INSTITUTE FOR DEFENSE ANALYSES

Streamlining the Risk Management Framework (RMF) Process for Urgent and Emerging Capabilities

Laura A. Odell, *Project Leader*

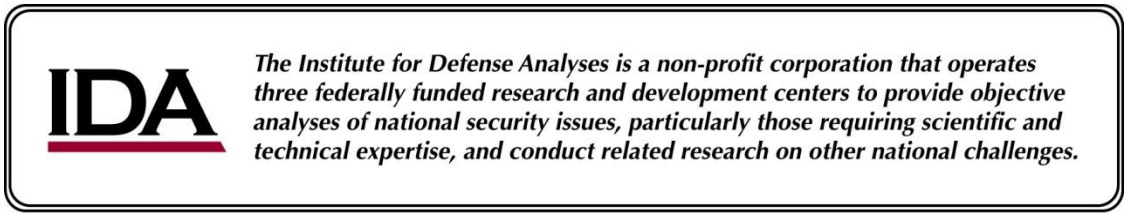
Cameron E. DePuy
J. Corbin Fauntleroy
Tyler C. Rabren
Miranda G. Seitz-McLeese

March 2018

IDA Document
D-8981

INSTITUTE FOR DEFENSE ANALYSES
4850 Mark Center Drive
Alexandria, Virginia 22311-1882

Distribution authorized to U.S. Government agencies only; Administrative or Operational Use 27 Mar 2018.
Other requests for this document shall be referred to OSD/A&S/DASD (C3CB).



About This Publication

This work was conducted by the Institute for Defense Analyses (IDA) under contract HQ0034-14-D-0001, Task AA-5-4077, "Cyber Technical Baseline Automated Assessment," for Cyber & Space Programs, DASD(C3CB), OUSD(AT&L). The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

Acknowledgments

Gary D. Guissanie, Ronald G. Bechtold

For more information:

Laura A. Odell, Project Leader
lodell@ida.org, 703-845-2009

Margaret E. Myers, Director, Information Technology and Systems Division
mmyers@ida.org, 703-578-2782

Distribution authorized to U.S. Government agencies only; Administrative or Operational Use 27 Mar 2018.
Other requests for this document shall be referred to OSD/A&S/DASD (C3CB).

INSTITUTE FOR DEFENSE ANALYSES

IDA Document D-8981

Streamlining the Risk Management Framework (RMF) Process for Urgent and Emerging Capabilities

Laura A. Odell, *Project Leader*

Cameron E. DePuy
J. Corbin Fauntleroy
Tyler C. Rabren
Miranda G. Seitz-McLeese

Distribution authorized to U.S. Government agencies only; Administrative or Operational Use 27 Mar 2018.
Other requests for this document shall be referred to OSD/A&S/DASD (C3CB).

Distribution authorized to U.S. Government agencies only; Administrative or Operational Use 27 Mar 2018.
Other requests for this document shall be referred to OSD/A&S/DASD (C3CB).

Executive Summary

The Department of Defense (DoD) needs to build cybersecurity into mission-critical acquisitions. The DoD Information Assurance Certification and Accreditation Process (DIACAP), which DoD established in 2007, was primarily a compliance-based process. The Risk Management Framework (RMF), published by the National Institute of Standards and Technology (NIST) in 2010 and adopted by DoD in 2014 is a risk management-oriented process. While both start at the initiation of a new system or modification to a major system, the difference lies in *how* to begin the process. DIACAP began fresh with each new system or major modification, whereas RMF is designed to build upon the work of other programs and systems.

Unfortunately, rapid technology acquisition for operational requirements has been late to need, thereby introducing risk rather than mitigating risk and negating the original desired outcome of the RMF. Given that urgent and emerging capability acquisitions are granted rapid acquisition authorities because of a time-critical need, this report examines the question of whether the RMF process can be streamlined, adjudicated, or waived to meet the needed timely delivery to the warfighter.

