Irregular Warfare Technical Support Directorate (IWTSD)

Cybersecurity Guidelines for IWTSD Projects Development

Version 1.0

Prepared by:

IWTSD Advanced Development Subgroup

Revision History

Date	Revision	Description	Author
October 2023	0.1	Initial draft creation.	IWTSD
December 2023	0.2	Updated based on peer-review and to more align with the IWTSD Technology Transition Handbook.	IWTSD
January 2024	0.3	Updated based on peer-review and additional feedback.	IWTSD
February 2024	0.4	Updated based on additional peer-reviews.	IWTSD
February 2024	1.0	Final.	IWTSD

Table of Contents

Contents

Table of Figures

Table of Tables

Executive Summary

Most IWTSD projects and requirements rely on information technologies (IT) to rapidly develop and deliver capabilities that create an advantage for the warfighter. Federal law and DoD policy requires the integration of cybersecurity (DoDI 8500.01) and Risk Management Framework (DoDI 8510.01) processes across IT life cycles, and that federal organizations assess and authorize IT systems and components before using them operationally[1]. As an OSD component, IWTSD works with end users and information system owners to conduct the Risk Management Framework (RMF) activities throughout the acquisition process to increase operational security.

IWTSD's goal is to transition Research, Development, Test and Evaluation (RDT&E) systems, prototypes, and capabilities to our end users, so we need to integrate cybersecurity using the RMF processes throughout project development so deliverables are eligible for operational use. If we develop prototypes that fail to comply with the cybersecurity requirements in the DoDI 8510.01, that could result in an unacceptable risk posture and a denial of authorization, which means that the project deliverable is not authorized to operate and not placed in operation, or it is not authorized for use by a customer organization unless/until cybersecurity weaknesses or deficiencies are addressed. This potentially adds cost, delays delivery of a capability, and/or cancels a project without transitioning.

This document provides vendors an overview of risk management and cybersecurity considerations in the context of IWTSD RDT&E projects that will transition to end user systems and operating environments and identifies the artifacts that may be necessary throughout the project development process to demonstrate compliance with cybersecurity requirements in support of an assessment and authorization decision, such as an Authority to Operate (ATO).

It is important to note that different projects may have unique requirements; therefore, the project development life cycles may look different. However, the guidance provided in this document serves as a core foundation that can be tailored to meet the specific needs of a given project. By following this guidance, project teams can ensure that they follow an approved framework addressing cybersecurity concerns throughout the development process, regardless of the project's specific requirements.

[1] See DoDI 8510.01, *Risk Management Framework (RMF) for DoD IT*

1. Introduction

1.1. What is Cybersecurity?

Cybersecurity is protecting against unauthorized access to Federal/DoD information. DoD Instruction 8510.01 establishes the RMF for DoD Information Technology as a means to harden and secure DoD systems, maintain the security posture of that DoD system throughout its lifecycle, and manage risk to DoD systems.

1.2. What is the Risk Management Framework (RMF)?

The RMF is a set of guidelines that help organizations identify, measure, assess, manage, and monitor risks to their information and information systems. RMF provides a standard approach for organizations to determine their unique risks and implement the appropriate resources (people, process, and technology) to reduce the overall enterprise risks. RMF requires that security and privacy considerations are integrated from the beginning of a project and continuously monitored instead of making adjustments after the project is already operational.

Note: Federal law and DoD policy requires federal agencies to implement RMF when developing or acquiring systems that receive, process, store, display, or transmit federal information.

1.3. Does RMF Apply?

If you answer ***Yes*** to any of the questions listed below, then RMF applies to your project:

- Are you developing Department of Defense (DoD) or Federal information systems (weapon systems, standalone systems, control systems, or any other type of systems with digital capabilities)?
- Will your project transmit/process/display/store Federal data or information (at any classification level)?
- Will your project/solution integrate with a DoD or other Federal information system/network?
- Will you deploy your project/solution on a DoD or other Federal information system/network?
- Will users access your project /solution remotely from a DoD or other Federal information system/network?

See Appendix A for Frequently Asked Questions and Appendix B for more information on the RMF process.

1.4. Getting Started with RMF

The RMF is a structured process that helps organizations manage and reduce risks to their information and systems. The RMF identifies risk as a function of the information received, processed, stored, displayed, or transmitted by a system, and the impact if that information is disclosed, altered, or unavailable.

The RMF Knowledge Service (RMF KS) is the authoritative source for everything RMF, which provides additional information about the policy, templates, publication downloads, etc. The RMF KS can be access at https://rmfks.osd.mil.

Figure 1 depicts the steps of the RMF: Preparation, Categorization, Security Control Selection, Implementation, Assessment, Authorization, and Continuous Monitoring. By following this framework, organizations can effectively manage risks to their information and systems and ensure that they are in compliance with relevant regulations and standards.

