The Department of Defense

Cybersecurity Reciprocity Playbook

Version 1.0
March 2024

DoD Cybersecurity Reciprocity Playbook

The DoD Cybersecurity Reciprocity Playbook is designed to provide clear, credible information on key Department priorities for employing cybersecurity reciprocity in DoD systems, consistent with DoD Instruction (DoDI) 8510.01, *"Risk Management Framework for DoD Systems"* Please contact the Chief, Cybersecurity (CS) Implementation / Risk Management Framework Technical Advisory Group (RMF TAG) Chair on specific matters. *(osd.pentagon.dod-cio.mbx.rmf-tag-secretariat@mail.mil)*

Contents

1. Importance of Cybersecurity 1

1.1 RMF Role in Cybersecurity 1

2. Cybersecurity Activities 3

3. Definition of Reciprocity 3

3.1 Benefits of Leveraging Reciprocity 4

3.2 Risks of Failing to Leverage Reciprocity 5

4. Reciprocity Use Cases 5

4.1. Enterprise – Cloud 5

4.2. Enterprise – ISRMC 6

4.3 Community – Consortium of AOs 10

4.4 One-to-One (Re-use of Artifacts) 12

4.5 DoD and Intelligence Community 15

5. Role of Various Types of AOs in Reciprocity 17

6. Security Configuration Guides & Secure Configurations 18

7. eMASS Reciprocity Search 19

8. List of Enterprise AOs 20

9. DoD CIO Role in Resolving Reciprocity Conflicts 20

10. Conclusion 21

Glossary 22

References 24

1. Importance of Cybersecurity

Cybersecurity is a paramount concern that underpins the nation's ability to safeguard its critical assets, information, and operations in an increasingly interconnected digital landscape. The Department recognizes that malicious cyber activities pose significant threats to national security, economic stability, and public safety. As technology evolves and adversaries become more sophisticated, ensuring the confidentiality, integrity, and availability of sensitive data and systems has become an imperative mission.

1.1 RMF Role in Cybersecurity

The DoD Risk Management Framework (RMF) plays a crucial role in our cybersecurity strategy by providing a comprehensive framework for identifying, assessing, and mitigating cyber risks across the entire spectrum of DoD operations. RMF enables a consistent approach to cybersecurity by establishing a set of processes and guidelines for managing risks associated with applications, systems, and networks which can be tailored based on system/network needs. By adhering to RMF principles, the Department sets the standards and guidelines for Components to categorize assets, implement appropriate security controls, evaluate vulnerabilities, authorize these assets, and continuously monitor and respond to emerging threats.

The significance of RMF lies not only in its ability to bolster the resilience of the Department's digital infrastructure but also in its capacity to promote a proactive and adaptive cybersecurity culture. The framework fosters collaboration among various stakeholders, (e.g., system developers, administrators, and security professionals) ensuring that cybersecurity considerations are integrated from the inception of a system throughout its lifecycle, facilitating the "re-use" of capabilities proven secure within the DoD. As the threat landscape evolves, RMF allows the DoD to make informed risk-based decisions and allocate resources effectively, ultimately enabling the DoD to maintain a robust and effective cybersecurity posture in the face of evolving challenges.

The Federal Risk and Authorization Management Program (FedRAMP) is another way the Department maintains cognizance of its cybersecurity posture. FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring that cloud service providers (CSPs) must follow to gain authorization to work with federal agencies. This is especially important as the Department continues to adopt cloud technologies to modernize its digital infrastructure and operations as it emphasizes security and protection of federal information and helps accelerate the adoption of secure cloud solutions. The DoD can leverage FedRAMP or independently initiate a DoD Provisional Authorization for cloud service offerings (CSOs) that DoD must use. Mission Owners (MOs) must understand the type of data, the authorized impact level, and the conditions outlined in the Provisional authorization when choosing an authorized CSO. Determination of the appropriate Impact Level for a specific mission and mission data will be the responsibility of the mission AO.

- **Impact Level 2 (IL2)** accommodates publicly releasable data or nonpublic unclassified data where the unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. This includes all data cleared for public release as well as some low confidentiality unclassified information **not** designated as Controlled Unclassified Information (CUI) or military/contingency operations mission data, but the information may require some minimal level of access control (e.g., user ID and password). This Impact Level accommodates non-CUI information categorizations based on Committee on National Security Systems Instruction (CNSSI)1253 at moderate Confidentiality, Integrity, and Availability (C-I-A). For noncontrolled unclassified information, Impact Level 2 CSP/CSO customers include whomever the CSP chooses to market the CSO to, which may include government customers, commercial customers, and the public within the same Impact Level 2 cloud environment. Access to CSO at this impact level is via the internet. DoD has reciprocity with FedRAMP for use of CSOs on the FedRAMP Marketplace for all DoD mission systems that process IL2 data.
- **Impact Level 4 (IL4)** accommodates nonpublic, unclassified data where the unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. This encompasses CUI and/or other mission data, including that used in direct support of military or contingency operations. CUI is information the federal government creates or possesses that a law, regulation, or government-wide policy requires, or specifically permits, an agency to handle by means of safeguarding or dissemination controls. Impact Level 4 CSOs may support a U.S. government community or a DOD-only community (i.e., the CSO is DOD Private). Commercial Impact Level 4 CSP/CSO customers include all U.S. government customers (federal, state, local, and tribal) and commercial customers that support them. In some cases, an Impact Level 4 PA may be granted to CSOs that support other commercial entities but not the public.
- **Impact Level 5 (IL5)** accommodates nonpublic, unclassified National Security Systems (NSS) data (i.e., unclassified National Security Information) or nonpublic, unclassified data where the unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. This includes CUI and/or other mission data that may require a higher level of protection than that afforded by Impact Level 4 as deemed necessary by the information owner, public law, or other government regulation. This Impact Level accommodates NSS and CUI information categorizations at High-High-X (H-H-X). Per CNSS Policy (CNSSP) 32, the minimum requirement for all unclassified NSS is equivalent to the FedRAMP High baseline. Impact Level 5 CSOs may support DOD private clouds such as a federal government community or DOD-only community.