Statutory Requirements for Risk Management

Although no statutory changes are needed to simplify or improve the agility of the defense acquisition systems for urgent and emerging capability acquisitions, the risk-adverse posture of some programs is resulting in security authorization packages (including the ATO decision) that are not tailored to accurately reflect the operational situation. Foundationally, statutory requirements for risk management fall under the Federal Information Security Modernization Act (FISMA) of 2014. [1] FISMA delegates the authorities for developing and overseeing the implementation of policies, principles, standards, and guidelines on information security for DoD systems to the Secretary of Defense. [2] In other words, DoD has the authority to develop policy, instructions, procedures, and other guidelines for risk management for all DoD systems.

All information systems that "receive, process, store, display, or transmit" DoD data must receive an Authorization to Operate (ATO) before they are deployed.[i]

FISMA does not apply to National Security Systems (NSS), with the exception of coordination with government-wide efforts on information security policies and practices and reporting on the effectiveness of information security policies and practices. [3] The

Committee on National Security Systems (CNSS), under National Security Directive (NSD) No. 42, *National Policy for the Security of National Security Telecommunications and Information Systems*, is responsible for developing policy, instructions, and guidelines for NSS. [4]

DoD, as the chair of the committee under NSD-42, worked with CNSS (whose membership includes the Intelligence Community (IC)) to develop a security categorization and control process for NSS that could cover NSS and DoD and IC systems.[1] This resulted in DoD and the IC using a single control catalog (NIST Special Publication (SP) 800-53[2] [5]) vice separate departmental instructions. DoD and the Director of National Intelligence (DNI) agreed to have CNSS publish an instruction (CNSS Instruction (CNSSI) 1253, *Security Categorization and Control Selection for National Security Systems*) that provided the security control requirements (baselines and overlays) for NSS and uses and points to an expanded NIST SP 800-53 as the controls catalogue. [6] DoD published DoD Instruction 8510.10, *Risk Management Framework (RMF) for DoD Information Technology (IT)* to establish and use an integrated enterprise-wide decision structure for cybersecurity risk management based on CNSSI 1253.

DoD Directive 5000.71, *Rapid Fulfillment of Combatant Commander Urgent Operational Needs*, defines the types of acquisitions that qualify as urgent operational needs and dictates how components should expedite processes. However, this directive does not specifically address which processes (i.e., ATO and Interim Authorization to Test (IATT)) senior leaders should act swiftly upon. [12]

DoD has the ability to influence regulations and policies associated with risk management as chair of CNSS and as a member of the Joint Transformation Task Force (JTTF).[3]

Observations on the RMF Process

The RMF documents cybersecurity requirements for mission-critical acquisitions. However, the development of RMF core documents (required by CNSSI 1254, *Risk Management Framework Documentation, Data Element Standards, and Reciprocity Process for National Security Systems*, and DoD Instruction (DoDI) 8510.10, Enclosure 6, Section 4) has become a compliance-based rather than a performance-focused process,

---

[1] To maintain consistency across the Department, DoD applies the NSS requirements across all DoD systems.

[2] NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, provides processes and procedures for risk management.

[3] The JTTF comprises NIST, DNI, and DoD. It does not meet; rather, it reviews requested changes to existing or new NIST publications.

resulting in significant delays and increased costs when deploying urgent and emerging capabilities. [10] The content of the security authorization documents is driven by the requirements of DoDI 8510.01, the guidelines of the organization, and the expectations of the Authorizing Official (AO); the more detail requested by the organization or AO, the larger the document becomes. In addition, ATO decisions are being made in a risk-adverse environment resulting from the recent Executive Order for strengthening the cybersecurity of federal networks and critical infrastructure, which places greater accountability on Agency Heads. [11]

Recommendations for Streamlining the RMF Process

The following actions would streamline the RMF process for urgent and emerging capabilities.