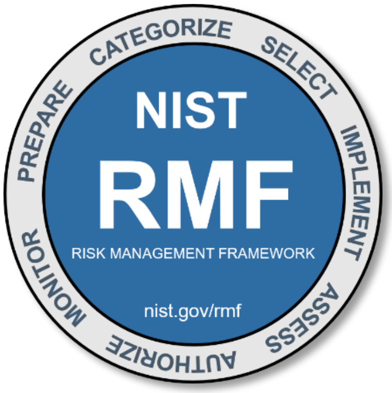


Figure 1: The Risk Management Framework

Chapter 3.1 of NIST SP 800-37, Rev 2, and Chapter 2 of NIST SP 800-39, explain the elements of managing risk from an organization perspective. Organizations, programs, and vendors all share responsibility for risk in DoD systems.

The first step of RMF is determining the types of information that a system will receive, process, store, display, transmit, and the impact level for each information type. The impact level drives the security categorization (step 1 of the RMF process), and the categorization determines which security controls apply.

NIST 800-53 provides a security control catalogue, broken down by control family, and identifies which controls and control enhancements apply for low, moderate, or high impact systems. Some controls and control enhancements are implemented by the organization, some are implemented by the system through technical means, and some can be implemented through a combination of the two (step 2 of the RMF process).

Using the appropriate assessment procedure, the security control assessor tests the security controls to determine if the controls are implemented correctly, operating as intended, and producing the intended outcome (step 3 of the RMF process).

Based on a determination of risk to the organization's operations, individuals, or assets, including the results of the System Security Plan (SSP), Security Authorization Report (SAR), and Plan of Actions and Milestones (POA&Ms), the AO issues an authorization decision to grant or reject the request for the project to become operational (step 5 of the RMF process). If the AO issues an ATO and the project team deploys the project, continuous monitoring activities begin and are performed throughout the project life cycle (step 6 of the RMF process).

Refer to Appendix B: RMF Process for additional information on activities and source publications to assist with each step.

2. Aligning RMF with IWTSD Projects

In order to develop, deliver, and transition IT systems, applications, or components for end users that are eligible for operational use, project teams (including IWTSD Program Managers (PMs), end users, and vendors) should consider information security and system integration requirements at every phase of the project. This includes integrating cybersecurity, RMF processes, and technical security controls into system requirements reviews and preliminary designs, iteratively implementing security throughout development and testing (including remediation of open findings and vulnerabilities), understanding which artifacts may be required to document and demonstrate security implementation to facilitate security assessments and authorization decisions, and considering continuous monitoring requirements (including ongoing patch management and quarterly Security Technical Implementation Guide (STIG) updates) when developing and delivering transition plans. Vendors should also understand how to interface with the operating environment, taking into account organizational policies/processes, such as account management, access control, and logging.

2.1. Artifacts to Support RMF Implementation During IWTSD Projects

Most IWTSD projects are broken out into phases with deliverables due at the end of each phase. In general, projects may incorporate the following phases:

- Phase 1 – Project kickoff and System Requirements Review
- Phase 2 – Initial design and configuration, concluding with a Preliminary Design Review
- Phase 3 – Ongoing design and testing of system configurations and components in preparation for a Critical Design Review
- Phase 4 – Prototype development based on approved design, concluding with a Test Readiness Review
- Phase 5 – Prototype test and evaluation
- Phase 6 – Final delivery of system/prototype (including required documentation) and training

During each phase, vendors should demonstrate how they are integrating cybersecurity and RMF processes into deliverables and associated documentation to manage and mitigate risk throughout the project lifecycle.

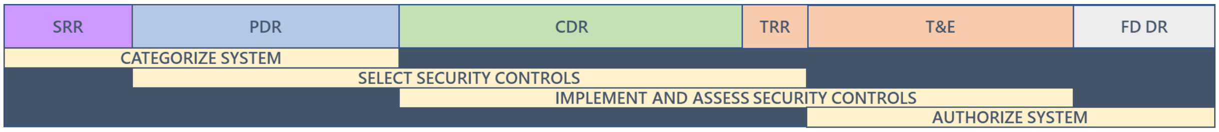


Figure 2: Aligning RMF with IWTSD Project Life Cycle

2.1.1. Project Kickoff and System Requirements Review

IWTSD initiates projects in response to end user requirements and capability gaps. When reviewing the proposed system requirements and performance specifications for the project kick off, the vendor should also work closely with IWTSD and the end users to identify the applicable cybersecurity requirements and potential deployment environment. To ensure a smooth transition, it is recommended to establish a communication channel between the IWTSD cybersecurity team and the end users' cybersecurity team to establish transition security requirements.

Different networks operate differently and may have different security requirements, and organizations have varying levels of risk tolerance; therefore, the vendor should review security requirements to integrate or deploy the prototype or system on the end user’s network or operating environment. For security planning and documentation purposes, it is important to understand if the user’s network has an existing ATO and the processes to integrate new applications or components within an existing authorization boundary, or if the project will need its own ATO or authorization decision.

During the **System Requirements Review (SRR)**, the vendor should identify data sets and information types that will be stored, processed, and/or transmitted by the project. The vendor may be required to determine the system's security categorization and security impact levels based on the end user’s network security requirements. The authorization boundary information and information types are important inputs for system categorization and drives which security controls apply. Use the Federal Information Processing Standards (FIPS) 199[2], the National Institute of Standard and Technology Special Publication (NIST SP) 800-60[3], and its appendices as guides to determine the overall security categorization and security impact levels for the information types of the system.

