Values	Semi-Quantitative Values		Description
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 system. List the risks to system 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	Security Control(s)	Likelihood (Tables 2 & 3)	Impact (Table 4)	Risk (Tables 5 & 6)
e.g. Hurricane	*Power Outage*	*Backup generators*	*PE-12*	*Moderate*	*Low*	*Low*

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

_____

Signature
Government Information Owner

_____

Printed Name, Title, and Phone Number

Note: *Information Owner acknowledgment is only provided if necessary or required by the DCSA AO. (Examples: Legacy Operating Systems, Risk concerns raised based on the results of the RAR, deviations from the DCSA baseline, etc.)*

APPENDIX D: RISK MANAGEMENT FRAMEWORK SECURITY PLAN SUBMISSION AND CERTIFICATION STATEMENT

To: Defense Counterintelligence and Security Agency (DCSA)

27130 Telegraph Road

Quantico, VA 22134

Subject: Risk Management Framework (RMF) Security Plan Submission and Certification Statement

Facility Name:	CAGE Code:
Address:	
ISSM Name:	
ISSM Phone:	
System Name:	

Note: *The System Name must follow the DCSA guidance for the National Industrial Security Program (NISP) Enterprise Mission Assurance Support Service (eMASS) System Naming – Details provided in the NISP eMASS Industry Operation Guide. Example: 12345-SUSA-GAUNTLET*

By submitting this security plan, I am providing formal certification that the requirements and implementation procedures listed within the RMF security plan are in accordance with National Industrial Security Process Manual (NISPOM), National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, and the DCSA Assessment and Authorization Manual (DAAPM). I certify that all security controls and protection measures as described in the completed plan 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 Milestones (POA&M).

By signing below, I certify that the information provided 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 E: INFORMATION SYSTEM SECURITY MANAGER APPOINTMENT LETTER

MEMORANDUM FOR RECORD

SUBJECT: Information System Security Manager (ISSM) Appointment

References:

a. Department of Defense (DoD) 5220-22-M, *National Industrial Security Program Manual (NISPOM)*, Incorporating Change 2, May 18, 2016.
b. Defense Counterintelligence and Security Agency (DCSA) Assessment and Authorization Manual (DAAPM) v2.1, March 9, 2020.

1. Effective immediately, [INSERT NAME] is appointed to the ISSM in support of [INSERT FACILITY NAME], [INSERT CAGE CODE].

2. The ISSM will acquire and maintain the appropriate knowledge in accordance with NISPOM, Chapter 8, Section 103 and DAAPM, section 3.6. Required training depends on the complexity and scope of the systems managed by the ISSM and associated responsibilities.

3. I confirm that the above named individual meets the qualifications required for oversight of the system security program and policies.

4. The ISSM shall perform the duties and responsibilities as outlined in the above cited references to ensure the appropriate operational security posture is implemented and maintained.

5. This appointment will remain in effect from the date noted above until rescinded in writing, the ISSM is found not competent, or the individual is replaced.

The point of contact for this action is the Facility Security Officer (FSO), [INSERT NAME], at [INSERT PHONE NUMBER and EMAIL].

_____

FIRSTNAME LASTNAME Signature Date

FSO/another Key Management Personnel (KMP) or Program Manager

ISSM Acceptance of Appointment Requirements

_____

FIRSTNAME LASTNAME Signature Date

APPENDIX F: HARDWARE LIST

HARDWARE LIST

Device/System Name	Type	Manufacturer/Model	Serial Number	Memory/Media Size & Type	Clearing/Destruction Procedure
e.g. Desktop #1	PC	Dell OptiPlex 755	1HS36H1		
e.g. Desktop #2	PC	Dell OptiPlex 755	1HS36K6		
e.g. Printer	Color	HP 8500	KLH2315		

- Provide a unique identifier (e.g., serial number, barcode) for any device that retains classified information when all power is removed.
- List the size/capacity of any memory or media that retains classified information when all power is removed.
- If the device has all volatile memory, specify Power Off in this column. If more lengthy sanitization or write-protection methods are used, reference the artifact that includes the sanitization or write-protection procedures.

Note: The Hardware List must include all security relevant hardware.

APPENDIX G: SOFTWARE LIST

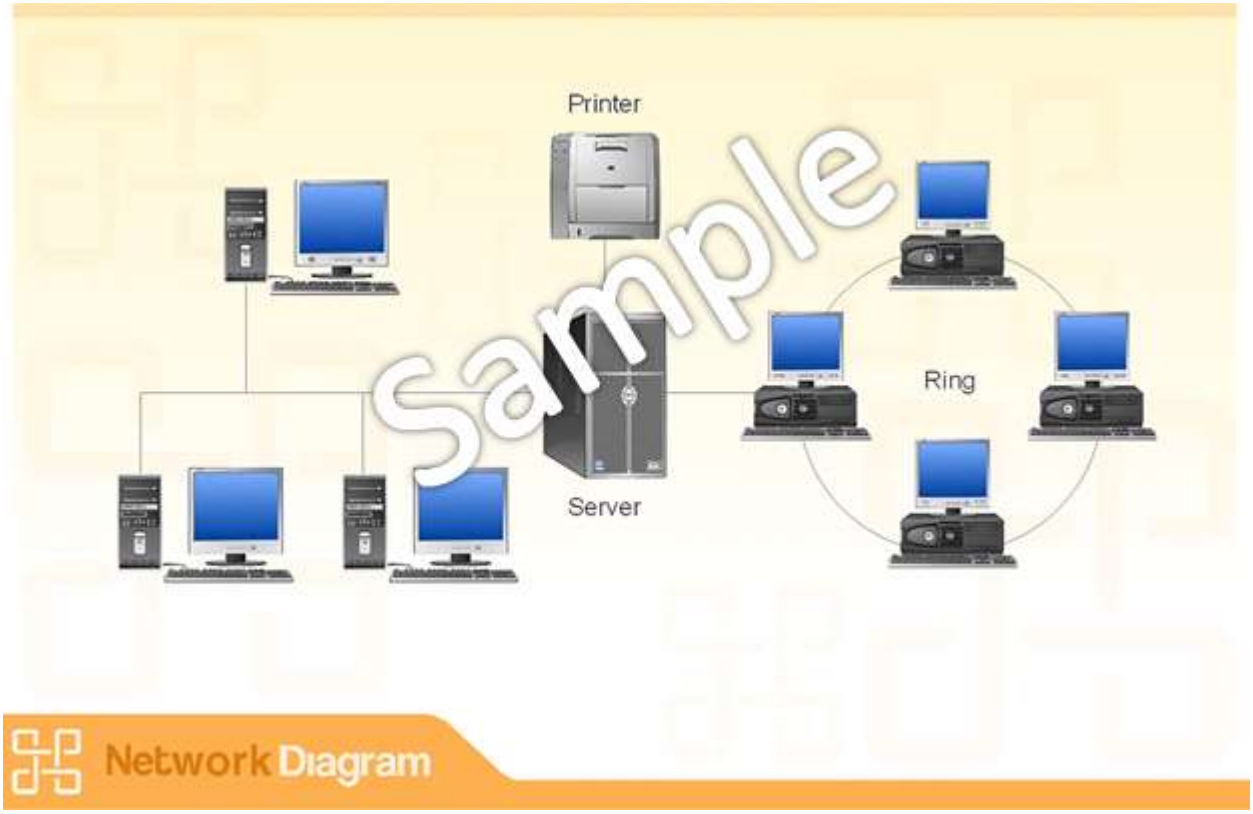
SOFTWARE LIST

Manufacturer	Software Name	Version	Purpose
e.g. Microsoft	Windows	10	O/S
e.g. Symantec	Endpoint Protection 14	14.2.1031.0100	Antivirus, malicious code, endpoint protection
e.g. Adobe	Reader	11.0	Office automation

Note: The Software List must include all security relevant software. Reference Appendix A, CM-3 DCSA Supplemental Guidance.

