DoD RMF Reciprocity:

Authorizations, Not Software

Correcting a Persistent Misinterpretation of Authorization Reciprocity

Author: Karen Cummings, Raven Solutions Chief Security Officer, PMP, CISSP-ISSMP, CCSP

A B S T R A C T

Reciprocity under the DoD Risk Management Framework (RMF) is a well-established mechanism for reducing redundant security assessments. When properly applied, it streamlines the authorization process and promotes use of vetted enterprise solutions. However, a persistent and systemic misinterpretation has taken root across the DoD enterprise: that an existing Authorization to Operate (ATO) for a commercial software product can be reused by any organization deploying that same software product in a different environment. This paper clarifies the correct scope of reciprocity, identifies where and why the misinterpretation occurs, and distinguishes reciprocity from the related but separate practice of security artifact reuse. Intended for cybersecurity practitioners, program managers, and authorizing officials across the DoD, this paper aims to enable defensible, policy-consistent authorization decisions.

1. Background and Purpose

The DoD Risk Management Framework, governed by DoDI 8510.01, provides a structured process for managing cybersecurity risk across information systems. Central to the RMF is the Authorization to Operate, a formal risk acceptance decision issued by a designated Authorizing Official (AO) based on the results of security categorization, control selection, implementation, assessment, and authorization activities.

Reciprocity, as defined within the RMF, permits an organization to accept the security assessment results and authorization of another system or service, avoiding the need to repeat evaluation activities when the security posture has already been rigorously established. This mechanism promotes efficiency, reduces duplicative workload, and supports the DoD's broader goal of enterprise-level security consistency.

Despite its clear intent, a recurring and consequential misinterpretation of reciprocity has become embedded in how authorization decisions are understood and communicated across many programs and installations. This paper addresses that misinterpretation directly: reciprocity applies to authorization decisions at the system level - not to software products.

2. What Reciprocity Is — and What It Is Not

2.1 The Correct Understanding

Reciprocity allows an organization to leverage an existing ATO when it is consuming, inheriting, or operating within an already-authorized capability without materially altering its risk posture. In these situations, the foundational conditions of the original authorization remain intact: the system boundary, hosting environment, architecture, configuration, data types, and control implementations are substantively unchanged. The original AO's risk acceptance remains valid and applicable.

Appropriate applications of reciprocity include:

- Consuming a centrally authorized enterprise shared service without modifying its risk posture;
- Inheriting capabilities from a cloud service offering where the authorized provider environment is used directly as authorized (e.g. FEDRAMP) ; and
- Operating within an existing authorized platform boundary, without deviation from its established configuration or controls.

2.2 The Persistent Misconception

A common and incorrect application of reciprocity takes the following form:

> *"Another organization has an ATO for this software product. We can use that ATO as reciprocity for our deployment."*

This interpretation is incorrect. An ATO is a risk-based determination issued for a specific system implementation. It is bounded by the defined system boundary as defined within its ATO package, the hosting environment and infrastructure, the system architecture and configuration, the data types processed and the user population served, and the specific implementation of security controls within that context.

Reciprocity applies to the same authorized system or service - not to the reuse of the same commercial software product in an independently deployed environment. A separately installed instance of a software product, operating in a different infrastructure with independently implemented controls, constitutes a new system. That new system has its own unique risk posture and requires its own authorization.

3. Why This Distinction Matters

Different deployment environments introduce distinct risks, dependencies, and control implementations. Accepting a prior ATO as applicable to a new deployment - without validating equivalency in risk posture - produces several serious consequences:

Risk	Impact
Unassessed Security Controls	Controls that are independently implemented may have gaps, misconfigurations, or deviations that were never evaluated. The prior ATO provides no assurance for these implementations.
Unsupported Authorization Claims	Asserting reciprocity where it does not apply creates a false record of authorization status, potentially exposing the program and AO to compliance liability.
Undermined RMF Integrity	The credibility of the RMF process depends on the accuracy of authorization decisions. Misapplied reciprocity introduces systemic inaccuracy into the authorization record.
Deferred Risk Visibility	Security weaknesses in the new deployment may remain undetected, deferring risk rather than managing it – a direct contradiction of the RMF's purpose.
Delays and Miscommunication	Incorrect terminology use frequently causes delays, frustration, and "spinning" as personnel speak past each other instead of from a shared understanding. This can cause an accreditation to experience costly delays and false starts as acceditations fail to pass basic tests.