2.1.2. Preliminary Design Review

As part of the **Preliminary Design Review (PDR)**, the vendor should capture all system components, connections, and data flows of the system or final product. This is an important step in ensuring that the system is designed and developed in accordance with the project requirements and specifications. By capturing all the necessary information, the project team can identify potential cybersecurity issues early on in the development process, which can save time and resources in the long run. It is also important for the vendor to consider any security or privacy concerns when capturing this information.

The vendor should leverage the Department of Defense Architecture Framework (DoDAF) standard to develop operational and systems viewpoints within their deliverables, plans, and/or design documents to illustrate the security interfaces. As part of the preliminary design documents, the vendor should include the following artifacts:

Operational Viewpoint (OV-1) explains the purpose and main features of a mission or scenario. It describes the interactions of the subject architecture within a specific environment and its interactions with external systems. The OV-1 is useful for highlighting unique aspects of operations and the main concepts.

Systems Viewpoint (SV-1) addresses the composition and interaction of systems, which also incorporates human elements as types of Performers. The primary of the SV-1 is to show resource structure, for example, identify the primary sub-systems, performer and activities and their interactions. This is an important step in developing and managing complex systems, as it helps the PMs and the end user better understand the relationships and dependencies between different subsystems and activities, which can help them make informed decisions about resource allocation and project scope. Additionally, the SV-1 can be used to identify potential security risks and technical issues early on in the project lifecycle.

At this project stage, the vendor should start drafting the **SSP**, including the OV-1, SV-1, and risk and vulnerability assessment procedures. The SSP is a living document that describes the components included within the system, the environment in which the system operates, how the security requirements are implemented, and the relationships with or connections to other systems.

2.1.3. Critical Design Review

At the **Critical Design Review (CDR)**, the vendor should present the initial product baseline for the system and its constituent system elements with the PM and stakeholders. The CDR should specify requirements and system interfaces for enabling system elements such as support equipment, data systems, and operations and maintenance. The vendor may need to conduct initial tests of technologies or product preparing the project team for the CDR, but should not start building the system until the Government has approved the design during the CDR.

In conjunction with the critical design review, IWTSD may also require the vendor to develop a detailed test plan that includes specific steps to implement security controls into systems and sub-systems. IWTSD may require vendors to conduct security control assessments and implement necessary security controls if the project reaches a maturity level where the vendor begins conducting components and integration tests. These may include but are not limited to design and code reviews, application scanning, regression testing, unit testing, functional testing, acceptance testing, or security configuration reviews. Vendors may be required to provide evidence of assessment results to be reused in the security authorization process.

To ensure that the system being developed meets the necessary security standards, the IWTSD cybersecurity team may need to conduct security assessment independently. Therefore, it is advisable for the vendor to work together with cybersecurity teams to finalize a detailed security implementation plan before the CDR and present the plan to the stakeholders during the review. This will allow any necessary security controls to be identified and implemented early on in the development process, reducing the risk of potential security vulnerabilities being discovered later on. The plan should outline an iterative and systematic approach to implement security controls. Also, the plan should provide a method to implement the security controls specified in the SSP in accordance with applicable STIGs or Security Requirements Guides (SRGs) and/or the control implementation guidelines described in NIST SP 800-53, Security and Privacy Controls for Information Systems and Organizations.

2.1.4. Test Readiness Review

Following the CDR, the vendor will start building the prototype and implementing security controls based on the approved design. During the **Test Readiness Review (TRR)**, the vendor presents the status of the system/product being developed and shows the system/product is ready to go through the system and security testing. As a part of TRR, the vendor should present capability readiness and features, including security controls that are incorporated into the system/product.

The vendor should also update the SSP to include a functional description of the controls in place and how the controls satisfy security requirements. If controls have not yet been implemented, the vendor should describe the plan for meeting the security requirements. Controls provided by common control providers should be marked as such in the SSP.

A vendor may be required to provide evidence to show that security and privacy controls have been implemented as applicable. Additionally, vendors may be required to develop system security documentation, including:

- Security Control Traceability Matrix (SCTM)**:** lists all controls selected for the system as well as additional details on each control, e.g. implementation status, monitoring frequency, etc.
- POA&M: Used to list vulnerabilities and security gaps identifying current risk and milestones to work towards mitigating those risks.

2.1.5. Test and Evaluation

Test and Evaluation (T&E) is a critical process that involves the systematic examination and validation of various systems, products, or technologies to ensure they meet specific requirements and perform as intended. T&E activities help to assess the performance, reliability, safety, and security of the system/product being evaluated and identify any technical or security issues to be corrected before they are deployed.

The vendor should continue identifying security gaps and correct all critical and high findings as much as possible during the **T&E**. It is the vendor's responsibility to continue updating, hardening, and patching system(s) with the latest updates and provide a plan to continuous monitoring risks leading to the full deployment decision review. Refer to Appendix C: POA&M Implementation for remediation timelines.