APPENDIX H: SYSTEM DIAGRAM/NETWORK TOPOLOGY

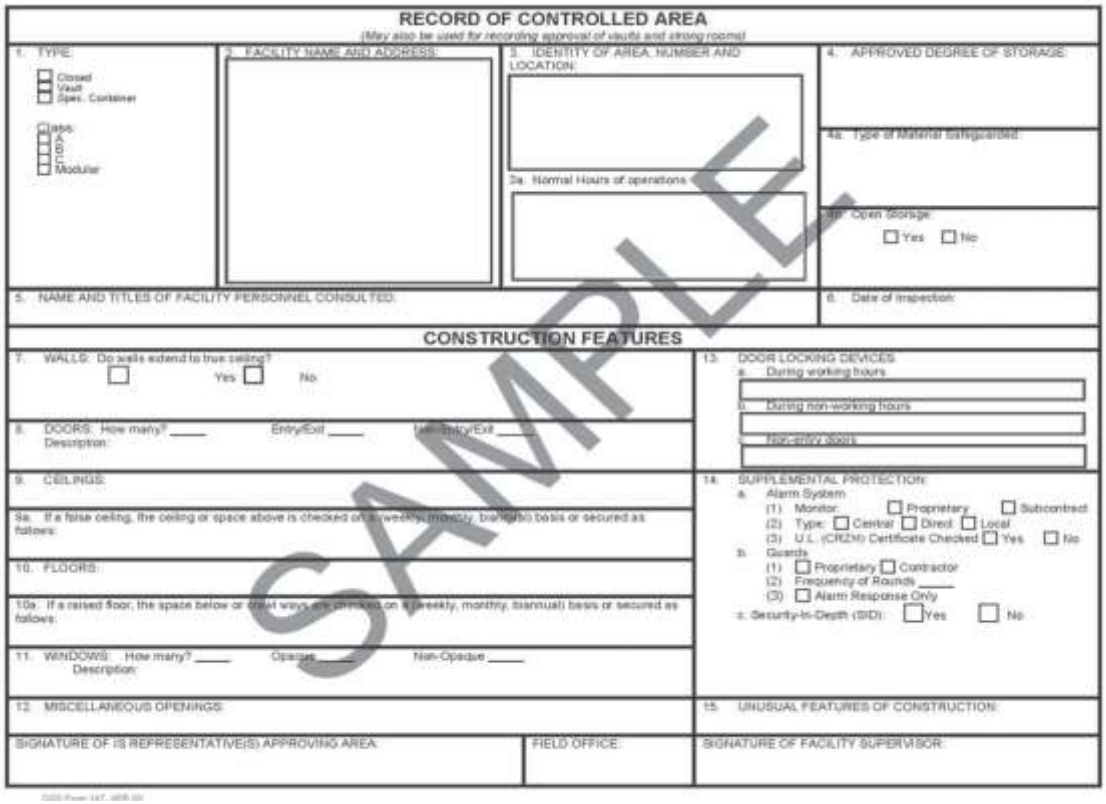
SYSTEM DIAGRAM/NETWORK TOPOLOGY



Note: A system diagram/network topology must be provided for the system (e.g., data flows, storage, workstations, etc.).

APPENDIX I: RECORD OF CONTROLLED AREA

RECORD OF CONTROLLED AREA (DSS FORM 147, APR 00)



RECORD OF CONTROLLED AREA

(May also be used for recording approval of vaults and strong rooms)

1. TYPE:
- Closed
- Vault
- Spec. Container
- Class:
- Open
- Modular

2. FACILITY NAME AND ADDRESS:

3. IDENTITY OF AREA, NUMBER AND LOCATION:

3a. Normal Hours of operations:

4. APPROVED DEGREE OF STORAGE:

4a. Type of Material Safeguarded:

4b. Open Storage: ☐ Yes ☐ No

5. NAME AND TITLES OF FACILITY PERSONNEL CONSULTED:

6. Date of Inspection:

CONSTRUCTION FEATURES

7. WALLS: Do walls extend to true ceiling? ☐ Yes ☐ No

8. DOORS: How many? ____ Entry/Exit ____ Non-Entry/Exit ____ Description:

9. CEILINGS:

9a. If a false ceiling, the ceiling or space above is checked on a (weekly, monthly, biannual) basis or secured as follows:

10. FLOORS:

10a. If a raised floor, the space below or crawl ways are checked on a (weekly, monthly, biannual) basis or secured as follows:

11. WINDOWS: How many? ____ Opaque ____ Non-Opaque ____ Description:

12. MISCELLANEOUS OPENINGS:

13. DOOR LOCKING DEVICES:
a. During working hours:
b. During non-working hours:
c. Non-entry doors:

14. SUPPLEMENTAL PROTECTION:
a. Alarm System
(1) Monitor: ☐ Proprietary ☐ Subcontract
(2) Type: ☐ Central ☐ Direct ☐ Local
(3) U.L. (CRZH) Certificate Checked ☐ Yes ☐ No
b. Guards
(1) ☐ Proprietary ☐ Contractor
(2) Frequency of Rounds ____
(3) ☐ Alarm Response Only
c. Security-In-Depth (SID): ☐ Yes ☐ No

15. UNUSUAL FEATURES OF CONSTRUCTION:

SIGNATURE OF IS REPRESENTATIVE(S) APPROVING AREA:

FIELD OFFICE:

SIGNATURE OF FACILITY SUPERVISOR:

SAMPLE

Note: A Form 147 is not required for a Restricted Area.

APPENDIX J: INFORMATION SYSTEM ACCESS AUTHORIZATION AND BRIEFING FORM

<SYSTEM NAME>

INFORMATION SYSTEM ACCESS AUTHORIZATION AND BRIEFING FORM

Printed Name: _____ Phone: _____

I have the necessary clearance for access to the following classified system: <SYSTEM NAME>. As a system user, I understand that it is my responsibility to comply with all security measures necessary to prevent any unauthorized disclosure, modification, or destruction of information. I am responsible for all actions taken under my account. I will not attempt to "hack" the system or any connected systems, or gain access to data to which I do not have authorized access. I have read or will read all portions of the security plan pertaining to my level of responsibilities and agree to the following:

1. Protect and safeguard all information in accordance with the security plan.
2. Fulfill the responsibilities detailed in the Defense Counterintelligence and Security Agency Assessment and Authorization Process Manual (General User – Section 3.10).
3. Protect all media used and generated on the system by properly classifying, labeling, controlling, transmitting and destroying it in accordance with security requirements and security classification guide.
4. Protect all data viewed on the screens and/or outputs produced at the level of system processing until it has been reviewed.
5. Process only data that pertains to official business and is authorized to be processed on the system.
6. Use the system for performing assigned duties, never personal business.
7. Report all security incidents or suspected incidents to the Information System Security Manager (ISSM) or designee. This includes any indication of intrusion, unexplained degradation or interruption of services, or the actual or possible compromise of data or file access controls.
8. Discontinue use of any system resources that show signs of being infected by a virus or other malware and report the suspected incident.
9. Challenge unauthorized personnel that appear in work area.
10. Ensure that access is assigned based on ISSM and Information System Owner (ISO) approval.
11. Notify the ISSM if access to system resources is beyond that which is required to perform your job.
12. Attend user security and awareness training annually and/or as required by the ISSM.
13. Coordinate user access requirements, and user access parameters, with ISSM and ISO.
14. Safeguard resources against waste, loss, abuse, unauthorized users, and misappropriation.
15. Sign all logs, forms and receipts as required.

16. Obtain permission from the ISSM or designee prior to adding/removing/reconfiguring/ or modifying any system hardware or software.
17. Comply with all software copyright laws and licensing agreements.
18. Ensure all files and media are checked for viruses and malicious logic using a current virus detection tool prior to, or at the time of introduction to a system.
19. Prevent non-authorized personnel from accessing the system and/or data.
20. Notify the ISSM or designee when access the system is no longer needed (i.e., transfer, termination, leave of absence, or for any period of extended non-use).
21. Only perform data transfers if authorized by the ISSM. If authorized, Data Transfer Agent (DTA) appointment letter and training will be executed. In addition, all data transfers will be performed in accordance with authorized procedures.
22. Follow guidelines regarding the explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.
23. Comply with the following password requirements:
    a. Protect system passwords commensurate with the level of information processed on the system and never disclose to any unauthorized persons.
    b. Report suspected misuse or compromise of a password to the ISSM or designee.
    c. Report discovery of unauthorized use, possession, or downloading of a password-cracking tool to the ISSM or designee.
    d. Select a password that is a minimum of 14 non-blank characters. The password will contain a string of characters that does not include the user's account name or full name. The password includes one or more characters from at least 3 of the following 4 classes: Uppercase, lowercase, numerical, and special characters.
    e. If access is granted to a Generic/Group account, document actions in a manual log (or other approved method) to ensure individual user accountability.

I understand that all of my activities on the system are subject to monitoring and/or audit. Failure to comply with the above requirement will be reported and may result in revocation of system access, counseling, disciplinary action, discharge or loss of employment, and/or revocation of security clearance.

_____ _____

User Signature Date

FOR SECURITY AND ADMINISTRATOR USE ONLY

☐ Employee ☐ Visitor / Company: _____

Visit request expires on: _____

Clearance/ Special Briefings: _____

Verified By: _____

Account Name: _____ Date Added: _____

Other, Access/Privileges, or Comments: _____

_____ _____

ISSM or designee Signature Date

Note: The Information System Access Authorization and Briefing Form is a template. Industry should modify the template to comply with contractual requirements and include specific Rules of Behavior that are necessary to secure the system.