- **Impact Level 6 (IL6)** accommodates nonpublic, classified NSS data (i.e., classified National Security Information) or nonpublic, unclassified data where the unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. At this time, only information classified as SECRET or below, in accordance with the applicable executive orders, is permitted to be hosted at this Impact Level. Access to the CSO is via one or more private SIPRNet connections or approved CNSSP 11 circuits.

2. Cybersecurity Activities

Effective monitoring and analysis capabilities, incident response procedures, efficient communication management and control, and timely reporting are critical activities to ensure healthy network operations on which strong network security is built. These cybersecurity activities cannot be oversimplified or ignored for the sake of operational expediency. RMF emphasizes and then requires that such activities be implemented for a capability to obtain an Authorization to Operate (ATO). All systems without an ATO must begin the RMF process, regardless of the system life-cycle stage (e.g., acquisition, operation).

3. Definition of Reciprocity

As defined in the Committee on National Security Systems Instruction (CNSSI) 4009, cybersecurity reciprocity *(*hereinafter referred to as *"reciprocity")* is the "agreement among participating organizations to accept each other's security assessments, to reuse system resources, and/or to accept each other's assessed security posture to share information". During the reciprocity process, Authorizing Officials (AOs) make system authorization decisions by reviewing the body of evidence (BoE). The BoE is the complete set of RMF documentation on the testing, implementation, and assessment of security controls, consisting of the RMF core documents and RMF data elements as defined in Annex C of CNSSI 1254. According to CNSSI 1254, the RMF core documents are the:

1. System Security plan (SSP)
2. Security Assessment Report (SAR)
3. Risk Assessment Report (RAR)
4. Plan of Action and Milestones (POA&M)
5. Authorization Decision Document

DoD CIO issued a memorandum in October 2016 (reference g), reiterating the Department's Cybersecurity Reciprocity policy, as established in DoDI 8510.01, and as implemented by the cybersecurity reciprocity related content pages on the RMF Knowledge Service (KS) (*rmfks.osd.mil/rmf/PolicyandGovernance/Reciprocity/Pages/default.aspx*). The memorandum emphasized that reciprocity is the default for assessment and authorization of a system already deployed in the Department and Components will maximize the use of previous assessment results and authorizations of common information technology systems and software by fellow Department Components in their risk determination and authorization process. Additionally, DoD CIO issued a memorandum in March 2023 (reference j), supporting the reissuance of DoDI 8510.01, which emphasized Components should leverage reciprocity to the greatest extent possible by utilizing a robust BoE.

To improve the use of reciprocity, CIO has emphasized in policy the "re-use" of security testing evidence as the foundation for reciprocity, eliminating and invalidating the practice to issue an authorization decision memo without examining the body of evidence. DoDI 8510.01 states, "The DoD Information Enterprise will use cybersecurity reciprocity to reduce redundant testing, assessing, documenting, and the associated costs in time and resources." By focusing on "re-use", CIO ensures data is provided to Components to enable risk-based decision making, while eliminating duplication of effort.

Reciprocity is **not** a passive acceptance of security assessments, certifications, or authorizations from other entities without careful consideration, and comprehensive review of the context, risk factors, sensitivity of the data, and relevance to the specific systems or networks within its purview. Instead, reciprocity involves a thoughtful, risk-based assessment process and a careful examination of the BoE to determine their applicability and suitability within a specific security landscape.

In essence, reciprocity emphasizes the importance of maintaining a strong security posture while maximizing efficiency through the re-use of the BoE. Thus, reciprocity demands a discerning approach that safeguards the integrity of its systems, while leveraging the insights and efforts of trusted partners to enhance its cybersecurity resilience.

3.1 Benefits of Leveraging Reciprocity

Reciprocity is designed to expedite authorization through the re-use of assessments and artifacts, which leads to cost reduction. Executed appropriately, reciprocity reduces redundant testing, assessment and documentation, and the associated costs in time and resources.

To support reciprocity, DoD Components share security authorization packages with affected information owners and interconnected system owners. The re-use of artifacts allows AOs to accept assessments done on systems they intend to deploy rather than repeat the assessments. Acceptance of relevant artifacts from similar assessments results in fewer costly assessments, allowing systems to be authorized more quickly and efficiently.

In some cases, an organization may want to deploy a capability developed by another organization. It can leverage the existing authorization package if both organizations have similar mission requirements and plan to deploy the same system components with similar dataflows and network architectures. In these cases, the Receiving organization becomes the system owner and, while not needing to re-authorize the system, it must issue an authorization to use (ATU). This ATU includes a statement by the Receiving AO granting approval for a Granting system to connect to the hosting/receiving system where the systems are linked through inheritance in the RMF Inventory Tool (e.g., eMASS, Xacta). It also provides a copy of implementing documentation to the Granting AO and notifies and provides guidance to subordinate site(s) that the system is authorized to operate and/or connect only in the authorized configuration. Overall, this re-use can result in significant resource savings.

3.2 Risks of Failing to Leverage Reciprocity

Failing to leverage reciprocity to the greatest extent possible can lead to redundant and resource-intensive efforts. Without recognizing the assessments conducted by other entities, the organization might be compelled to undertake its own comprehensive evaluations of systems and networks, even when similar assessments have already been performed by trusted partners. This results in a wasteful allocation of time, manpower, and financial resources, hindering the organization’s ability to efficiently manage and enhance its cybersecurity posture.