1. *Develop a tactical overlay for DoD to emphasize appropriate tailoring of core minimum security controls that are relevant to the operational environment.* The RMF Technical Advisory Group (TAG) should establish a working group, chaired by the Office of the Secretary of Defense (OSD) and with membership including the appropriate members of the Military Departments, to develop a tactical overlay for urgent and emerging capabilities. The RMF process should begin with the tactical overlay. This first step encourages the necessary tailoring that may be required for urgent and emerging capabilities, thus streamlining the RMF process. This has the added benefit of reducing the time in the review process since changes in the control set would have been approved by CNSS.
2. *Consider reciprocity first—emphasizing performance and operational value over a checklist or compliance methodology.* For any urgent or emerging capability with an existing ATO on a DoD network, reciprocity should be actively pursued as a first step. RMF is designed to build upon the work of other programs and systems, using reciprocity to the greatest extent possible. Reciprocity minimizes duplication of effort and potentially decreases time to deployment. In addition, the Program Manager (PM) should provide a roadmap as part of the reciprocity request that maps the boundaries and controls of the system being submitted for an ATO to the boundaries and controls of the system that currently has an ATO. The roadmap must specify name changes, page numbers, and a detailed justification of why reciprocity should be considered. Further, the identification of any deltas between the reciprocal system controls and the controls for the target environment should be annotated. This is particularly important when the requesting organization is not the same as the receiving organization since the AO will likely have no knowledge of the capability being requested if it is not already in operation in the target

environment. The following recommendations would improve the ability of program managers to use reciprocity.

a. *Add text analytics to eMASS to expedite user friendly search capabilities to identify systems, or system components, which currently hold an ATO.* In eMASS, the user has the ability to search on a system name to find information. However, many systems are comprised of sets of software and hardware packages specific to the system. An AO, or AO's representative, is not able to search the document repository in eMASS for software or hardware that might be a component of a larger system. Currently, there is no indexing system that allows the user to search on a component and get a list of all systems containing that component. This makes reciprocity difficult if the PM cannot search for the system he is using. For example, Naval System X, with an ATO, may comprise several tools (e.g., Tool A, Tool B, and Tool C). If Army System Y contains Tool A, eMASS has no mechanism that allows the Army PM to identify Naval System X as a candidate for possible reciprocity. DoD should add a search capability to eMASS using natural language processing to help PMs identify possible reciprocity opportunities.

b. *Provide AOs with greater access to security authorization packages within common functional and technical areas that may not be within their direct organization.* Even if a search capability were available in eMASS, AOs limit exposure of information about systems in their areas of responsibility in eMASS. The intent is to reduce the possibility of insider threat. A standardized approach in this regard is indicated. For example, if an Army PM wants to use reciprocity based on a Navy system that already has an ATO, the PM must contact the appropriate office in the Navy to obtain a copy of the security authorization package. However, as part of the ATO process, all documents associated with a security authorization package are uploaded to eMASS. PMs should be encouraged to contact their AO to obtain information about any system loaded into eMASS. This would improve the PMs' ability to find opportunities for reciprocity and gain much quicker access to the documentation.

3. *Allow an urgent and emerging capabilities off-ramp for the ATO decision and AO review when the mission need demands that the solution not be "late to need."* The following recommendations could streamline the ATO decision process for urgent and emerging capabilities.

a. *Agreed upon Not to Exceed (NTE) timelines for the ATO decisions that satisfy operational need.* Once the RMF core documents and artifacts are submitted for an ATO decision, they are reviewed for any risks that have not been

addressed. The RMF core documents should be based on a minimum set of controls defined in a tactical overlay. Depending on the level of complexity and the workload of the reviewers, it may take months before an ATO decision is made. This is unacceptable if operational commands are dependent on the capability. Urgent and emergent capabilities need an ATO decision within a pre-determined NTE threshold.

b. *Submit the RMF to the Defense Information Assurance Security Accreditation Working Group (DSAWG) in parallel with submission to the AO.* This allows the DSAWG to review the RMF in parallel with the AO. If the ATO does not make a decision in a timely manner, the decision can be escalated to the Information Security Risk Management Committee (ISRMC) for review and ATO decision.

c. *For urgent capabilities that require short, non-enduring ATO decisions, submit the request for ATO directly to the ISRMC.* The ISRMC has the ability to make decisions out of cycle, and those decisions will be binding on the AO. A temporary ATO can be authorized with a requirement to meet AO security requirements if the capability becomes an enduring need. If this step is taken, the system owner will need to go through the DSAWG review process.