APPENDIX K: INFORMATION SYSTEM PRIVILEGED ACCESS AUTHORIZATION AND BRIEFING FORM

<SYSTEM NAME>

INFORMATION SYSTEM PRIVILEGED ACCESS AUTHORIZATION AND BRIEFING FORM

Printed Name: _____ Phone: _____

I have the necessary clearance for PRIVILEGED access to the following classified system: <SYSTEM NAME>. As a privileged user, I understand that it is my responsibility to comply with all security measures necessary to prevent any unauthorized disclosure, modification, or destruction of information. I am responsible for all actions taken under my account. I will not attempt to "hack" the system or any connected systems, or gain access to data to which I do not have authorized access. I have read or will read all portions of the security plan pertaining to my level of responsibilities and agree to the following:

1. Protect and safeguard all information in accordance with the security plan.
2. Fulfill the responsibilities detailed in the Defense Counterintelligence and Security Agency Assessment and Authorization Process Manual (Privileged User – Section 3.9).
3. Protect all media used and generated on the system by properly classifying, labeling, controlling, transmitting and destroying it in accordance with security requirements and security classification guide.
4. Protect all data viewed on the screens and/or outputs produced at the level of system processing until it has been reviewed.
5. Process only data that pertains to official business and is authorized to be processed on the system.
6. Use the system for performing assigned duties, never personal business.
7. Report all security incidents or suspected incidents to the Information System Security Manager (ISSM) or designee. This includes any indication of intrusion, unexplained degradation or interruption of services, or the actual or possible compromise of data or file access controls.
8. Discontinue use of any system resources that show signs of being infected by a virus or other malware and report the suspected incident.
9. Challenge unauthorized personnel that appear in work area.
10. Ensure that access is assigned based on ISSM and Information System Owner (ISO) approval.
11. Notify the ISSM if access to system resources is beyond that which is required to perform your job.
12. Attend user security and awareness training annually and/or as required by the ISSM.
13. Coordinate user access requirements, and user access parameters, with ISSM and ISO.
14. Safeguard resources against waste, loss, abuse, unauthorized users, and misappropriation.
15. Sign all logs, forms and receipts as required.

16. Obtain permission from the ISSM or designee prior to adding/removing/reconfiguring/ or modifying any system hardware or software.
17. Comply with all software copyright laws and licensing agreements.
18. Ensure all files and media are checked for viruses and malicious logic using a current virus detection tool prior to, or at the time of introduction to a system.
19. Prevent non-authorized personnel from accessing the system and/or data.
20. Notify the ISSM or designee when access the system is no longer needed (i.e., transfer, termination, leave of absence, or for any period of extended non-use).
21. Only perform data transfers if authorized by the ISSM. If authorized, Data Transfer Agent (DTA) appointment letter and training will be executed. In addition, all data transfers will be performed in accordance with authorized procedures.
22. Follow guidelines regarding the explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.
23. Receive approval and direction from the ISSM or designee prior to adding/removing users to the Domain Administrators, Local Administrator, or Power Users group.
24. Receive approval and/or specific guidance prior to allowing user to access the system.
25. Use the special access or privileges granted to me ONLY to perform authorized tasks or mission related functions only.
26. Comply with the following password requirements:
    a. Protect the root password and/or authenticators at the highest level of data it secures.
    b. NOT share the root password and/or authenticators with individuals who are not authorized access.
    c. Protect system passwords commensurate with the level of information processed on the system and never disclose to any unauthorized persons.
    d. Report suspected misuse or compromise of a password to the ISSM or designee.
    e. Report discovery of unauthorized use, possession, or downloading of a password-cracking tool to the ISSM or designee.
    f. Select a password that is a minimum of 14 non-blank characters for non-privileged accounts and 15 characters in length for privileged accounts. The password will contain a string of characters that does not include the user's account name or full name. The password includes one or more characters from at least 3 of the following 4 classes: Uppercase, lowercase, numerical, and special characters.
    g. If access is granted to a Generic/Group account, document actions in a manual log (or other approved method) to ensure individual user accountability.
27. Use my privileged user account for official administrative actions ONLY.

I understand that all of my activities on the system are subject to monitoring and/or audit. Failure to comply with the above requirement will be reported and may result in revocation of system access, counseling, disciplinary action, discharge or loss of employment, and/or revocation of security clearance.

_____ _____

User Signature Date

FOR SECURITY AND ADMINISTRATOR USE ONLY

☐ Employee ☐ Visitor / Company: _____

Visit request expires on: _____

Clearance/ Special Briefings: _____

Verified By: _____

Account Name: _____ Date Added: _____

Other, Access/Privileges, or Comments: _____

_____ _____

ISSM or designee Signature Date

Note: The Information System Privileged Access Authorization and Briefing Form is a template. Industry should modify the template to comply with contractual requirements and include specific Rules of Behavior that are necessary to secure the system.

APPENDIX L: UPGRADE/DOWNGRADE PROCEDURE RECORD

UPGRADE/DOWNGRADE PROCEDURE RECORD

	UPGRADE Procedures: 1. Clear area of unauthorized persons and verify classified processing sign is posted. 2. Obtain classified media from approved storage. 3. Inspect Security Seals. 4. Install classified drives. 5. Boot system. 6. Document upgrade action.			DOWNGRADE Procedures: 1. Verify classified material has been removed from printers. 2. Verify classified hard drives and media are removed and properly stored. 3. Shutdown/power down system for 30 seconds. 4. Document downgrade action.		
Component or System#	Date	Time	Person	Date	Time	Person

Note: The Upgrade/Downgrade Procedure Record is a template. Industry should modify the template to comply with any additional and/or contractual requirements necessary to secure the system.

APPENDIX M: SECURITY SEAL LOG

SECURITY SEAL LOG

Seal No.	Date Seal Applied	Seal Location	Name/Signature of Person Applying Seal	Date Seal Broken	Signature of Person Breaking Seal	Reason for Seal Breaking

Note: If applicable, the Security Seal Log template can be used to capture tamper seal records. Approved tamper-proof, pre-numbered seals should be used on hardware components anytime the hardware may be subject to access by uncleared personnel (e.g., used for periods-processing, in restricted areas, mobile systems, printers or relocation).

APPENDIX N: MAINTENANCE, OPERATING SYSTEM, & SECURITY SOFTWARE CHANGE LOG

MAINTENANCE, OPERATING SYSTEM & SECURITY SOFTWARE CHANGE LOG

Date	System Device Description	Component ID Number	Description of Actions	Person (Company if applicable)	PCL	Escort

Note: All entries must include date, description of action, and person taking action. Company of person performing action is only required if they are not an employee. Escort is only listed when the performing person does not have the requisite clearances and/or Need-to-Know. Personnel Security Clearance (PCL) must be included for entries involving changes to hardware or software. Hardware changes must include system/device description, ID number, and clear/sanitize actions if applicable.

The Maintenance, Operating System & Security Software Change Log is a template. Industry should modify the template to comply with any additional and/or contractual requirements necessary to secure the system.

APPENDIX O: DATA TRANSFER PROCEDURES

Data Transfers

There are three types of data transfers:

a. **Low-to-High** – A transfer from a lower classification system to a higher classification system (e.g., anti-virus updates, patching, install/update software, etc.)

b. **High-to-High** – A transfer between systems of the same classification.

c. **High-to-Low** – A transfer from a higher classification system to a lower classification system. A High-to-Low data transfer is also defined as an **Assured File Transfer (AFT)**.

All data transfers require a Data Transfer Agent (DTA). DTAs must be appropriately trained and appointed in writing. The number of DTAs should be kept to a minimum.

All data transfers must be tracked to include date, originator making request, filename, file format type, classification level, source, destination systems, number of copies created, and DTA performing the transfer. All data transfers can be maintained in one log, as long as the type of data transfer is clearly annotated.

High-to-Low data transfers also require Two Person Integrity (TPI). TPI requires that all actions involve the presence of two authorized individuals. Therefore, two authorized individuals must be physically present during the entire data transfer process. When logging these types of transfers, both the DTA performing the transfer and individual verifying the transfer must be tracked.

Note: The Information Owner (IO) may leverage additional requirements for data transfers and putting classified information on removable media. In these instances, Industry must follow the IO supplementary requirements.

Low-to-High and High-to-High transfers require:

a. Logging transfers (e.g., Secret to Top Secret, Unclassified to Secret, Secret (Program A) to Secret (Program B), etc.).

b. 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.

c. Testing of the write-protect mechanism. Once media is introduced, 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:

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

b. AO approval for use of automated tools or a manual transfer process/checklist, to include any IO requirements.

c. 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.

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

Defense Counterintelligence and Security Agency (DCSA) AFT (High-To-Low) Procedures

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.

For every file type or format, there are countless unique transfer procedures developed by industry and government. DCSA 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:

a. The file types/formats and transfer procedures must be authorized by DCSA and documented in the security plan.

b. Target media must be factory fresh.

c. All media must be scanned for viruses with the latest definitions prior to starting an AFT.

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

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

f. The compilation of all files on the target media does not cause an increased classification level due to aggregation.

g. Files are transferred using a known, authorized utility or command.

h. Target media is verified to contain only intended source files.

i. Files are verified on target media to contain the correct sensitivity of information and/or level of unclassified or lower classified information.

j. The target media displays the appropriate security classification label.

k. An administrative record of the transfer is created and maintained.

If the ISSM is unable to implement the DCSA File/Type Formats and Authorized Procedures, the security plan must include a description of the file format and/or procedure used. In addition to AO approval, a rigorous review is required prior to granting exceptions to the use of DCSA Authorized File Type/Formats and/or Procedures.

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.

DCSA 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

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

DCSA AFT (High-to-Low) Procedures (Windows-Based)

a. The target media must be factory fresh.

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

c. 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).