Moreover, the lack of reciprocity undermines interagency collaboration and information sharing. In an era characterized by the rapid evolution of cyber threats, the ability to quickly share cybersecurity insights and findings across different government agencies and organizations is critical. Reciprocity fosters a culture of cooperation and trust, enabling the Department to benefit from the expertise and perspectives of other entities, thereby enhancing its ability to detect, prevent, and respond to emerging threats effectively.

Not leveraging reciprocity hampers resource optimization and hinders collaborative efforts. Embracing reciprocity promotes efficiency, interagency cooperation, and information sharing, thereby contributing to a stronger and more robust cybersecurity posture that aligns with the evolving threat landscape.

4. Reciprocity Use Cases

The following use cases do not represent all possible reciprocity circumstances. The cases in sections 4.1 through 4.5 demonstrate how reciprocity is leveraged across the Department in some of the most common applications.

4.1. Enterprise – Cloud

A CSP with a service offering already approved by FedRAMP at the moderate baseline is eligible for use under reciprocity by the DoD for public data. To obtain the BoE for review, the MO must submit a FedRAMP Package Access Request form at: https://www.fedramp.gov/assets/resources/documents/Agency_Package_Request_Form.pdf.

For data categorized at IL4/5/6, DoD issues a PA. The security authorization package and inheritance is made available in the Enterprise Mission Assurance Support System (eMASS) for MOs to leverage when obtaining their department's ATOs.

- For IL4 and IL5, MOs inherit security controls from eMASS for CSOs and use the SSP and Security Requirements Traceability Matrix (SRTM) to understand control implementation guidance (inherited, hybrid or fully on MOs) and assess additional security controls based on MO's need for awarding an ATO.
- For IL2 (Public Data), the DISA AO issued a reciprocity memo for CSOs assessed, authorized, and listed in the FedRAMP marketplace at a minimum of the FedRAMP moderate Baseline. If that IL2 needs be uplifted to IL4/5, a DoD Sponsor must utilize the DoD Cloud Authorization Services (DCAS) SharePoint page: *https://dod365.sharepoint-mil.us/sites/DISA-RE-Apps/cas/SitePages/CASHome.aspx* to request DISA to begin the Cloud Authorization Process.
- All DoD PAs for authorized CSOs, including the DISA Memorandum on IL2 Reciprocity (reference k), can be found on DCAS.

4.2. Enterprise – ISRMC

The DoD Information Security Risk Management Committee (ISRMC) is a cross-functional committee responsible for overseeing the Enterprise risk management process for DoD systems and networks and one of the key stakeholders responsible for executing and supporting reciprocity for an enterprise system.

An "Enterprise system" is designed to satisfy a DoD-wide requirement and is deployed to multiple DoD Components across the DoD Information Enterprise. The following activities describe how to achieve reciprocity when a DoD Component deploys an Enterprise system (i.e., major application):

4.2.1 Granting Organization Activities

a. Initiate the security authorization package.

b. Provide the Defense Security/Cybersecurity Authorization Working Group (DSAWG), through the organization's DSAWG Representative, an electronic copy of the SSP, SAR, RAR, the System POA&M, Authorization Decision Document, and list of deployment sites and projected deployment dates.

(1) Granting AOs must also provide the complete security authorization package and body of evidence to Receiving AOs.

(2) Program managers (PMs) and system owners – who deploy systems across multiple DoD Components – can accomplish this sharing by posting security authorization documentation and the associated body of evidence to eMASS or

other automated assessment and authorization tools to provide visibility of authorization status and documentation to planned Receiving sites.

a. For organizations inheriting from incompatible or interoperable record keeping systems, or RMF inventory tools, the "manual inheritance" capability will be utilized.

c. This information sharing ensures all parties involved have visibility of the system's security artifacts and documentation.

(1) Granting systems with valid authorizations (from a DoD organization or other U.S. Government agency) into Receiving organizations may affect the security posture of the Receiving organization. Receiving organizations must review the Granting system's authorization and POA&M to ensure mitigations that reduce residual risk can be applied in the Receiving organization. The Receiving organization would request read-only access to the Granting system's authorization record, as no additional validation or verification testing is required.

(2) Configuration differences, introduced by using the system in a new or different environment, require additional testing.

a. If a baseline is changed, the local AO must authorize the new configuration based on additional testing.

(3) System owners and PMs from Granting organizations must coordinate system security requirements with Receiving organizations' representatives early and throughout system development.

d. Provide authorization status briefs to the DSAWG, as requested.

e. In coordination with the Receiving organization, ensure security assessments address any and all additional Receiving organization security controls or requested adjustments to the assigned security controls identified during DSAWG security reviews.

f. Ensure the Enterprise system complies with Information Assurance Vulnerability Management (IAVM) Program directions and operational orders issued by Joint Force Headquarters - Department of Defense Information Network (JFHQ-DODIN)

g. Register the Enterprise system in the DoD Ports, Protocols, and Services Management (PPSM) Registry.

h. Brief the ISRMC for approval or disapproval of the Enterprise system no later than 60 business days prior to the planned deployment.

   (1) If approved by the ISRMC, the Granting AO can issue an ATO for the Enterprise system and the version being deployed.

   (2) If disapproved by the ISRMC, the Granting AO must work with the DSAWG to adjust the Enterprise system, as needed, to comply with ISRMC guidance so it can receive an ATO.

i. Provide installation and configuration requirements documents to Receiving AOs prior to the Enterprise system deployment. This must include all applicable DoD Security Technical Implementation Guides (STIGs).

4.2.2 ISRMC Activities

a. Approve or disapprove the Enterprise system connection based on the DSAWG recommendation and other factors identified during the Granting organization's decision briefing.

b. If approved, the ISRMC will monitor the acceptability of the residual risk for organizations receiving the Enterprise system at Component sites and authorize connection to the DoD Information Network (DoDIN). Any change in acceptability of risk that cannot be mitigated will require a re-boarding at the ISRMC.