2.1.6. Full Deployment Decision Review

To prepare for the Full Deployment Decision Review (FDDR), the vendor may be required to deliver the following documents or artifacts:

- An updated SSP including the most recent test results for all applicable information assurance (IA) Controls.
- A vulnerability scan report that shows all critical and high findings have been remediated.
- An updated POA&M to depict the present-day state of risks in the system being developed with specific plans to mitigate those risks.
- A detailed plan with recommendations to address all identified risk, continue patching efforts, and maintain continuous monitoring activities to prevent and address new risks.

2.2. Transition Plan and Other Considerations

For IWTSD projects that don't require a formal security authorization, vendors should consider continuous security assessments to identify, manage and mitigate risk as part of their transition plan. This will ensure that the transition partner understands what risk is being introduced, so they can make an informed decision if the transition can still occur or if critical/significant risk must be addressed first.

For IWTSD projects that require formal security authorization, the AO reviews the security authorization package and makes a risk-based decision to formally accept or reject residual risks associated with the system or final product before issuing an ATO or a Denial Authority to Operate (DATO). Vendors should consider the authorization and continuous monitoring strategies in the transition plan.

The transition plan should specify the timeline and responsibilities for each system and security task, as well as any risks and mitigation strategies. The plan should also include a communication strategy to ensure stakeholders are informed of the transition and its impacts. The transition plan should be comprehensive and cover all aspects of the system, including hardware, software, data, security, and personnel.

It is important to note that security does not stop when a product is delivered to the operational environment. The vendor should also work with the end user to establish a continuous monitoring strategy that maintains situational awareness of the system's security posture and ensure that changes to the system or its environment of operation do not lead to unacceptable risks.

Appendix A: RMF Frequently Asked Questions

Is RMF mandatory?

Yes, federal law and DoD policy requires that federal agencies implement the RMF when developing or acquiring systems that receive, process, store, display, or transmit federal information. References:

- Federal Information Security Modernization Act of 2014 (FISMA)
- Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*
- DoDI 8500.01, *Cybersecurity*, March 14, 2014
- DoDI 8510.01, RMF for DoD Information Technology (IT), July 19, 2022
- Executive Order 13800 of May 11, 2017, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
- Executive Order 14028 of May 12, 2021, *Improving the Nation's Cybersecurity*

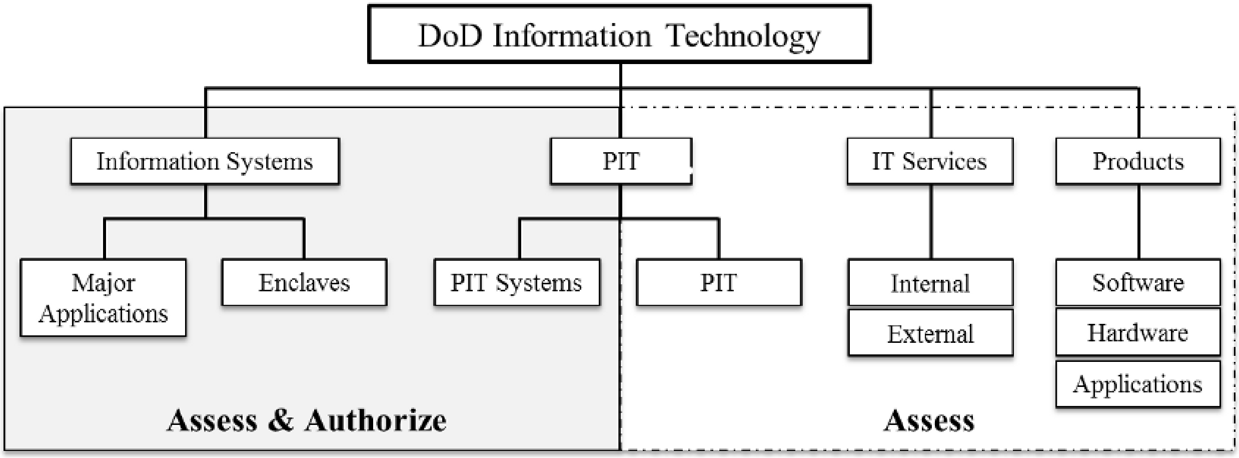
At what point does data become Federal government data or information?

Government information is information that is created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the Federal Government in any medium or form[4]. Any data that satisfies one or more of these conditions qualifies as federal government data.

My project will reside within another information system or major application. Do I need to take my project through the full RMF process?

Your project may not require its own authorization decision (i.e., ATO) unless explicitly required by the receiving organization, but you still need to follow the RMF process through the assess phase.

Not all information technology rises to the level of an information system or platform information system, even if it stores, processes, displays, or transmits DoD or federal information. According to the DoDI 8510.01, technologies below the system level (e.g., system components, hardware, software, external services) do not require an ATO. However, these technologies still need to complete the RMF process through the assess phase.



[4] See Circular A-130, *Management of Federal Information Resources*.

My project is developing a stand-alone system. Do I need to go through the RMF process?