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

e. As a general rule, files should be converted to one of the acceptable formats first DCSA 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. 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. For embedded objects, such as a graph created from an excel file, right click the worksheet object and select Edit Data. 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 DCSA-authorized formats from the drop-down menu of Save As Type.

f. 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.

g. 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. 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:

- 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.

- 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.

- 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.

- 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. If a document has multiple Sections, each Section may have different headers and footers.

- 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.

- 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.

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

- 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 DCSA-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.

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

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

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

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

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

m. 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.

DCSA AFT (High-to-Low) Procedures (Unix-Based)

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.

a. The target media must be factory fresh.

b. The procedure must be performed by a DTA.

c. 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).

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

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

f. 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.

   - 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.

   - 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.

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

   - Compressed archives should be reviewed and transferred uncompressed.

g. 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):

h. mt -f /dev/rst0 rew.

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

j. tar cvf /dev/rst0 /directory_name.

k. Create Tar file on tape.

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

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

   - mt -f /dev/rst0 rew.
   - Ensure tape is rewound (not required for floppy) tar tvf /dev/rst0 | lpr.
   - Print directory of file (| lpr may be omitted for on-screen review).

n. 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).

o. 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.

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

q. 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 System Name(s)/Contract(s):

Manager Request	
I request the above named individual be authorized to perform Data Transfers. 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 a Data Transfer and the mechanisms associated with the 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 Data Transfer Procedures.	
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 system. Additionally, he/she has demonstrated extensive knowledge of all appropriate security classification guides and authorized procedures associated with the information downloaded.	
Authorized AFT File Formats: ASCII/Text, HTM/HTML, JPEG, BMP, GIF Specify:	
Printed Name:	
Signature:	Date:

Note: The Data Transfer Agent (DTA) Authorization Form is a template. Industry should modify the template to comply with any additional and/or contractual requirements.

APPENDIX P: CONTINGENCY PLAN TEMPLATE

CONTINGENCY PLAN

Introduction

The <Program Name> < System Name> Contingency Plan (CP), documents the strategies, personnel, procedures, and resources required to respond to any short or long term interruption to the system.

Scope

This CP has been developed for <System Name> which is classified as a <moderate-low-low> impact system for the three security objectives: confidentiality, integrity, and availability. The procedures in this CP have been developed for a moderate-low-low impact system and are designed to recover the <System Name> within <Recovery Time Objective (RTO)> hours. The replacement or purchase of new equipment, short-term disruptions lasting less than <RTO> hours, or loss of data at the primary facility or at the user-desktop levels is outside the scope of this plan.

Note: *RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources and supported mission/business processes.*

Assumptions

Instruction*: A list of default assumptions are listed in this section.* ***The assumptions must be edited, revised, and added to so that they accurately characterize the system described in this plan.***

The following assumptions have been made about the <System Name>:

- The Uninterruptable Power Supply (UPS) will keep the system up and running for <total number of seconds/minutes>.
- The generators will initiate after <total number of seconds/minutes> from time of a power failure.
- Current backups of the application software and data are intact and available at the offsite storage facility in <City, State>.
- The <System Name> is inoperable if it cannot be recovered within <RTO hours>.
- Key personnel have been identified and are trained annually in their roles.
- Key personnel are available to activate the CP.

Roles and Responsibilities

The <System Name> roles and responsibilities for various task assignments and deliverables throughout the contingency planning process are depicted in the table below.

Table 1: Roles and Responsibilities

Roles	Responsibilities
INFORMATION SYSTEM OWNER/PROGRAM MANAGER (ISO/PM) – Disruption Occurs	The responsibilities of the ISO/PM when a disruption occurs are listed but not limited to the following: <enter responsibilities>
SYSTEM ADMINISTRATOR (SA)	The responsibilities of the SA are listed but not limited to the following: <enter responsibilities>
PROGRAM SECURTY OFFICER (PSO)	The responsibilities of the PSO are listed but not limited to the following: <enter responsibilities>
INFORMATION SYSTEM SECURITY MANAGER/INFORMATION SYSTEM SECURITY OFFICER (ISSM/ISSO)	The responsibilities of the ISSM/ISSO are listed but not limited to the following: <enter responsibilities>

System Description and Architecture

Instruction: *It is necessary to include a general description of the system covered in the CP. The description should include the Information Technology (IT) system architecture, locations, and any other important technical considerations.*

Provide a general description of system architecture and functionality. Indicate the operating environment, physical location, general location of users, and partnerships with external organizations/systems. Include information regarding any other technical considerations that are important for recovery purposes, such as backup procedures. Provide a diagram of the architecture, including security controls and telecommunications connections.

Contingency Plan Phases

This plan has been developed to recover and reconstitute the <System Name> using a three-phased approach. The approach ensures that system recovery and reconstitution efforts are performed in a methodical sequence to maximize the effectiveness of the recovery and reconstitution efforts and minimize system outage time due to errors and omissions. The three system recovery phases consist of activation and notification, recovery, and reconstitution.

1. **Activation and Notification Phase:** Activation of the CP occurs after a disruption, outage, or disaster that may reasonably extend beyond the RTO established for a system. The outage event may result in severe damage to the facility that houses the system, severe damage or loss of equipment, or other damage that typically results in long-term loss.

   Once the CP is activated, the system stakeholders are notified of a possible long-term outage, and a thorough outage assessment is performed for the system. Information from the outage

assessment is analyzed and may be used to modify recovery procedures specific to the cause of the outage.

2. Recovery Phase: The Recovery phase details the activities and procedures for recovery of the affected system. Activities and procedures are written at a level such that an appropriately skilled technician can recover the system without intimate system knowledge. This phase includes notification and awareness escalation procedures for communication of recovery status to system stakeholders.

3. Reconstitution: The Reconstitution phase defines the actions taken to test and validate system capability and functionality at the original or new permanent location. This phase consists of two major activities: validating data and operational functionality followed by deactivation of the plan.

   During validation, the system is tested and validated as operational prior to returning operation to its normal state. Validation procedures include functionality or regression testing, concurrent processing, and/or data validation. The system is declared recovered and operational by upon successful completion of validation testing.

   Deactivation includes activities to notify users of system operational status. This phase also addresses recovery effort documentation, activity log finalization, incorporation of lessons learned into plan updates, and readying resources for any future events.

Data Backup Readiness Information

The hardware and software components used to create the <System Name> backups are noted in Table 2.

Table 2: Backup System Components

System/Components	Description
Software Used	
Hardware Used	
Date of Last Backup	
Backup Type (Full, Differential, Incremental)	

Alternate Site/Backup Storage Information

Alternate facilities have been established for backup storage and/or restoration of the <System Name> as noted in Table 3. Current backups of the system configuration, software and data are intact and available at the alternate storage facility.

Table 3: Primary and Alternate Site Locations

Designation	Site Name	Site Type (Hot, Cold, Warm, Mirrored)	Address
Primary Site			
Alternate Site			
Alternate Site			

Activation and Notification

The activation and notification phase defines initial actions taken once a disruption has been detected or appears to be imminent. The RTO defines the maximum amount of time that the information system can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes, and the maximum tolerable downtime. Determining the information system resource RTO is important for selecting appropriate technologies that are best suited for meeting the maximum tolerable downtime. This phase includes activities to notify recovery personnel, conduct an outage assessment, and activate the CP. At the completion of the Activation and Notification Phase, key CP staff will be prepared to perform recovery measures to restore system functions.

Activation Criteria

The CP may be activated if one or more of the following criteria are met:

- The type of outage indicates <System Name> will be down for more than <RTO hours>
- The facility housing <System Name> is damaged and may not be available within <RTO hours>
- Other criteria, as appropriate

Recovery

The recovery phase provides formal recovery operations that begin after the CP has been activated, outage assessments have been completed (if possible), personnel have been notified, and appropriate individuals have been mobilized. Recovery phase activities focus on implementing recovery strategies to restore system capabilities, repair damage, and resume operational capabilities at the original or an alternate location. At the completion of the recovery phase, <System Name> will be functional and capable of performing essential functions.

Sequence of Recovery Operations

Instruction: *Modify the following list as appropriate for the system recovery strategy.*

The following activities occur during recovery of <System Name>:

- Identify recovery location (if not at original location)
- Identify required resources to perform recovery procedures

- Retrieve backup and system installation media
- Recover hardware and operating system (if required)
- Recover system from backup and system installation media
- Implement transaction recovery for systems that are transaction-based

Recovery Procedures

Instruction: *Provide general procedures for the recovery of the system from backup media. Specific keystroke-level procedures may be provided in an appendix. If specific procedures are provided in an appendix, a reference to that appendix should be included in this section. Teams or persons responsible for each procedure should be identified.*

The following procedures are provided for recovery of <System Name> at the original or established alternate location. Recovery procedures should be executed in the sequence presented to maintain an efficient recovery effort.

Instruction: *Describe recovery procedures.*

Reconstitution

Reconstitution is the process by which recovery activities are completed and normal system operations are resumed. If the original facility is unrecoverable, the activities in this phase can also be applied to preparing a new permanent location to support system processing requirements. A determination must be made on whether the system has undergone significant change and will require reassessment and reauthorization. The phase consists of two major activities: validating successful reconstitution and deactivation of the plan.