   (1) The Receiving organization would use the ISRMC risk acceptance as an RMF artifact to approve the change request in adding the Enterprise Capability into their system authorization record.

c. If disapproved, the ISRMC provides guidance through the DSAWG to the Granting organization on actions and mitigations that will result in an approval to connect to the DoDIN.

d. The ISRMC will not grant its approval until the Granting organization documents and mitigates any remaining risks, as directed by the ISRMC, in the Enterprise system POA&M.

4.2.3 Receiving Organization Activities

a. Maintain situational awareness of the Granting Enterprise system assessment activities via eMASS or other automated tools.

b. Make the system(s) security authorization package available to the Granting organization.

c. Determine the security impact of connecting the Granting Enterprise system within the Receiving system and use their DSAWG representative to identify issues that may preclude the system from connecting, such as requests for adjustments to the assigned security controls or requirements for additional controls.

d. Test security controls, as appropriate.

   (1) The Receiving organization must review the controls and the deployment guide to ensure that the local security posture meets the deployment conditions and implement inherited controls and deploy the system in accordance with (IAW) the deployment guide.

   (2) Security controls that are built into the system must not change when the system is deployed and do not need to be re-tested.

   (3) The Receiving organization must establish inheritance for the hybrid controls, providing supporting evidence to support implementation within the Receiving system.

e. Augment any security controls required for deploying the Enterprise system to a Receiving site.

   (1) The authorization documentation for the systems receiving/hosting the Enterprise system will be updated, as required.

   (2) This includes any installation and configuration requirement documents provided by the Granting organization and testing results of any configuration differences, if needed.

f. Execute a documented agreement with the Granting organization, such as a Memorandum of Understanding (MOU), Memorandum of Agreement (MOA), or Service Level Agreement (SLA), for maintaining and monitoring the system's security posture, including the system's security controls and cybersecurity service provider (CSSP). At a minimum, the agreement document must address: operating constraints, operation environment, monitoring requirements, security maintenance, vulnerability scanning, IAVM compliance, lifecycle replacement of software and components, and roles and responsibilities.

g. Issue a formal authorization to use and operate the Enterprise system. Not a new ATO, this determination includes a statement by the Receiving AO granting approval for a Granting system to connect to the Receiving system.

    (1) This “ATU” differs from the authorization issued by DISA for connection to the DISN. This “authorization to use” formally incorporates the Granting system into the Receiving system.

    (2) However, if multiple systems are reused but separately owned, managed, and maintained by different organizations, they are considered isolated instances and require separate authorizations. In these cases, Receiving organizations can use available completed test and assessment results to the greatest extent possible.

    (3) The Receiving AO provides a copy of implementing documentation, such as the “ATU”, to the Granting AO.

    (4) The Receiving AO will notify subordinate sites that the Granting Enterprise system (i.e., major application) is authorized to operate or connect to the Receiving organization’s systems, but only in the authorized configuration found in the updated system’s ATO documentation.

h. Update system authorization and connection documentation to reflect the incorporation and connection of the Enterprise systems.

i. Ensure all parts of the Receiving organization implement major application installation guidance and applicable DoD security configuration requirements.

j. Implement and maintain mitigations identified in the Granting Enterprise systems’ POA&M.

In summary, the execution of Enterprise reciprocity is a collaborative effort. Each party has distinct responsibilities, and this cooperative approach ensures that cybersecurity assessments and authorizations within the DoD are efficient and aligned while maintaining the security and integrity of the systems involved.

4.3 Community – Consortium of AOs

To address the challenge of reciprocity in complex authorization environments such as many of the DoD capabilities (e.g., Weapon Systems, Enterprise Systems, Clouds, DevSecOps, Coalition environments, Cross service environments, etc.), where there are multiple stakeholders and AOs involved, an AO Consortium (hereinafter referred to as an “AO

Committee") method was established as a tool to streamline the assessment and authorization process while maintaining a high level of security assurance.

The main objective of the AO Committee is to provide a mechanism for all stakeholders with authorization equity to have insight to the risk posture of the system, to participate in the ongoing assessments and to have awareness of the Continuous Monitoring (CONMON) and priorities established by the system/capability AO, which allow the identification and adjudication of any reciprocity challenges early as part of the continuous assessment and authorization process of the system/capability. The AO Committee provides the forum and structure to allow all authorization stakeholders the ability to participate in, understand, and trust the risk assessment of the system AO and the ability to correlate that to their risk tolerance, and their environment, achieving reciprocity as an outcome.

The committee of AOs would outline an interconnection service agreement (ISA); defining the relationships; roles and responsibilities, steps to address gaps between authorization boundaries and/or enterprise services, PPSM coordination, CSSP identification, incident response, and agreement review requirements to address later changes in technology and authorization statuses.

The following are the outcomes of utilizing an AO Committee to leverage reciprocity:

Outcome 1

- Allow all stakeholders a structured way to evaluate systems coming into their authorization boundary to participate in the development of the risk assessment of the system/capability.
- Understand the environment for the agreement being worked, as well as the assumptions and constraints.
- Work through the agreements and handoffs required between environments.
- Encourage AO-to-AO level communications.
  - This leads to:
    - Increased confidence and trust between the Authorization stakeholders, allowing increased ability to achieve reciprocity.
    - A tangential benefit of getting past the narrow view of compliance to artifacts and allowing focus on the intent and risk management objectives.

Outcome 2

- Provide a mechanism to track the visibility of actions between AOs and boundaries to form Government-to-Government collaborations and focus priorities of efforts across the authorization community toward the integrated efforts of the cyber security community.

  - AO Committees allow a simple way for actions and items to be addressed, adjudicated, and worked at the principal level in ways that would normally take longer.