A stand-alone system that stores, processes, displays, or transmits federal government information needs to go through the RMF process. DoD information systems and Platform Information Technology (PIT) systems that are stand-alone must be authorized to operate, but assigned security control sets may be tailored/modified as appropriate with the approval of the AO.[5] For instance, network-related controls may be eliminated for stand-alone systems.

Who signs off on the ATO?

The senior government official designated as the AO for the government organization awards an ATO to systems that meet requisite security requirements. The AO determines the degree of acceptable risk based on mission requirements, accepts security responsibility for the operation of an assessed system, and officially declares the system *authorized to operate*.

If the AO issues an ATO, is that transferrable to other organizations?

Yes, a security authorization decision issued by one federal government agency is transferrable to another. This concept is called **reciprocity**. Cybersecurity reciprocity makes it possible to develop and field IT capabilities rapidly and efficiently across federal government agencies by reducing time and resources spent on redundant test, assessment, and documentation efforts.

For reciprocity to occur, the developing organization provides the receiving organization with sufficient evidence regarding the security posture of the information system or technology, so that AO for the receiving organization can use that evidence to make credible, risk-based decisions regarding the acceptance and use of the IT or the information it stores, processes, or transmits.

The AO for the receiving agency may refuse reciprocity if the receiving organization determines:

- The core RMF documentation for the IT is incomplete and does not provide an informed understanding of potential or existing risks, or
- The risk is unacceptable when compared to the receiving organization's mission assurance requirement.

If the AO for a receiving organization refuses reciprocity, the AO will issue a Denial of Authorization to Operate (DATO) to document their refusal to accept the information system and provide the decision to the deploying organization and/or project team.

Who decides whether a project needs an assessment versus an ATO?

The organization that will be authorizing the project for use within its environment determines the type of assessment and authorization needed.

What are the roles and responsibilities between IWTSD, vendors, and end users as it relates to RMF?

Below are some of the responsibilities of the end users, IWTSD program team, and vendors as it relates to implementing the RMF.

End Users

The end users help the IWTSD program team determine the need, refine the requirements, and inspect and accept the delivered system. The end users will work with other units (e.g. information technology or

[5] See DoDI 8500.01, Cybersecurity https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/850001_2014.pdf

information security team) within their respective organizations to determine the prerequisites for utilizing the proposed solution within their organization and will communicate such requirements to the IWTSD PM. This includes, but is not limited to, determining the security assessment and authorization requirements, and coordinating with the information owner to determine the impact level(s) for the information that will be processed, stored, displayed, and/or transmitted by the project.

IWTSD PMs

IWTSD establishes the contract and owns the day-to-day relationship with the vendor. IWTSD PMs should incorporate RMF language and deliverables in their requirements and Statements of Work where applicable and oversee and monitor the vendor's implementation of technical requirements and security controls. The PM is responsible for reaching out to the vendor with questions, confirming the vendor completes all the necessary tasks and submits the agreed upon deliverables on time to facilitate the risk management process IAW the contract's scope, budget, and schedule. The PM should also coordinate with the end user and/or the IWTSD Advanced Development team to assess the vendor's implementation of security controls.

Vendors

The vendor is responsible for addressing security requirements in their design and implementing security controls iteratively throughout the development lifecycle. This includes remediating security weaknesses and deficiencies as required.

The vendor should employ best practices when implementing security controls, including system-engineering methodologies, system/security engineering principles, secure design, secure architecture, and secure coding techniques.

Appendix B: RMF Process

The RMF is a set of guidelines that help organizations identify, measure, assess, manage, and monitor risks to their information and information systems. RMF provides a standard approach for organizations to determine their unique risks and implement the appropriate resources (people, process, or technology) to reduce the overall enterprise risks.