Concurrent processing is the process of running a system at two separate locations concurrently until there is a level of assurance that the recovered system is operating correctly and securely.

Data Validation Testing

Instruction: *Describe procedures for testing and validation of data to ensure that data is correct and up to date as of the last available backup. Teams or persons responsible for each procedure should be identified. An example of a validation data test for a moderate-impact system would be to compare a database audit log to the recovered database to make sure all transactions were properly updated.*

Validation data testing is the process of testing and validating data to ensure that data files or databases have been recovered completely at the permanent location.

Functional Validation Testing

Instruction: *Describe procedures for testing and validation functional and operational aspects of the system.*

Functionality testing is a process for verifying that all system functionality has been tested, and the system is ready to return to normal operations.

Recovery Declaration

Upon successfully completing testing and validation, the <role name> will formally declare recovery efforts complete, and that <System Name> is in normal operations. <System Name> users and technical POCs will be notified of the declaration by the <role name>. The recovery declaration statement notifies the stakeholders and management that the <System Name> has returned to normal operations.

Post Reconstitution

Cleanup

Instruction: *Describe cleanup procedures and tasks including cleanup roles and responsibilities. Insert cleanup responsibilities in Table 4. Add additional rows as needed.*

Cleanup is the process of cleaning up or dismantling any temporary recovery locations, restocking supplies used, returning manuals or other documentation to their original locations, and readying the system for a possible future contingency event.

Table 4: Primary Cleanup Roles and Responsibilities

Roles	Cleanup Responsibilities

Backup Procedures

Instruction: *Provide procedures for returning retrieved backup or installation media to its offsite data storage location. This may include proper logging and packaging of backup and installation media, preparing for transportation, and validating that media is securely stored at the offsite location.*

It is important that all backup and installation media used during recovery be returned to the offsite data storage location. The following procedures should be followed to return backup and installation media to its offsite data storage location:

<Enter procedures>

Instruction: *Provide appropriate procedures for ensuring that a full system backup is conducted within a reasonable time frame, ideally at the next scheduled backup period.*

As soon as reasonable following recovery, the system should be fully backed up and a new copy of the current operational system stored for future recovery efforts. This full backup is then kept with other system backups. The procedures for conducting a full system backup are:

<Enter procedures>

After Action Reporting

It is important that all recovery events be well-documented, including actions taken and problems encountered during the recovery and reconstitution effort. Information on lessons learned should be included in the annual update to the CP. It is the responsibility of each CP team or person to document their actions during the recovery event.

Contingency Plan Testing

Contingency Plan operational tests of the <System Name> are performed **at least annually**. A Contingency Plan Test (CPT) report is documented after each annual test.

Instruction: *Describe the procedures for the annual contingency plan testing. Include a description of the required test environment. Operational tests typically include the following:*

1. *Restore files from backup tapes.*
2. *Verify that backup tapes are stored at designated off-site locations.*
3. *Determine whether data stored on backup tapes is valid and retrievable.*
4. *Perform failover testing.*
5. *Test the UPS to ensure that it operates correctly in the event of a power disruption;*
6. *Test the offsite backup vendor's delivery response timeliness of media during normal daytime hours and during nighttime hours*
7. *Test to ensure that offsite storage vendor only supplies backup tapes to authorized individuals*
8. *Test the generators to ensure that they turn on automatically*
9. *Perform tabletop exercises to test various possible contingency situations*
10. *Perform call tree exercises to ensure that employees can be reached in a timely manner.*

Instruction: *Describe methods used to test CP in this section.*

Contingency Plan Testing Report Template

Instruction: *This section should include a summary of the last Contingency Plan Test.*

Table 5: Contingency Plan Test Summary

Test Information	Description
Name of Test	
System Name	
Date of Test	
Team Test Lead and Point of Contact	
Location Where Conducted	
Participants	
Components	
Assumptions	
Objectives	Assess effectiveness of system recovery at alternate site Assess effectiveness of coordination among recovery teams Assess systems functionality using alternate equipment Assess performance of alternate equipment Assess effectiveness of procedures Assess effectiveness of notification procedures
Methodology	
Activities and Results (Action, Expected Results, Actual Results)	
Post Test Action Items	
Lessons Learned and Analysis of Test	
Recommended Changes to Contingency Plan Based on Test Outcomes	

Note: The Contingency Plan Template is intended as a guideline. Industry will need to adjust the Contingency Plan to meet their specific requirements and comply with any additional and/or contractual requirements.

APPENDIX Q: INCIDENT RESPONSE PLAN TEMPLATE

INCIDENT RESPONSE PLAN

Introduction

The <Program Name> <System Name> Incident Response Plan (IRP) documents the strategies, personnel, procedures, and resources required to respond to any incident affecting the system.

Scope

This IRP has been developed for <System Name> which is classified as a <moderate-low-low> impact system for the three security objectives: confidentiality, integrity, and availability.

Roles and Responsibilities

The <System Name> roles and responsibilities for various task assignments and deliverables throughout the incident response process are depicted in the table below.

Table 1: Roles and Responsibilities

Roles	Responsibilities
INFORMATION SYSTEM OWNER/PROGRAM MANAGER (ISO/PM) – Incident Occurs	The responsibilities of the ISO/PM when an incident occurs are listed but not limited to the following: <enter responsibilities>
SYSTEM ADMINISTRATOR (SA)	The responsibilities of the SA are listed but not limited to the following: <enter responsibilities>
PROGRAM SECURTY OFFICER (PSO)	The responsibilities of the PSO are listed but not limited to the following: <enter responsibilities>
INFORMATION SYSTEM SECURITY MANAGER/INFORMATION SYSTEM SECURITY OFFICER (ISSM/ISSO)	The responsibilities of the ISSM/ISSO are listed but not limited to the following: <enter responsibilities>

Definitions

Event

An event is an occurrence not yet assessed that may affect the performance of an information system and/or network. Examples of events include an unplanned system reboot, a system crash, and packet flooding within a network. Events sometimes provide indication that an incident is occurring or has occurred.

Incident

An incident is an assessed occurrence having potential or actual adverse effects on the information system. A security incident is an incident or series of incidents that violate the security policy. Security

incidents include penetration of computer systems, spillages, exploitation of technical or administrative vulnerabilities, and introduction of computer viruses or other forms of malicious code.

Types of Incidents

The term "incident" encompasses the following general categories of adverse events:

Data Destruction or Corruption**:** The loss of data integrity can take many forms including changing permissions on files so that they are writable by non-privileged users, deleting data files and or programs, changing audit files to cover-up an intrusion, changing configuration files that determine how and what data is stored and ingesting information from other sources that may be corrupt.

Data Compromise and Data Spills**:** Data compromise is the exposure of information to a person not authorized to access that information either through clearance level or formal authorization. This could happen when a person accesses a system he is not authorized to access or through a data spill. Data spill is the release of information to another system or person not authorized to access that information, even though the person is authorized to access the system on which the data was released. This can occur through the loss of control, improper storage, improper classification, or improper escorting of media, computer equipment (with memory), and computer generated output.

Malicious Code**:** Malicious code attacks include attacks by programs such as viruses, Trojan horse programs, worms, and scripts used by crackers/hackers to gain privileges, capture passwords, and/or modify audit logs to exclude unauthorized activity. Malicious code is particularly troublesome in that it is typically written to masquerade its presence and, thus, is often difficult to detect. Self-replicating malicious code such as viruses and worms can replicate rapidly, thereby making containment an especially difficult problem.

Virus Attack: A virus is a variation of a Trojan horse. It is propagated via a triggering mechanism (e.g., event time) with a mission (e.g., delete files, corrupt data, send data). Often self-replicating, the malicious program segment may be stand-alone or may attach itself to an application program or other executable system component in an attempt to leave no obvious signs of its presence.

Worm Attack: A computer worm is an unwanted, self-replicating autonomous process (or set of processes) that penetrates computers using automated hacking techniques. A worm spreads using communication channels between hosts. It is an independent program that replicates from machine to machine across network connections often clogging networks and computer systems.

Trojan Horse Attack: A Trojan horse is a useful and innocent program containing additional hidden code that allows unauthorized Computer Network Exploitation (CNE), falsification, or destruction of data.

System Contamination: Contamination is defined as inappropriate introduction of data into a system not approved for the subject data (i.e., data of a higher classification or of an unauthorized formal category).

Privileged User Misuse: Privileged user misuse occurs when a trusted user or operator attempts to damage the system or compromise the information it contains.

Security Support Structure Configuration Modification: Software, hardware and system configurations contributing to the Security Support Structure (SSS) are controlled since they are essential to maintaining

the security policies of the system. Unauthorized modifications to these configurations can increase the risk to the system.

Note: *These categories of incidents are not necessarily mutually exclusive.*

Incident Response

<Program Name> shall follow the incident response and reporting procedures specified in the security plan. Upon learning of an incident or a data spillage, the ISSM will take immediate steps intended to minimize further damage and/or regain custody of the information, material or mitigate damage to program security.

Instruction: *Provide an overview of your facility's incident response and reporting procedures.*

Incident response will follow the following six steps:

1. Preparation – one of the most important facilities to a response plan is to know how to use it once it is in place. Knowing how to respond to an incident BEFORE it occurs can save valuable time and effort in the long run.