Outcome 3

- When the Test communities (Director, Operational Test & Evaluation (DOT&E) and Operational Test & Evaluation (OT&E)) are involved in the AO Committee, it helps integrate the assessments done by all parties into a more holistic input for the AO to consider in rendering their determination.
- By partnering with the Test communities, AOs and system owners can be more proactive to assess the risk posture over time, as the findings and analysis are a valued part of the continuous assessing and authorizing approach and prioritization of mitigations.
  - This integration and collaboration leads to:
    - Increased confidence in the risk posture and assurance of the systems/capabilities.
    - Forged collaborations between the AOs.
    - Increased confidence in the assurance that the higher priority risks, given the operational context and risk tolerance are prioritized in a way that is supported by analytics of findings, vice compliance alone.

Overall, the Department's use of reciprocity within an AO Committee enhances efficiency, reduces redundancy, and promotes collaboration among various Components while maintaining a consistent and robust security posture across the entire system.

4.4 One-to-One (Re-use of Artifacts)

The responsibility for executing reciprocity in a one-to-one scenario (re-use of artifacts) is shared among various stakeholders. The Department recognizes that leveraging reciprocity through the re-use of cybersecurity artifacts can enhance efficiency and streamline the assessment process. In this scenario, the primary responsibility falls on both the Granting and Receiving organization involved in the artifact exchange. The following process steps detail the responsibilities of both organizations:

Prior to entering into a reciprocity agreement, both Receiving and Granting organizations need to complete several tasks. These tasks may include:

- Identifying who is responsible for providing the resources (e.g., funding, hardware, software, lifecycle replacement of system component, and personnel) required to manage and operate the system.
- Verifying compliance and maintenance of the reciprocity authorization by the Granting organization.

- Ensuring the Receiving organization implements the appropriate security controls required by the authorization package and applies mitigation strategies as directed by the Granting organization's POA&M.
- Ensuring the interconnected systems are not adversely affected by new (or aggregated) vulnerabilities.
- Verifying and maintain the correct configuration.
- Ensuring all stakeholders have access to the complete security authorization package, including configuration specifications.
- Formally documenting all tasks that must be completed and the associated responsible organization, as the result of agreement between the Granting and Receiving organizations.

4.4.1 Responsibilities of Granting Organization

- Provide the security authorization package and deployment instructions (or access to it), including a current POA&M, to Receiving organizations.
- Communicate all changes to the system during its lifecycle, such as version updates, to Receiving organizations.
- Notify Receiving organizations of any new findings, such as new threats, discovered vulnerabilities, or similar information, throughout the authorization life cycle.
- Gather requirements from potential leveraging organizations before developing the system to ensure the widest use of a standardized configuration and avoid modifications driving separate authorizations.
- Provide a point of contact (POC) to Receiving organizations requesting information.
- Notify Receiving organizations at least six months prior to any reauthorization events to ensure consideration of any input from Receiving organizations. (Acknowledgment of receipt required by impacted organizations).
- Notify Receiving organizations of any plans that may affect their use of the system, such as decommissioning or version changes. (Acknowledgement of receipt required by impacted organizations).
- Identify factors or conditions justifying termination of the MOU/MOA.
- Communicate and provide patches and updates in accordance with DoD and USCYBERCOM requirements and timelines, maintain the Enterprise Capability authorization baseline within the established DoD and USCYBERCOM timelines.
- Maintain deployment locations of the system within the Granting organizational authorization tracking tool.
- Ensure assignment of a JFHQ-DODIN accredited CSSP to maintain continuous monitoring, patch management, the IAVM Program, End Point Security Services (ESS) monitoring, Security Information and Event Management (SIEM)

monitoring, operational orders, POA&Ms, annual reviews, and quarterly or monthly reviews of authorized systems.

4.4.2 Responsibilities of Receiving Organization

- Request Security Authorization Package and deployment instructions (or access to it), including a current POA&M, from the Granting organization.
- Review the Granting organization AO's authorization decision and work with the Granting organization to implement the Enterprise Capability with any required mitigations.
- Deploy the system using configuration requirements in the security authorization package and deployment instructions.
- Provide all inherited security controls, mitigations, or support functions required by the reciprocity authorization.
- Obtain any necessary authorization to connect and operate the system within the organization's network.
- Provide a single POC to Granting organizations.
- Update necessary authorization tracking tools within the organization.
- Implement required patches and changes in accordance with Project Management (PM) guidance.
- Notify Granting organizations of any new findings, such as new threats, discovered vulnerabilities, or similar information throughout the authorization life cycle.
- Implement mitigations in accordance with the Granting Information Technology Security POA&M.
- Maintain the Enterprise Capability baseline by applying IAVAs and STIGs as new guidance is released, updating the POAM for any updates or configurations that cannot be applied.

Note: Additional testing may be required to satisfy all RMF requirements. However, systems must re-use existing security testing and assessment results to the greatest extent possible and the Granting and Receiving organizations must agree to all changes or additions to agreements in writing.

4.4.3 Change Management

All organizations must identify technical POCs as part of their MOU, MOA, or SLA to support the management and operation of the authorized system. Organizations must communicate to the PM and original AO any event that may affect the security posture of the authorized system or the installed environment. Agreements must include processes, timing, and notification requirements. Examples of events requiring notification include:

- Security incidents

- Disasters and other contingencies
- Material changes to system configuration, such as quarterly STIG releases
- Personnel changes in critical positions
- New user types, such as Foreign Nationals
- Changes to the operating environment (such as a facility once cleared for open storage no longer having such clearance)
- When the network the system is connected to is given a Denial of Authorization to Operate (DATO)
- IAVM program reporting
- Lifecycle Replacement requirements (such as an operating system or equipment firmware no longer supported by the vendor)
- Changes to Enterprise Tools or Capabilities (such as migration to a new ESS anti-virus tool)

Ultimately, successful execution of reciprocity in a one-to-one scenario (re-use of artifacts) hinges on collaboration, transparency, and a mutual commitment to cybersecurity best practices. Both the Granting and Receiving organizations play vital roles in upholding the integrity of the artifacts and ensuring that the security posture of the systems involved remains robust and aligned with the Department's cybersecurity objectives.