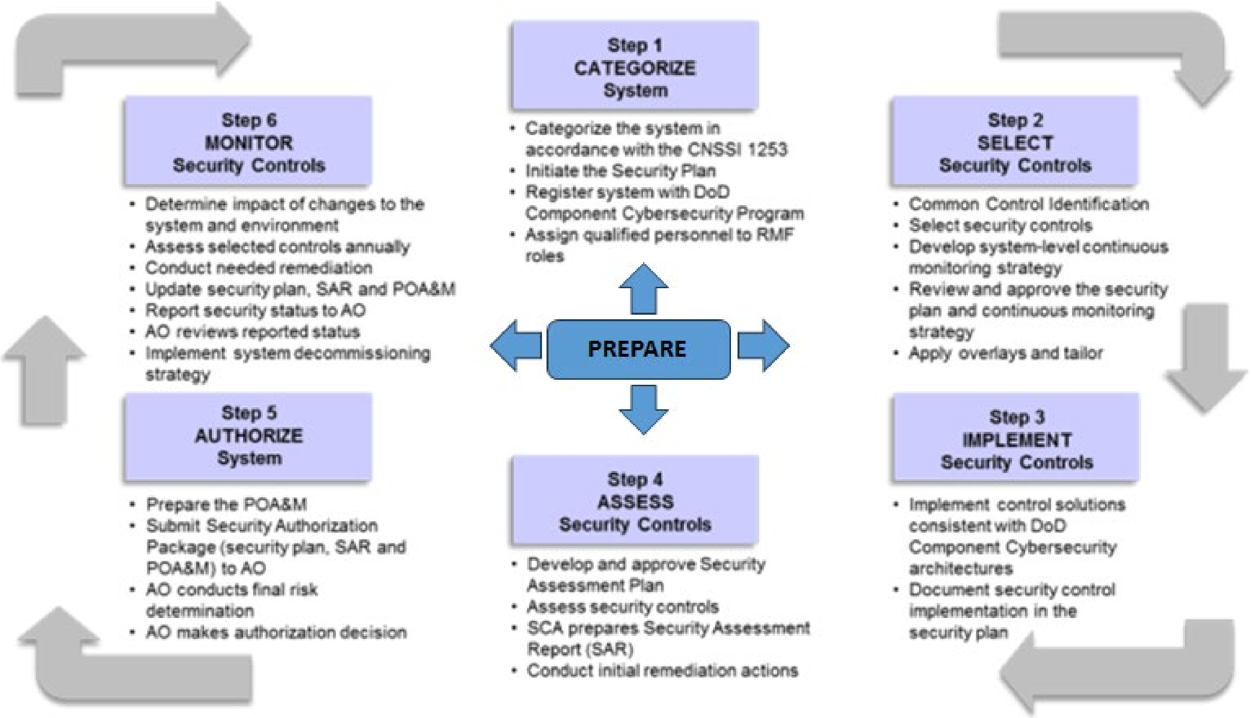

Step 1
CATEGORIZE
System
• Categorize the system in accordance with the CNSSI 1253
• Initiate the Security Plan
• Register system with DoD Component Cybersecurity Program
• Assign qualified personnel to RMF roles
Step 2
SELECT
Security Controls
• Common Control Identification
• Select security controls
• Develop system-level continuous monitoring strategy
• Review and approve the security plan and continuous monitoring strategy
• Apply overlays and tailor
Step 3
IMPLEMENT
Security Controls
• Implement control solutions consistent with DoD Component Cybersecurity architectures
• Document security control implementation in the security plan
Step 4
ASSESS
Security Controls
• Develop and approve Security Assessment Plan
• Assess security controls
• SCA prepares Security Assessment Report (SAR)
• Conduct initial remediation actions
Step 5
AUTHORIZE
System
• Prepare the POA&M
• Submit Security Authorization Package (security plan, SAR and POA&M) to AO
• AO conducts final risk determination
• AO makes authorization decision
Step 6
MONITOR
Security Controls
• Determine impact of changes to the system and environment
• Assess selected controls annually
• Conduct needed remediation
• Update security plan, SAR and POA&M
• Report security status to AO
• AO reviews reported status
• Implement system decommissioning strategy
PREPARE

Figure 3: RMF Process

The addition of the "Prepare" step is to help simplify RMF execution by preparing many activities and artifacts up front, such as:

- Create a Risk Management Strategy
- Identify risk management roles, points of contact, and stakeholders
- Create architecture diagrams and define the authorization boundary

The following table lists the policy documentation used at each step of the RMF process:

Table 1: RMF Steps, Policies, and Descriptions

Step	Policy Documentation	Description
Step 1: Categorize the System	CNSS 1253, FIPS 199, NIST SP 800-60 – security categorization drives what NIST 800-53 IA Controls to test against the Federal/DoD system for compliance	Essential activities to prepare the organization to manage security and privacy risks. Categorize the system and information processed, stored, and transmitted based on an impact analysis.

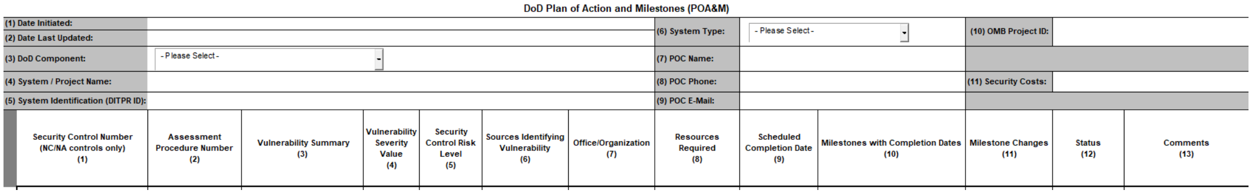
Step	Policy Documentation	Description
Step 2: Select Security Controls	FIPS 200, NIST SP 800-53	Select the set of NIST SP 800-53 controls to protect the system based on risk assessment(s).
Step 3: Implement Security Controls	NIST SP 800-70, NIST SP 800-160	Implement the controls and document how controls are deployed.
Step 4: Access Security Controls	NIST SP 800-53A	Assess to determine if the controls are in place, operating as intended, and producing the desired results.
Step 5: Authorize System	NIST SP 800-37	Senior official makes a risk-based decision to authorize the system (to operate).
Step 6: Monitor Security Controls	NIST SP 800-37, NIST SP 800-53A, NIST SP 800-137	Continuously monitor control implementation and risks to the system.