4. *Provide guidelines for expediting urgent and emerging capabilities through the RMF process.* Guidelines should be added to DoDI 5000.71, *Rapid Fulfillment of Combatant Commander Urgent Operational Needs*, for expediting urgent and emerging capabilities through the RMF process. DoDI 8510.01 allows tailoring of the RMF core documents and provides off-ramps for quicker decision-making. However, there are no clear guidelines for identifying a capability as urgent or emerging in DoDI 8510.01, or associated timelines that allow the Services to react to operational needs.

Distribution authorized to U.S. Government agencies only; Administrative or Operational Use 27 Mar 2018.
Other requests for this document shall be referred to OSD/A&S/DASD (C3CB).

Contents

Figures and Tables

1. Introduction

The Department of Defense (DoD) acquisitions uses the Risk Management Framework (RMF) to document and build cybersecurity into mission-critical acquisitions. All information systems that "receive, process, store, display, or transmit" DoD data must receive an Authorization to Operate (ATO) before they are deployed.[i] As technology has become more prevalent, in practice, this definition means that almost any technology acquisition must go through the RMF process, which can be cumbersome and time-consuming. This can impede rapid technology acquisition for operational needs.

Given that urgent and emerging capability acquisitions are granted rapid acquisition authorities because of a time-critical need, this report examines the question of whether the RMF process can be streamlined, adjudicated, or waived to meet the needed timely delivery to the warfighter.

Example of Delays in the RMF Process

A Joint Urgent Operational Needs (JUON) was approved and established in March 2017. The approval and requirements generation took 14 days. The procurement, development, and testing took 72 days. The RMF process took more than 210 days before an ATO was given. From March 2017 to October 2017, the team developed a 600-page RMF that was sent back to be redone on three occasions, once because of a formatting change. The estimated cost of executing the RMF process is six times the cost of the item to be deployed. Note: The initial ATO was limited to a single installation, but the JOUN project was expected to be used in multiple installations.

A. Approach

The Deputy Director, Cyber & Space Programs, Office of the Deputy Assistant Secretary of Defense Command, Control, and Communication, Cyber, and Business Systems (C3CB), Office of the Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)) asked the Institute for Defense Analyses (IDA) to identify and review statutory requirements and relevant policy and guidance for RMF implementation and make recommendations for streamlining the RMF process for urgent and emerging capability acquisitions. The IDA team began this effort by reviewing U.S. statutes and DoD Instructions and Directives to identify the laws, policy, and guidance that directly impact acquisition and, in particular, RMF implementation. The team also reviewed relevant documents from the Committee on National Security Systems (CNSS) and publications from the National Institute of Standards and Technology (NIST) that formed the foundation of RMF implementation.

The IDA team also interviewed several organizations charged with procuring urgent or emerging capabilities to gain an understanding of the challenges and issues they face in receiving an ATO for new hardware or software to meet operational needs. Their comments provided additional insights into the RMF process. Using the results of the document analysis and the insights gained from the interviews, the IDA team developed a set of recommended actions for streamlining the RMF process. This report provides a discussion of the results of the document analysis, the insights gained from the interviews, and the recommended actions.

2. Risk Management in DoD

The E-Government Act of 2002 (Public Law 107-347) recognizes the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, *Federal Information Security Management Act of 2002*, addresses this area. Since that time, DoD has developed processes to identify, assess, and monitor risk to information systems. The following discussion provides an overview of the current statutory requirements, policies, guidance, and DoD directives and instructions for risk management.

A. Statutory Requirements

Current statutory requirements for risk management fall under the Federal Information Security Modernization Act (FISMA) of 2014.[4] FISMA requires "agencies…to identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of—(A) information collected or maintained by or on behalf of an agency; or (B) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency…." [1] Section 11331 of Title 40 states that the National Institute of Standards and Technology (NIST) shall develop the minimum required standards for information security and that these standards will be binding. [2] FISMA requires Agencies to comply with "the requirements of [this Act] and related policies, procedures, standards, and guidelines, including … information security standards promulgated under section 11331 of title 40." [3]