2. Identification – identify whether or not an incident has occurred. If one has occurred, the response team can take the appropriate actions.

3. Containment – involves limiting the scope and magnitude of an incident. Because so many incidents observed currently involve malicious code, incidents can spread rapidly. This can cause massive destruction and loss of information. As soon as an incident is recognized, immediately begin working on containment.

4. Eradication – removing the cause of the incident can be a difficult process. It can involve virus removal, conviction of perpetrators, or dismissing employees.

5. Recovery – restoring a system to its normal business status is essential. Once a restore has been performed, it is also important to verify that the restore operation was successful and that the system is back to its normal condition.

6. Follow-up – some incidents require considerable time and effort. It is little wonder, then, that once the incident appears to be terminated there is little interest in devoting any more effort to the incident. Performing follow-up activity is, however, one of the most critical activities in the response procedure. This follow- up can support any efforts to prosecute those who have broken the law. This includes changing any company policies that may need to be narrowed down or be changed altogether.

Incident Response Training

All Program personnel will receive incident response training at least annually and a record of the training will be maintained. This training can be integrated into the overall program specific annual security awareness training.

Table 2: Roles Incident Response Worksheet

SECURITY INCIDENT REPORT SECTION 1 – POC Information			
Report Classification:			
Report No.:		Report Organization:	
Report Date:		Report Type (initial, final, status):	
Report Generated By:		Date:	Time:
Title:	Telephone:	E-mail:	
Signature:			

SECTION 1 – POC Information			
Incident Reported By:		Date:	Time:
Location:	Telephone:	E-mail:	
Signature:			
PSO/ISSM Notified (Name):		Date:	Time:
Location:	Telephone:	E-mail:	
Signature:			
DCSA Notified (Name):		Date:	Time:
Location:	Telephone:	E-mail:	
Method of Notification:			
IO Notified (Name):		Date:	Time:
Office:	Telephone:	E-mail:	
Method of Notification:			

SECTION 2 – Incident Information		
Incident:	Time of Incident:	Ongoing?
Incident Facility Name:	Incident Facility Location:	
Affected Computer Systems (Hardware and/or Software):		
Classification of Affected Computer Systems:		
Physical Location of Affected Systems:		
Connections of Affected Systems to Other Systems:		
Type of Incident (Data Destruction/Corruption, Data Spill, Malicious Code, Privileged User Misuse, Security Support Structure Configuration Modification, System Contamination, System Destruction/Corruption/Disabling, Unauthorized User Access, other – please identify):		
Suspected Method of Intrusion/Attack:		
Suspected Perpetrators or Possible Motivations:		
Apparent Source (e.g., IP address) of Intrusion/Attack:		
Apparent Target/Goal of Intrusion/Attack:		
Mission Impact:	Success/Failure of Intrusion/Attack:	
Attach technical details of incident thus far. Include as much as possible about the Detection and Identification, Containment, Eradication, and Recovery – steps taken (with date/time stamps), persons involved, files saved for analysis, etc.		

APPENDIX R: CLASSIFIED SPILL CLEANUP PROCEDURES

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)). **When a classified spill occurs, STOP PROCESSING.** Do NOT delete/copy anything and disable all involved user accounts as soon as possible. Notify your assigned Defense Counterintelligence and Security Agency (DCSA) representative immediately.

Coordination

Employees or security managers who report the discovery of classified information on unclassified or lower classified systems are not to delete the classified data, but to isolate the systems and contact the cognizant Facility Security Officer (FSO), Information System Security Manager (ISSM) or Information Sysetms Security Officer (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, mobile devices, 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 backups (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

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).

g. If utilizing cloud services, third party providers, or dynamically allotted storage area networks, ensure procedures or Service Level Agreements (SLAs) align with the authorized security plan.

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 SP 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 CDs and Digital Versatile Disks (DVDs) in optical drives, tapes in tape backup-units, thumb drives/compact flash drives, BIOS passwords, printing devices, and network storage devices. Include relevant documentation when a 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. Mobile computing devices may also contain sensitive information such as passwords or confidential data.

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 media and devices 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 Incident Response Plan:

- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-88 , *Guidelines for Media Sanitization*
- NIST SP 800-61, *Computer Security Incident Handling*
- Committee on National Security Systems Instruction (CNSSI) No. 1001, *National Instruction on Classified Information Spillage*
- Committee on National Security Systems Policy (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

Role	Responsibilities
	• Assess the risks of the contamination and follow any special guidelines of the IO (customer) • Assign appropriately cleared individuals to participate in the cleanup effort
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 security plan. 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. • Report vulnerabilities, cleanup actions, and any other pertinent information to DCSA 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 • Determine if user based local backups contain spill data (e.g., backup of PSTs, local external removable media, etc.) • Investigate possibility of proxy accounts, mobile computing device access, remote access and any other possible “feeds” from the contaminated accounts • Isolate any contaminated assets of the sender/receiver

APPENDIX S: MEDIA SANITIZATION

Media Sanitization

Media sanitization decisions occur throughout the system life cycle. Factors affecting information disposition and media sanitization are decided at the start of a system's development. **The guidance below does not capture all forms of media. Industry must follow guidance provided by the Information Owner (IO).** Please reference additional National Security Agency (NSA) resources on NSA's Media Destruction Guidance website: https://www.nsa.gov/resources/everyone/media-destruction/.

Before storage media is released out of organizational control, becomes obsolete, or is no longer usable or required for a 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 Authorizing Official (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 Information System Security Manager (ISSM) is responsible for the security of all media assigned under his/her purview. To protect these assets, he/she must ensure proper security measures and policies are followed. Additionally, the ISSM, with AO approval, may publish a Standard Operating Procedure (SOP) 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 security plan 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 (EPL). The 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 compact disks (CDs) and digital versatile disks (DVDs). Optical storage devices cannot be sanitized, only destroyed. Refer to NSA/Central Security Service (CSS) Policy Manual 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 EPL for Optical 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. If the drive is to be repurposed, an SSD can be cleared utilizing National Institute of Standards and Technology (NIST) Special Publication (SP) 800-88 procedures for reuse in a collateral environment only. **Utilizing a wiping utility does not suffice in sanitizing solid state drives.** Refer to NSA/CSS Policy Manual 9-12 for detailed procedures related to the destruction (e.g., smelting) of solid state storage devices.

Release of Systems and Components

The ISSM/Information System Security Officer (ISSO), in conjunction with the organization's equipment custodian will develop equipment removal procedures for systems and components. These procedures will be included in the security plan. 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 non-volatile 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 non-volatile, 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.

Non-volatile Memory Components

Components that retain data when all power sources are discontinued are non-volatile memory components. Some non-volatile 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 non-volatile components (e.g., removable/non-removable hard disks) may be released after successful completion of the sanitization procedures as defined in the security plan.

Other Non-volatile 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 (CRT), 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, CRTs 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 a 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/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 security plan. 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					
Electrically Erasable PROM (EEPROM)				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 T: MOBILITY SYSTEM PLAN TEMPLATE

MOBILITY SYSTEM PLAN

For the Movement of a Classified System:

Facility
Address
City, State Zip Code

Date of Mobility System Plan
Revision Number

A. Introduction

This plan outlines the procedures for the transporting of classified system equipment between [Facility] and various sites as listed in the Mobility System Plan (provided as a supporting artifact to the security plan).

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.

Instruction: *Provide a list of equipment.*

C. Identification of Participating Government and Cleared Contractor Representatives

- Facility
- Name of Information System Security Manager (ISSM)
- Address
- Contact information
- Local Defense Counterintelligence and Security Agency (DCSA) Representative
- System Name
- Address
- Contact information

D. Movement

Movement of the equipment will originate from [Facility]. Equipment will be transported to various sites listed in the Mobility System Plan. The Mobility System Plan will include details regarding the site's physical environment. The ISSM will notify the DCSA Representative prior to movement of the system to

or from any off-site location. All equipment will be shipped either as classified at system authorization 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? Is it Government Furnished Equipment (GFE)?

F. Hand Carry (Courier)

This must be authorized by the Facility Security Officer (FSO) and/or designated security representative. 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] of the following:

- Security relevant problems that occur.
- Discrepancies in the documentation or equipment.

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

CLEARED CONTRACTOR LETTERHEAD

[DATE]

FROM: [Information System Security Manager (ISSM)]

TO: [Name of Government Site Point of Contact (POC)/Address]

SUBJECT: Relocation of Defense Counterintelligence and Security Agency (DCSA) Authorized System [System Name] from [Company Name] to [User Agency Site or Test-Site].

On [Authorization Date], the system identified as [System Name] located at [Company Name and Address] was authorized to process classified information at the [Level of Classified Information] level by the DCSA 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 [Information Owner (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 system outside of the DCSA-approved area changes the original intent of DCSA authorization.

Prior to the above system being relocated to your site, an authorized official of [Site Name] 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 a system and security cognizance for the above-specified system while it will be located at your site and under your jurisdiction. [Name of Cleared Contractor] anticipates the system will be removed from [Site Name], and consequently your jurisdiction, by [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 [Cleared Contractor POC] at [Telephone Number] or by email at [email].