4.5 DoD and Intelligence Community

Both DoDI 8510.01 and Intelligence Community Directive (ICD) 503 emphasize the context of reciprocity for assessment only and acknowledge the needed testing for configuration changes that arise from the movement of capabilities.

DoDI 8510.01, the RMF KS, and ICD 503 align to assert the following regarding reciprocity:

a. Components of the DoD and IC will make appropriate authorization decision documentation available to other IC elements, to the non-IC parts of the DoD (i.e., Military Departments, Combatant Commands and Defense Agencies), and to non-IC agencies of the Federal Government.
b. Authorizing Officials of DoD and IC Components will make appropriate security assessment documentation of a system available to other IC elements, to the non-IC parts of the DoD, and to other non-IC agencies of the Federal Government.
c. DoD and IC Components will accept the security assessment of a system by another Component without requiring or requesting any additional validation or verification testing of the system with the following caveats.

i. Components of the DoD and the IC will test only the configuration differences introduced by using the system in a new or different environment.

ii. AOs and Authorizing Official Designated Representatives (AODRs) of DoD and IC Receiving organization will consider the Granting organization's security assessment when making the authorization decision for placing a system into operation as a new or additional part of any system for which the AO or AODR exercises authorization authority.

iii. Additional consideration must be given to Security Control Overlays (e.g., Intelligence A (INT-A), INT-B, INT-C, Cross Domain Transfer Cross Domain, Cross Domain Access, Privacy, etc.)

4.5.1 Body of Evidence Sharing

IC and DoD agencies utilize one of only a few major RMF inventory tool suites to manage their RMF documentation (e.g., eMASS, Xacta). These tools grant each agency the ability to customize their workflows, essential elements of information, and policy mappings captured within its RMF implementation.

The IC released the Extensible Markup Language (XML) Data Encoding Specification for Body of Evidence (BOE.XML) as a standard for the way the BoE is stored within RMF inventory tools. This specification has been closely aligned with CNSSI 1254 and associated policies to facilitate this exchange and is intended to provide the data fields that are necessary to capture and convey the relevant information that would be used to facilitate the acceptance and reciprocity of established systems and their security authorizations.

When sharing a BOE, each IC and DoD AO and Chief Information Security Officer (CISO) understands the technological complexity, cybersecurity strengths and weaknesses, and mission critical portions of their IT enterprise. Each AO must decide the right balance of cybersecurity risk against the need to execute critical mission at any point in time. As such, there are several overall cybersecurity risk items that may vary amongst agencies and must be considered before a decision on authorization for a reciprocal capability is rendered.

To facilitate the exchange of BoE for reciprocity, the DoD and IC worked together to establish the following initiatives:

- Alignment to the BOE.XML specification across all DOD and IC systems to simplify ease of sharing amongst RMF system of record tools.

- Establishment of centralized access to RMF BoE by CISO organizations for Services of Common Concern (SoCC), Programs of Record, or community wide service providers (e.g., Commercial Cloud Enterprise (C2E)).
- Use of Security Content Automation Protocol (SCAP) protocols within automated and manual assessment activities (e.g., Open Vulnerability and Assessment Language (OVAL), Open Checklist Interactive Language (OCIL), Extensible Configuration Checklist Description Format (XCCDF), etc.) as well their use within Commercial off the Shelf (COTS) RMF support tools.

5. Role of Various Types of AOs in Reciprocity

To maintain the narrowest scope, we identified that with reciprocity, there are two types of AOs – *'Granting' or 'Receiving',* as outlined in the "Reciprocity MOA MOU" template (available on the related reciprocity pages on the RMF KS) which provides the guidelines to be applied as the basis for practicing reciprocity, in accordance with Department of Defense Instruction (DoDI) 8510.01, *Risk Management Framework for DoD Systems*, 19 July 2022.

The default option is for Components to use each system/application in its native environment. This use case will be referred to as "co-use" and will only require authorization by the Granting organization. Granting organization are responsible for establishing notification processes (e.g., cybersecurity incidents, PII breaches, etc.) for co-use systems, applications, and cloud services. When an authorized, operational system and/or application in one environment is designated for install and use in another environment, cybersecurity reciprocity will be the default method for assessment and authorization by the Receiving organization.

Prior to initiating testing or a risk assessment for a system to be hosted in the Receiving organization's environment, the *Receiving AO* is responsible for determining whether the system has been authorized by another AO. If a current authorization exists, the *Receiving AO* and SCA will proceed with reciprocity based on RMF documentation required by DoDI 8510.01.

When the specific documents required by DoDI 8510.01 are not available, the *Receiving AO* must consider the body of evidence available from the Program Office or system owner, to include, but not limited to the following information:

- The Enterprise Capability POA&M, listing the open vulnerabilities, justification, and residual risk.
- Residual risk assessment for each "High" or "Very High" risk vulnerability
- The authorization boundary diagram sometimes referred to as the network. diagram, depicting the Defense-in-depth security architecture for the platform (building, ship, Humvee, command center, etc.) and enclave.
- Data-flow diagrams, interface diagrams and cross-domain interfaces that specify type of interface, direction of data flow, and any in-line security solutions.

- Impact and technical justification for any “High” or “Very High” risk vulnerabilities that remain.
- IAVM plan, Continuity of Operations Plan (COOP), Disaster Recovery Plan, and incident management plans.
- Hardware and software lists, with the associated STIG checklists.
- Validation or verification test results.