4. Artifact Reuse: A Valid, Distinct Practice

The fact that software-based reciprocity is inappropriate does not mean that organizations must begin every authorization from scratch. Security artifact reuse is a separate, legitimate, and encouraged practice that can substantially reduce authorization burden without misrepresenting authorization status.

When a comparable authorized implementation of a product exists, the following artifacts may be adapted and leveraged for a new authorization effort:

- Security control implementation details and assessment results, where verified to be applicable to the new deployment context;
- Configuration baselines, hardening guidance, and SCAP content developed for the product;
- Vendor-provided documentation, including security guides, data flow diagrams, and system descriptions; and
- System Security Plans (SSPs) and Security Assessment Reports (SARs) from comparable implementations, used as a starting framework — not as evidence of existing authorization.

Artifact reuse accelerates the assessment process and improves documentation quality. It is policy-consistent and does not require that the new system be equivalent in environment, architecture, or

risk posture to the source. The critical distinction is that artifact reuse supports the process of achieving a new authorization - it is not itself an authorization.

**All reused artifacts must be validated for applicability to the new system's environment and implementation.*

5. Decision Framework

The following questions provide a practical framework for practitioners evaluating whether reciprocity applies to a given situation:

Question	Yes	No
Are you consuming the exact same authorized system/service instance - not a new deployment?	Reciprocity may apply. Validate equivalency.	Reciprocity does not apply. New authorization required.
Is the hosting environment, boundary, and configuration substantively unchanged?	Continue reciprocity evaluation.	New authorization required.
Are controls inherited from the authorizing entity — not independently implemented?	Reciprocity may apply.	Reciprocity does not apply.
Is the original ATO still active and the authorization basis still valid?	Proceed with reciprocity documentation.	Reciprocity is not available. Authorization required.

6. Policy Considerations and Recommendations

The misinterpretation documented in this paper is not isolated to any single program or Component. It reflects a gap between the policy intent embedded in DoDI 8510.01 and the operational understanding that has developed at the program and installation level. Addressing this gap requires deliberate policy communication and reinforcement.

The following actions are recommended for DoD cybersecurity leadership:

1. **Issue supplemental guidance.** Publish clear, authoritative guidance explicitly distinguishing reciprocity of authorization decisions from reuse of commercial software products. This guidance should include illustrative examples of both appropriate and inappropriate reciprocity claims.

2. **Formally endorse artifact reuse.** Define and codify artifact reuse as a separate, distinct, and sanctioned practice within the RMF workflow, with guidance on how it should be documented and what limitations apply.
3. **Reinforce through Component channels.** Direct Component CIOs and AOs to communicate the correct application of reciprocity through program reviews, training programs, and validator guidance.
4. **Address RMF as a whole.** RMF is a great system that suffers from severe implementation inefficiency. Misunderstandings on policy, terminology, responsibilities, and inefficiencies run rampant throughout the process in the DoD implementation.

7. Conclusion

Reciprocity, properly understood and applied, is a valuable tool for reducing authorization burden and promoting the use of vetted enterprise solutions across the DoD. It is not, however, a mechanism for bypassing the authorization process when the same commercial software is independently deployed in a different environment.

The distinction is not a procedural technicality - it reflects the fundamental premise of the RMF: that authorization is a risk-based determination tied to a specific implementation in a specific context. An ATO for software Product X in Organization A's environment says nothing about the risk posture of Product X in Organization B's environment.

Practitioners who understand this distinction can make authorization decisions that are both efficient and defensible. They can leverage artifact reuse to accelerate assessments. They can apply reciprocity where it is genuinely warranted. And they can avoid the compliance risk and false assurance that comes from misapplying a valuable policy tool.

Clearer enterprise guidance will strengthen security posture, improve mission outcomes, and support a more consistent and credible authorization ecosystem across the DoD.

Applicable Policy References

- DoDI 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," current edition
- NIST SP 800-37, "Risk Management Framework for Information Systems and Organizations," Revision 2
- NIST SP 800-53, "Security and Privacy Controls for Information Systems and Organizations," Revision 5
- CNSS Instruction 1253, "Security Categorization and Control Selection for National Security Systems"