Sincerely,

[ISSM's Signature]

[ISSM's Name]

[Title/Company]

Attachments: DCSA Authorization Letter

Copy to: [Cognizant DCSA Industrial Security Representative (ISR)]

CONCURRENCE:

_____

(Name/Title of Government 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) to the local Defense Counterintelligence and Security Agency (DCSA) 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/IO 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 Code

Specific Processing Location (Bldg/Room)	Cage Code

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

DCSA 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 yes, how will the equipment be handled? Will the equipment leave possession of the contractor? (*Note: Provide details in the Mobility System Plan*)		
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 yes, is the connection authorized by DCSA? Provide details of authorized connection, to include ISA. (*Note: Provide details in the Mobility System Plan*)	☐ Yes	☐ No
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**

System or List of Components Being Moved to the Relocation Site

Quantity	Make/Model	Serial Number	Memory	Non-volatile	Method of Sanitization

Note: The Mobility System Plan Template is intended as a guideline. Industry will need to adjust the plan to meet their specific requirements and comply with any additional and/or contractual requirements.

APPENDIX U: GOVERNMENT-TO-CONTRACTOR ISA TEMPLATE

Interconnection Security Agreement

Between

(Name of User Agency)
and
Defense Counterintelligence and Security Agency

REFERENCES: (A) DODD 8500.1
(B) NISPOM, CHAPTER 8
(C) (GCA Regulation)

This Interconnection Security Agreement (ISA) between (User Agency) and the Defense Counterintelligence and Security Agency (DCSA), Designated Approval Authority for (Company Name), is for the purpose of establishing a secure communications link between (User Agency) and (Company Name) for the electronic transfer of classified information. Each of the undersigned agrees to and understands the procedures that will be in effect and adhered to. It is also understood that this ISA summarizes the information system (IS) security requirements for approval purposes and supplements (Company Name) approved system security plan (SSP).

1. Contract Information

This ISA describes the classified network arrangement between (Company Name) and (User Agency) in support of the (Name of Program). The (Name of Program) is a (brief description of program) sponsored by (User Agency). The contract number is (Contract Number). The Prime contractor is (Name of Prime Contractor), whose Cage Code is (Cage Code Number).

At (User Agency) direction, (Company or User Agency Name) is establishing a remote access capability to the (Name of Classified Computer System and Unique Identifier); with a remote access IS located at (List User Agency or Company, as appropriate). *(Note to Template User: Please word this paragraph so that it is obvious who will be the host, if applicable, and who will be the remote site(s))*. This capability will allow (Company or User Agency, as appropriate) personnel to access the (List Name of Classified IS and UID) as remote users. The (User Agency) IS is located at (address).

The following (DCSA) key points of contact are identified:

Name	Title	Phone	Email
Karl Hellmann	NISP Authorizing Official	571-305-6627	Karl.j.hellmann.civ@mail.mil
Jonathan Cofer	DCSA HQ MOU Coordinator	571-305-6739	Jonathan.h.cofer2.civ@mail.mil
	Regional Authorizing Official		
	ISSP		

The following (Company) key points of contact are identified:

Name	Title	Phone	Email

The following (User Agency) key points of contact are identified:

Name	Title	Phone	Email

2. Description

(Company or User Agency Name) operates the (List Names of Classified System) IS at (Identify C-I-A categorization), whereby all users have the clearance and need to know for all information on the system. The highest level of classification of the IS is (Level of Information). All personnel with access to the (Name of Classified System) will be briefed for (Give name of specific briefing, e.g. COMSEC).

(*Describe connection and connection approval process. An example follows*): The (Company or User Agency Name) IS will be connected to the (Name of Classified System at different enclave (if needed)) at (Company or User Agency Name at different enclave (if needed)), by a communication circuit for the transfer of data. The circuit will be protected at each end by an NSA Type 1 encryption device, to provide encryption of the circuit. Operational key for the NSA Type 1 encryption shall be at the (classification level) level.

Any further network security requirements not described within this document are detailed in the attached network security plan and connection approval process.

3. Network Information System Security Officer (Network ISSO) Responsibilities

The Network ISSO (Network ISSO Name) at (host--Company and User Agency Name) will have the following responsibilities. He or she will brief operator personnel involved with use of the communications link on network operating procedures and their responsibilities for safeguarding classified information in accordance with the requirements of paragraph 5-100 of the National Industrial Security Program Operating Manual (NISPOM) or applicable Department of Defense policy. The IS Security Officer at (List Names of other User Agency or Company Site) will conduct an equivalent briefing for network responsible personnel.

The Network ISSO at (Company and User Agency Name) and the IS Security Officer at (Name of other site(s)) will indoctrinate system operators and support personnel concerning:

a. The need for sound security practices for protecting information handled by their respective IS, including all input, storage, and output products.

b. The specific security requirements associated with their respective IS as they relate to Need-to-Know (NTK) and operator access requirements.

c. The security reporting requirements and procedures in the event of a system malfunction or other security incident occurs.

d. What constitutes an unauthorized action as it relates to system usage.

e. Their responsibility to report any known or suspected security violations.

It is the responsibility of each individual operator to understand and comply with all required procedures for using the (Name of Classified System at Company Site), as described in the SSP which is approved by the Defense Counterintelligence and Security Agency (DCSA).

The system user shall report all instances of any security violations to the ISSM *(or Network ISSO if located at company)* at (Company Name). In addition, the User Agency IS Security Officer *(or Network ISSO if located at User Agency)* will report any security violations to the system.

4. Interconnect Procedures

The communication link at (Host Site Name) will be available (insert hours) per day. The operating system at the host IS automatically records all operators logging in and out. When logged in, the operators at (Contractor or User Agency Name) will be able to access the system for the transfer of classified data.

All signers agree there are no further connections on this network to DISN networks, including the SIPRNet.

Each interconnected site must maintain a current and valid accreditation in accordance with Department of Defense policy.

When the communications link between (User Agency) and (Company Name) is no longer required, communications between sites will be disabled by removing the remote users from the "system password file" and physically disabling the encrypted link from the router, if applicable. Additionally, the user agency will notify DCSA in writing of cancellation of the ISA.

5. Approval

The secure communication link between (User Agency) and (Company Name) shall not be initialized until approval of these procedures by all AOs is indicated below. This agreement will remain in effect for three years from the date of the signatures below, unless specifically terminated by either AO. This ISA becomes effective upon signatures of all parties.

Defense Counterintelligence and Security Agency	(User Agency)
_____	_____
KARL HELLMANN	(Name of User Agency Official and Rank)
NISP Authorizing Official	Authorizing Official
Date:	Date:

APPENDIX V: WARNING BANNER

Defense Counterintelligence and Security Agency (DCSA) 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. -- 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. -- 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 W: ACRONYMS

A&A	Assessment and Authorization
AC	Access Control
AFT	Assured File Transfer
AI	Administrative Inquiry
AO	Authorizing Official
AP	Assessment Procedure
ATA	Advanced Technology Attachment
ATD	Authorization Termination Date
ATO	Authorization to Operate
ATO-C	Authorization to Operate With Conditions
AU	Audit and Accountability
CAC	Control Approval Chain
CAGE	Commercial and Government Entity
CCP	Common Control Provider
CCI	Control Correlation Identifier
CD	Compact Disk
CDS	Cross Domain Solution
CI	Counterintelligence or Controlled Interface
C-I-A	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
CNWDI	Critical Nuclear Weapon Design Information
COMSEC	Communications Security
CONOPS	Concept of Operations
COOP	Continuity of Operations
COTS	Commercial-off-the-Shelf
CP	Contingency Planning
CPG	Connection Process Guide
C/S	Client/Server
CSA	Cognizant Security Agency
CSS	Central Security Service
CTTA	Certified TEMPEST Technical Authority
DAAPM	DCSA Assessment and Authorization Process Manual
DAR	Data At Rest

DARPA	Defense Advanced Research Projects Agency
DATO	Denial of Authorization to Operate
DCO	Device Configuration Overlay
DCSA	Defense Counterintelligence and Security Agency
DSS	Defense Security Service
DISA	Defense Information Systems Agency
DISN	Defense Information System Network
DNS	Domain Name System
DoDIN	Department of Defense Information Network
DREN	Defense Research and Engineering Network
DRP	Disaster Recovery Plan
DSA	Designated Security Authority
DSWAN	DARPA Secret Wide Area Network
DTA	Data Transfer Agent
DTEN	DISN Test Evaluation Network
DVD	Digital Versatile Disk
EAP	Extensible Authentication Protocol
ECA	External Certification Authority
EEPROM	Electrically Erasable Programmable Read-Only Memory
eMASS	Enterprise Mission Assurance Support Service
eWAN	Enterprise Wide Area Network
EPL	Evaluated Products List
EPROM	Erasable Programmable Read-only Memory
FCL	Facility (Security) Clearance
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
IAM	Information Assurance Manager
IATC	Interim Approval to Connect
IATT	Interim Authorization to Test
I/O	Input / Output