Requests for documentation not included in the Granting organization’s RMF package must be endorsed by the requesting Component CISO, or equivalent, before being forwarded to the *Receiving AO.*

The *Granting AO* will ensure documentation providing the body of evidence is freely shared with the Receiving organization.

The Receiving organization becomes responsible for establishing and maintaining a full authorization if it continues using any system, application, or cloud service that is no longer supported by the Granting organization.

6. Security Configuration Guides & Secure Configurations

Within the Department, secure configuration guides take various forms, such as STIGs and Security Requirement Guides (SRGs). These guides offer detailed step-by-step instructions for securing specific technologies, platforms, and environments, ranging from operating systems and applications to cloud services. By following these guides, Components establish a consistent baseline security posture, reducing the attack surface and potential vulnerabilities that adversaries could exploit.

These guides facilitate reciprocity by providing standardized and approved security configurations. When a system adheres to the recommended settings outlined in these guides, it becomes easier for other Components to trust the security of that system, accelerating the authorization and deployment process. This not only streamlines operations but also enhances the overall security posture of the DoD by maintaining a consistent level of security across the enterprise.

While the SRGs define the high-level requirements for various technology families and organizations, STIGs are the detailed guidelines for specific products. STIGs provide product-specific information for validating, attaining, and continuously maintaining compliance with requirements defined in the SRG for that product’s technology area. The security requirements contained within the SRGs and STIGs, in general, are applicable to and required by all DoD-administered systems, all systems connected to DoD networks, and all systems operated and/or administrated on behalf of the DoD. This requirement remains in force for all mission owners building systems in a cloud service.

In the case of cloud service, where CSP systems must comply with configuration guidance consistent with the National Institute of Standards and Technology Special Publication (NIST SP) 800-53 security control "CM-6 Configuration Settings" by using STIGs/SRGs. Secure configuration guides, such as the Cloud Computing SRG, play an essential role in ensuring that cloud deployments align with DoD cloud security requirements. As the Department increasingly leverages cloud technologies, these guides offer a roadmap for configuring cloud resources, addressing shared security responsibilities, and meeting compliance standards. By adopting secure configurations outlined in these guides, the Department can confidently extend its reciprocity to CSOs, fostering a secure and agile cloud environment that supports its mission-critical operations.

7. eMASS Reciprocity Search

Certain capabilities exist within eMASS to support reciprocity activities across Federal Organizations. Among these capabilities is the eMASS "Reciprocity" user role, which grants a set number of reciprocity users per eMASS instance—to be appointed by an Organization-defined Enterprise role (e.g., AO, CISO, CIO)— access to the eMASS reciprocity search function, allowing them to find reciprocity systems more easily. Reciprocity users can utilize this function to search across eMASS for the re-use and acceptance of systems that have an existing RMF assessment and authorization by another Organization. The eMASS Reciprocity Job Aid *(https://rmfks.osd.mil/rmf/HelpandResources/References/Reference%20Library/eMASS_Reciprocity_Job_Aid.pdf)* is intended to assist a Reciprocity user in searching for and viewing System security assessments located in any eMASS instance.

Accordingly, the "Interagency Partners" capability is intended to provide better support for these cases of collaboration or information sharing efforts. Organizations, via their eMASS System Administrators and Organization System Administrator, can identify and grant the Interagency Partner (IP) role to their users as appropriate. The Interagency Partner role appears as an "Additional" role that can be granted to a user's account. The eMASS Interagency Partner Job Aid (*https://rmfks.osd.mil/rmf/HelpandResources/References/Reference%20Library/eMASS_InteragencyPartner_Job_Aid.pdf)* is intended to assist an Interagency Partner user in searching for and viewing System security assessments located in external eMASS instances.

By default, all new records are listed as reciprocity systems when registering. Users must list a reciprocity exemption justification if the option is deselected. Systems can also be designated as a reciprocity system at any time through the "System Information" page. Systems that are enabled for reciprocity will be visible to certain users across the various eMASS instances.

Reciprocity users can search for systems with reciprocity enabled using the "Search Reciprocity Systems" hyperlink on the eMASS homepage. After entering search criteria and searching for systems, eMASS will display the results and list all available systems and their associated organizations. (*Systems will not appear in search results if they are decommissioned, have a DATO authorization status, or have opted-out of the eMASS reciprocity capability.)*

Once a system is selected, users will have view-only access to system information, security control assessments, POA&M items, artifacts, and system-level reports. This feature is designed to allow users to find similar systems and utilize their existing RMF assessments more easily. For more detailed information on eMASS capabilities, please refer to the eMASS Functionality guide (*https://rmfks.osd.mil/rmf/HelpandResources/References/Reference%20Library/eMASS_Functionality_Guide.pdf*).

8. List of Enterprise AOs

The full list of Enterprise AOs will be made available on the RMF KS site (*https://rmfks.osd.mil/rmf/PolicyandGovernance/RMFRoles/Pages/RoleDirectory.aspx*) and it will also be uploaded to the "Help" section in eMASS.

9. DoD CIO Role in Resolving Reciprocity Conflicts

The Deputy Secretary of Defense (DSD) issued a memorandum in March 2024 (reference i), emphasizing the importance of a culture of collaboration in cybersecurity testing and reciprocity in order to accelerate delivery of innovative capabilities while maintaining our cybersecurity standards. The DSD expects testing re-use and reciprocity to be implemented except when the cybersecurity risk is proven to be too great.

In a collaborative cybersecurity reciprocity culture, AOs trust one another and are inclined to granting reciprocity, thereby accepting the risk determination to deploy a capability made by another AO unless there are compelling operational and procedural reasons that prevent the risk acceptance (i.e., to refuse reciprocity). Therefore, the Receiving AO should make every attempt to accept the risk determination made by the Granting AO. However, before making the decision, Receiving AOs must thoroughly review the security authorization package provided by the Granting AO, focusing on content and not the organization or format. The content should clearly demonstrate the security posture, risk assessment, and rationale for the risk determination.