Appendix C: POA&M Implementation

Open Findings and Risk

Risk to a Federal/DoD system can come from a variety of places, such as hardening the assets, patch management finding missing updates, penetration testing identifying incorrect configurations, etc. Failing to track these risks and acting upon them can prevent a prototype from transitioning to production, disrupt normal operations, delay obtaining an accreditation for a POR, cause an existing accreditation to be revoked, etc.

All open risks for Federal/DoD systems must be tracked on a POA&M. Following DoD guidelines, the Scheduled Completion Date is based on the discovery date and severity of the risk. Once a Scheduled Completion Date is entered, it **cannot** be changed. Milestones identify the baby steps to work towards mitigating the risk. If the original milestones change for any reason, the Milestones Changes column is used with new/updated Milestones and Milestone Dates entered.



DoD Plan of Action and Milestones (POA&M)

(1) Date Initiated:		(6) System Type:	- Please Select -	(10) OMB Project ID:	
(2) Date Last Updated:					
(3) DoD Component:	- Please Select -	(7) POC Name:			
(4) System / Project Name:		(8) POC Phone:		(11) Security Costs:	
(5) System Identification (DITPR ID):		(9) POC E-Mail:			

Security Control Number (NC/NA controls only) (1)	Assessment Procedure Number (2)	Vulnerability Summary (3)	Vulnerability Severity Value (4)	Security Control Risk Level (5)	Sources Identifying Vulnerability (6)	Office/Organization (7)	Resources Required (8)	Scheduled Completion Date (9)	Milestones with Completion Dates (10)	Milestone Changes (11)	Status (12)	Comments (13)

Figure 4: POA&M Template

Remediation Timelines

The table below illustrates the correlation between the standard DoD categories (CAT I-III) and the severity levels (Critical, High, Medium, Low) used by the ACAS Security Center.

Table 2: Remediation Times Based on Severity of the Open Findings

DoD Category Level	Severity Level	Days to Remediate/Mitigate
CAT I	Critical	21
CAT I	High	30
CAT II	Medium	45
CAT III	Low	60

Risk Acceptance

Federal Government PMs and AO will **not** risk accept any open CAT I findings, which includes Critical and High findings from the table above. Open CAT I findings will prevent a Federal/DoD system from proceeding with any transition to production and/or obtaining an ATO. Open CAT I findings that are not remediated within the mitigation timeline, as identified in Table 5, can put an existing Federal/DoD system, POR and ATO in jeopardy.

If an Open finding cannot be remediated for any reason, such as breaking a piece of functionality needed for operational usage, a valid justification is required. The AO has the final decision on accepting any risk acceptance request from the vendor. Proper comments, mitigations, and impact descriptions on implementing and not implementing a change must be included for any risk acceptance requests to the AO. Any risk acceptance request rejected by the AO must be addressed and mitigated by the vendor.

Appendix D: STIG Implementation, Patch Management & Continuous Monitoring

STIG Baseline

Once a Hardware/Software baseline is established by the vendor, the latest version of all applicable STIGs, as released by the Defense Information Systems Agency (DISA), must be applied to all devices, operating systems, etc. in a new Federal/DoD system. Along with continuous patching, this creates the initial STIG security posture to be maintained and identifies any risk up front from open STIG findings to be tracked on the POA&M for further mitigation.

Quarterly STIGs

DISA provides updated STIGs at the end of January, April, July, and October every year. DISA posts updated quarterly STIGs here: https://cyber.mil/stigs/ (Public Key (PK) enabled to access CUI STIGs).

- The Federal Government expects all applicable STIGs to be implemented when they are quarterly released by DISA.
- The Federal Government expects updated STIGs that are released out-of-cycle to also be implemented, to maintain the security posture of the project.

STIG Compliance

If the devices, virtual machines, etc. are not accessible to Federal/DoD staff, all manual STIG checks not performed from an automated process (Nessus, approved script) should include a screen shot to demonstrate compliance with that STIG check. For manual STIG checks, if there is no screen shot provided, then there's no way for the Federal Government to verify compliance for that STIG check without direct access to the asset.

Federal Government STIG Expectations

The Federal Government expects that all risk for Open STIG findings are tracked on a POA&M with milestones to work towards addressing those Open findings.

Continuous Monitoring also includes maintaining the security posture of the Federal/DoD system through quarterly STIG implementation.

Patch Management

Keeping a Federal/DoD system patched with the latest updates is at the forefront of minimizing risk. Microsoft Patch Tuesday, weekly Linux YUM and package updates, Apache suite updates, etc. help keep updated patches installed, and ensure less Open findings come from scans later.

The Federal Government usually uses the ACAS to scan for missing patches, identifying Zero-Day vulnerabilities, etc. throughout the Federal/DoD project lifecycle. This will inform engineers and administrators what patches are needed to bring the Federal/DoD system up to current with the latest updates, to maintain the proper security posture at all steps of the system lifecycle.