IA	Information Assurance
IDS	Intrusion Detection System
IO	Information Owner
IP	Internet Protocol
IR	Incident Response
IRAD	Independent Research and Development
IRP	Incident Response Plan
IS	Information System
ISA	Interconnection Security Agreement
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
JITC	Joint Interoperability Test Command
JTEN	Joint Training and Experimentation Network
JTF	Joint Task Force
KS	Knowledge Service
KVM	Keyboard/Video/Mouse
KMP	Key Management Personnel
LAN	Local Area Network
LCD	Liquid Crystal Display
LED	Light Emitting Diode
LOP	Local Operating Procedure
LRU	Lowest Replaceable Unit
MA	Maintenance
MAC	Media Access Control
MACE	Multi-Agency Collaboration Environment
MDACNet	Missile Defense Agency Classified Network
MFD	Multifunction Device
M-L-L	Moderate-Low-Low
MP	Media Protection
NAO	NISP Authorization Office
NATO	North Atlantic Treaty Organization
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
NSI	National Security Information
NTK	Need-to-Know
ODAA	Office of the Designated Approving Authority
P2P	Peer-to-Peer
PAC	Package Approval Chain
PCL	Product Compliant List
PDS	Protected Distribution System
PE	Physical and Environmental Protection
PED	Portable Electronic Device
PL	Planning or Protection Level
PM	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
RAM	Random Access Memory
RAR	Risk Assessment Report
RD	Restricted Data
REL TO	Authorized for Release to
RF	Radio Frequency
RFID	Radio Frequency Identification
RFP	Request for Proposal
RFI	Request for Information
RMAT	Remote Maintenance and Testing
RMF	Risk Management Framework
RO	Releasing Officer
ROM	Rough Order of Magnitude
ROM	Read Only Memory
SA	System and Services Acquisition
SA	System Administrator
SAAR	System Access Authorization Request
SAP	Special Access Program
SAPF	Special Access Program Facility

SAR	Security Assessment Report
SCA	Security Control Assessor
SCAP	Security Content Automation Protocol (pronounced S-CAP)
SCC	SCAP Compliance Checker
SCG	Security Classification Guide
SCP	Secure Communications Plan
SDREN	Secure Defense Research Engineering Network
SI	System and Information Integrity
SIPRNet	Secret Internet Protocol Router Network
SLA	Service Level Agreement
SLCM	System-Level Continuous Monitoring
SOP	Standard Operating Procedure
SP	Special Publication
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
TPI	Two Person Integrity
TSCO	Top Secret Control Officer
UAC	User Account Control
UHF/VHF	Ultra-High Frequency/Very High Frequency
UPS	Uninterrupted Power Supply
USERID	Individual User identifier
USG	U.S. Government
VDS	Video Distribution System
VPL	Validated Products List
VPN	Virtual Private Network
VTC	Video Teleconference
VVoIP	Voice and Video Over Internet Protocol
WAN	Wide Area Network
WDE	Whole Disk Encryption

APPENDIX X: DEFINITIONS

Assured File Transfer	A High-to-Low data transfer.
Authorization	Formal declaration by the Authorizing Official (AO) that a system is authorized 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 Wide Area Network (WAN) AO allowing the connection of a node to a WAN.
Authorization to Operate	Approval granted by an AO for a system 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 a system and other safeguards, made in support of the assessment and authorization process, to establish the extent that a particular design and implementation meets a set of specified security requirements by the Information System Security Manager (ISSM).
Classified Information	Official information that has been determined, pursuant to Executive Order (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 a 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 National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 or in Committee on National Security Systems Instruction (CNSSI) 1253, that provides equivalent or comparable protection for an information system.
Command Cyber Readiness Inspection	A review of a system connected to the Secret Internet Protocol Router Network (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.
Control Correlation Identifier (CCI)	Decomposition of a NIST control into a single, actionable, measurable statement.
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 a Facility (Security) Clearance (FCL) by a Cognizant Security Authority (CSA).
Denial of Authorization to Operate	When a security plan has been accepted and reviewed by an Information System Security Professional (ISSP) and is not granted an authorization 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 a system.
Executive Order (E.O.) 12829	The National Industrial Security Program (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	A system that is outside of the boundary established by the AO and can be part of an interconnected system (Government-to-Contractor).

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 (FCL)	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 Defense Counterintelligence and Security Agency (DCSA) mission across an assigned area of responsibility. Industrial Security Representatives 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, North Atlantic Treaty Organization (NATO), Authorized for Release to (REL TO), Critical Nuclear Weapon Design Information (CNWDI), Communications Security (COMSEC) or Crypto variable information, Formerly Restricted Data (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 an Interconnection Security Agreement (ISA) for the WAN. The Host also determines the requirements that must be met before connection to the WAN is permitted.
Information Owner (IO)	An element of a United States (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 system security, and operational compliance with the documented security measures and controls, at the cleared contractor facility.
Information System Security Officer (ISSO)	The ISSO is assigned by the ISSM when the facility has multiple authorized systems, 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 system security program warrants the appointment.

Interconnection Security Agreement (ISA)	Agreement used to establish an interconnection between two or more separately authorized systems.
Interim Approval to Connect (IATC)	Temporary approval granted by a WAN AO allowing the connection of a node to WAN.
Interim Authorization to Test (IATT)	Temporary authority to connect granted to the WAN host for a defined period of time in order to test the communication capability with a remote node prior to authorization. The test data must not be classified or contain program information.
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.
Interconnection Security Agreement (ISA)	An agreement established between the organizations that own and operate connected systems to document the requirements of the interconnection.
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.
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	A computer network is a group of computer systems and other computing hardware devices that are linked together through communication channels to facilitate communication and resource-sharing among a wide range of users. Networks are commonly categorized based on their characteristics.
NISP Authorization Office (NAO)	Delegated the responsibility for the DCSA mission for cleared contractor system assessment and authorization oversight.
Node	Any device or collection of devices authorized under a single 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 DCSA 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.
Program Security Officer (PSO)	Individual with assigned responsibility for maintaining the appropriate operational security posture for a system security program.

Protected Distribution System (PDS)	Secure conduit for protecting classified lines, transmitting data outside of a DCSA approved area (Closed 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.
Reauthorization	An action taken by DCSA when security relevant changes are made to an approved system. An action taken by DCSA when the Authorization Termination Date (ATD) has been reached.
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 Assessment	Process of analyzing threats to, and vulnerabilities of, a 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 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	A piece of equipment utilized to enable encrypted/secure voice and/or data communication.
Security Classification Guide	Comprehensive guidance regarding security classification of information concerning any system, plan, program, or project; the unauthorized disclosure of which reasonably could be expected to cause damage to the national security. Precise classification guidance is prerequisite to effective and efficient information security and assures that security resources are expended to protect only that which truly warrants protection in the interests of national security.
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 Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) benchmarks and Operating System (OS) specific baselines to analyze and report on the security configuration of the system. 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 a system or its 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 Information Assurance (IA) and IA enabled devices/systems.
Service Level Agreement (SLA)	A contract between a service provider (either internal or external) and the end user that defines the type, level, and quality of service expected from the service provider.
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.
System Security Plan (SSP)	Formal document that provides an overview of the security requirements for the system and describes the security controls in place or planned for meeting those requirements.
Threat	The potential for a threat-source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.
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.
Two Person Integrity (TPI)	A provision that prohibits one person from acting alone.
User	Person or process authorized to access a system.
User Code	Software that allows a user to modify data or functions of a system. Determining if a system has user code may be a matter of degree, but as an example: If a system 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 system, then the system 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 Internet Protocol (IP).

Vulnerability	A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.
Wide Area Network (WAN)	Network that exists over a large-scale geographical area.

APPENDIX Y: 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.

- Executive Order (E.O.) 12829, *National Industrial Security Program*, January 6, 1993
- E.O. 13526, *Classified National Security Information*, December 29, 2009
- Department of Defense (DoD) 5220.22-M, Change 2, *National Industrial Security Program Operating Manual*, May 18, 2016
- Committee on National Security Systems Instruction (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
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, Revision 1, *Guide for Conducting Risk Assessments,* September 17, 2012
- NIST SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations – A System Life Cycle Approach for Security and Privacy*, December 20, 2018
- NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View,* March 1, 2009
- NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems,* September 1, 2002
- NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 30, 2013 (Updates as of January 22, 2015)
- NIST SP 800-53A, Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans*, December 18, 2014
- NIST SP 800-60, Volume 1, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*, August 1, 2008
- NIST SP 800-61, Revision 2, *Computer Security Incident Handling Guide*, August 6, 2012
- NIST SP 800-88, Revision 1, *Guidelines for Media Sanitization*, December 17, 2014
- NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, September 30, 2011

- NIST SP 800-180, Volume 1, *Security Systems Security Engineering, Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems,* March 21, 2018

- FIPS 140-2, *Security Requirements for Cryptographic Modules*, May 25, 2001; Change notice December 3, 2002

- Committee on National Security Systems Directive (CNSSD) 504, *Directive on Protecting National Security Systems From Insider Threat,* September 30, 2016

- E.O. 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing of Classified Information,* October 7, 2011

- Presidential Memorandum, *National Insider Threat Policy and Minimum Standards for Executive Branch Threat Programs,* November 21, 2012