Receiving AOs have the right to refuse participating in reciprocity with another organization due to insufficient content demonstrating an informed understanding of the security posture, risk assessment of the system, and the rationale for the risk determination as defined on the RMF KS, or due to excessive risk to the enclave or site, as determined by the site AO. However, the Receiving AO must document and report this refusal to the Granting organization's AO within 10 business days. If a refusal does occur, both organizations will continue to work, and re-work, the ATO package to reach an agreement, if at all possible. When AOs cannot reach an agreement to leverage re-use and reciprocity, both parties must use the following resolution process to gain assistance in resolving the impasse:

1. If a conflict arises, due to reciprocity refusal there should be an attempt to resolve it at the AO level. This could include, but not limited to, the Granting AO conducting new assessments.

2. If the conflict cannot be resolved at the AO level, the RMF TAG Secretariat will be notified and the RMF TAG Chair will attempt to mediate the dispute as appropriate.

3. If the RMF TAG Chair cannot reach a resolution, the issue will be taken to the AO Council, chaired by the DoD CISO, who will serve as a mediator for the dispute.

In addition to potentially mediating conflicts, DoD CIO plays a strategic role in shaping reciprocity policies and frameworks. This includes advocating for standardized processes, fostering the adoption of best practices, and championing the importance of leveraging trusted assessments from other agencies or entities. By providing strategic direction and promoting a cohesive approach to reciprocity, DoD CIO contributes significantly to the organization's overall cybersecurity resilience and effectiveness in an increasingly complex threat landscape.

10. Conclusion

In conclusion, this playbook serves as an invaluable starting point for organizations seeking to navigate the intricate landscape of cybersecurity reciprocity. However, recognizing the dynamic nature of the cybersecurity landscape, we encourage continuous improvement and collaboration. Therefore, should you identify areas for enhancement or have innovative ideas to contribute to the playbook, we invite you to engage with the RMF TAG Secretariat (*osd.pentagon.dod-cio.mbx.rmf-tag-secretariat@mail.mil*). Through this ongoing dialogue and collective efforts, we can continue to fortify our defenses and employ cybersecurity reciprocity in DoD systems.

GLOSSARY

ACRONYMS

Acronym	***Meaning***
3PAO	third party assessment organization
AO	authorizing official
AODR	authorizing official designated representative
ATO	authorization to operate
ATU	authorization to use
BOE	body of evidence
CIO	chief information officer
CISO	chief information security officer
CNSSI	Committee on National Security Systems Instruction
CNSSP	Committee on National Security Systems Policy
CSO	cloud service offering
CSP	cloud service provider
CSSP	cybersecurity service provider
CUI	controlled unclassified information
DATO	denial of authorization to operate
DISA	Defense Information Systems Agency
DoD ISRMC	DoD Information Security Risk Management Committee
DoDI	DoD Instruction
DSAWG	Defense Security/Cybersecurity Authorization Working Group
eMASS	Enterprise Mission Assurance Support Service
FedRAMP	Federal Risk and Authorization Management Program
IAVM	Information Assurance Vulnerability Management
IL	impact level
JAB	Joint Authorization Board
JFHQ-DODIN	Joint Force Headquarters-Department of Defense Information Network

Acronym	*Meaning*
KS	knowledge service (RMF)
MO	mission owner
MOA	memorandum of agreement
MOU	memorandum of understanding
NIST	National Institute of Standards and Technology
NSS	National Security System
PA	provisional authorization
PAO	principal authorizing official
P-ATO	provisional authority to operate
POA&M	plans of action and milestones
PM	program manager
POC	point of contact
RAR	risk assessment report
RMF	risk management framework (for DoD systems)
SAR	security assessment report
SCA	security control assessor
SCA-R	security control assessor-representative
SP	special publication
SRG	security requirements guide
SRTM	security requirements traceability matrix
SSP	system security plan
STIG	security technical implementation guide
TAG	Technical Advisory Group (RMF)
USCYBERCOM	United States Cyber Command

REFERENCES

a. Committee on National Security Systems Instruction Number 4009, *"Committee on National*
b. *Security Systems (CNSS) Glossary,"* March 2, 2022
c. Committee on National Security Systems Instruction Number 1254, "*Risk Management Framework Documentation, Data Element Standards, and Reciprocity Process for National Security System"* August 2016
d. Department of Defense Cybersecurity Resource and Reference Guide, 28 February 2022
e. Department of Defense Instruction (DoDI) 8510.01, *Risk Management Framework for DoD Systems,* 19 July 2022
f. Department of Defense Manual (DoDM) 8530.01, *Cybersecurity Activities Support Procedures,* 31 May 2023
g. Department of Defense Memorandum, *Cybersecurity Reciprocity*, 18 October 2016
h. Department of Defense Memorandum, *DoD Information System Certification and Accreditation Reciprocity,* July 2009
i. Department of Defense Memorandum, *Resolving Risk Management Framework and Cybersecurity Reciprocity Issues*, March 2024
j. Department of Defense Memorandum, *Supporting Guidance on the Reissuance of DoD Instruction (DoDI) 8510.01*, "*Risk Management Framework (RMF) for DoD Systems"*, 29 March 2023
k. DISA Memorandum, *Department of Defense (DoD) Memorandum of Reciprocity for FedRAMP Authorized Moderate Baseline Cloud Service Offerings (CSO) at Impact Level 2 (IL2)*, 15 August 2019
l. Intelligence Community Directive Number 503, *Intelligence Community Information Technology Systems Security Risk Management,* 21 July 2015
m. National Institute of Standards and Technology Special Publication 800-53*, "Security and Privacy Controls for Information Systems and Organizations,"* December 10, 2020