The Federal Government expects that all risk for Open ACAS findings, not addressed within the remediation timelines based on Severity, are tracked on a POA&M with milestones to work towards addressing those Open findings.

Continuous Monitoring

The Federal Government's expectation is that security doesn't stop once a product is delivered, as ongoing patching, hardening, and monitoring are required to keep a system operational. Federal/DoD vendors shall be familiar with NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations* for ongoing monitoring in support of risk management.

Continuous monitoring is an ongoing effort to monitor and maintain the security posture of the Federal/DoD system. This includes regular/weekly ACAS scans, quarterly STIG implementation, patch management compliance, addressing POA&Ms, monitoring logs for anomalous activity, etc. where applicable.

Appendix E: IA Tools

The table below is a list of common IA tools used for Federal/DoD systems. Additional IA tools may be used based on Federal Government approval.

Table 3: IA Tools

IA Tool	Description
Assured Compliance Assessment Solution (ACAS) Security Center	Used to perform discovery scans, vulnerability scans, etc. to determine current risk to the Federal/DoD system(s) based on missing patches, invalid software versions, etc.
Electronic Policy Orchestrator (ePO)	Centralized hub to manage all security policies for the various HBSS components deployed for the Federal/DoD system(s).
Enterprise Mission Assurance Support Service (eMASS)	Automates a broad range of processes for comprehensive, fully integrated cybersecurity management, including dashboard reporting, workflow automation, and continuous monitoring supporting RMF for Assessment and Authorization (A&A).
FortiAnalyzer	Tool used for firewall performance monitoring and alerts for denial-of-service attacks, etc.
Endpoint Security Solution (ESS), formally Host-Based Security System (HBSS)	Suite of software applications used within the DOD to monitor, detect, and defend the Federal/DoD system(s).
Network Mapper (NMAP)	Tools for scanning a Federal/DoD system to determine all open and closed ports for an IP to verify PPSM settings, etc.
Security Information and Event Management (SIEM)	Used to log/record device and system events 24/7. Provides a customized dashboard to monitor system events, improper/failed logins, errors, alerts, etc. to help audit, identify and detect intrusion activities.
Wireshark	Protocol analyzer used to identify network attacks, such as Domain Name Service (DNS) spoofing.

Approved operators for ACAS, eMASS and ePO for Federal/DoD systems must complete required training and provide a DD 2875 requesting access from the Federal Government represented ISSM.

Note: Depending on the implementation, location of the Federal/DoD system, etc., ACAS and ePO may be managed by a Cybersecurity Service Provider (CSSP). For example, a CSSP may provide ACAS, but it’s the vendor’s responsibility to perform the ACAS scans and export the results for POA&M implementation. A CSSP may provide the ePO and load updates for ESS, but it’s the vendor’s responsibility to deploy ESS components, updates and virus definitions to the Federal/DoD system, monitor for intrusion detection alerts, etc.

Appendix F: Acronyms

Table 4: Acronym List

Acronym	Definition
A&A	Assessment and Authorization
ACAS	Assured Compliance Assessment Solution
AO	Authorizing Official
ATO	Authorization to Operate
CDR	Critical Design Review
CNSS	Committee on National Security Systems
CSSP	Cybersecurity Service Provider
DATO	Denial Authorization to Operate
DISA	Defense Information Systems Agency
DNS	Domain Name Service
DoD	Department of Defense
DoDAF	Department of Defense Architecture Framework
DoDI	DoD Instruction
eMASS	Enterprise Mission Assurance Support Service
ePO	Electronic Policy Orchestrator
ESS	Endpoint Security Solution
FDDR	Full Deployment Decision Review
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
HBSS	Host-Based Security System
IA	Information Assurance
IT	Information Technology
IWTSD	Irregular Warfare Technical Support Directorate
NIST SP	National Institute for Standards and Technology, Special Publication
NMAP	Network Mapper
OMB	Office of Management and Budget
OV-1	Operational Viewpoint
PDR	Preliminary Design Review
PIT	Platform Information Technology

Acronym	Definition
PK	Public Key
PKI	Public Key Infrastructure
PM	Program Manager
POA&M	Plan of Action and Milestone
POR	Program of Record
RDT&E	Research, Development, Test and Evaluation
RMF	Risk Management Framework
RMF KS	Risk Management Framework Knowledge Service
SAR	Security Assessment Report
SCTM	Security Control Traceability Matrix
SIEM	Security Information and Event Management
SRG	Security Requirements Guideline
SRR	System Requirements Review
SSP	System Security Plan
STIG	Security Technical Implementation Guide
SV-1	Systems Viewpoint
T&E	Test and Evaluation
TRR	Test Readiness Review

Appendix G: Terms & Definitions

Table 5: Terms and Definitions

Terms	Definition
Availability	Ensuring timely and reliable access to and use of information
Common Control Provider	An individual, group, or organization that is responsible for the implementation, assessment, and monitoring of inherited controls.
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information
Integrity	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity
Security Control Traceability Matrix (SCTM)	SCTM lists all of the controls selected for the system as well as additional details on each control, e.g. implementation status, monitoring frequency, etc.