There are two exceptions to the requirements in this Act: (1) FISMA does not apply to National Security Systems (NSS), with the exception of coordinating with Government-wide efforts on information security policies and practices and reporting on the effectiveness of information security policies and practices [4] and (2) the Committee on National Security Systems (CNSS), under National Security Directive No. 42, *National Policy for the Security of National Security Telecommunications and Information Systems*, is responsible for developing policy, instructions, and guidelines for NSS. [5]

Similarly, FISMA delegates the authorities for developing and overseeing the implementation of policies, principles, standards, and guidelines on information security for DoD systems to the Secretary of Defense. [3] In other words, DoD has the authority to develop policy, instructions, procedures, and other guidelines for risk management for all DoD systems.

[4] FISMA was amended in 2014 and included several modifications that were intended to modernize federal security practices to address evolving security concerns.

B. NIST Information Security Standards and Risk Management Guidance

Per Section 11331 of Title 40, NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems. [2] In response to FISMA, NIST developed the Federal Information Processing Standards (FIPS) for information security. No provision is provided under FISMA for waivers of these standards.

- *FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems*. Describes the security categorization of federal information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels.
- *FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems*. Describes the minimum security requirements for information and information systems in each security category.

NIST also developed a number of Special Publications (SP) to support risk management efforts across the Federal Government.

- SP 800-30 (Rev 1), *Guide for Conducting Risk Assessments.* Provides guidance for conducting risk assessments of federal information systems and organizations, amplifying the guidance in Special Publication 800-39.
- SP 800-37 (Rev 2), *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*. Provides guidelines for applying the Risk Management Framework to federal information systems to include security categorization, security control selection and implementation, security control assessment, information system authorization, and security control monitoring.
- SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*. Provides guidance for an integrated, organization-wide program for managing information security risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation resulting from the operation and use of federal information systems.
- SP 800-53 (Rev 5), *Security and Privacy Controls for Federal Information Systems and Organizations.* Provides a catalog of security and privacy controls for federal information systems and organizations and a process for selecting controls to protect organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation from a diverse set of threats, including hostile cyberattacks, natural disasters, structural failures, and human errors (both intentional and unintentional). It is used in conjunction with FIPS 199 and FIPS 200 to ensure appropriate security requirements and security controls are applied to all federal information systems.

- SP 800-53A (Rev 4), *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans.* Provides a set of procedures for assessing security controls and privacy controls employed within federal information systems and organizations.
- SP 800-59, *Guideline for Identifying an Information System as a National Security System.* Provides guidelines for identifying an information system as a national security system.
- SP 800-60, (Rev 1) *Guide for Mapping Types of Information and Information Systems to Security Categories.* Provides guidelines for recommending the types of information and information systems to be included in each security category.
- SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations.* Provides guidelines to assist organizations with the development of a continuous monitoring strategy and the implementation of a continuous monitoring program that provides visibility into organizational assets, awareness of threats and vulnerabilities, and visibility into the effectiveness of deployed security controls.

C. Committee on National Security Systems Instructions

Section 11331 of U.S. Code Title 40 provides a caveat for standards and guidelines for national security systems (NSS). [2] The president holds this authority over NSS. In National Security Directive (NSD) 42, the president delegates that authority to the CNSS. [6] Under this authority, CNSS issued CNSS Policy (CNSSP) No. 22, *Policy on Information Assurance Risk Management for National Security Systems* [15], and CNSS Instruction (CNSSI)-1254, *Risk Management Framework Documentation, Data Element Standards, and Reciprocity Process for National Security Systems* [7], which implement Title 44 and Title 40 statutes for NSS. CNSSP-22 states that "CNSS intends to adopt NIST issuances where applicable." [6] Specifically, CNSSP-1254 requires organizations to follow FIPS-200, NIST SP 800-30, NIST 800-37, NIST 800-39, NIST SP 800-53, and NIST SP 800-53A. [7]

DoD, as the chair of the committee under NSD-42, worked with CNSS (whose membership includes the Intelligence Community (IC)) to develop a security categorization and control process for NSS that could cover NSS and DoD and IC systems.[5] This resulted in DoD and the IC using a single control catalog (NIST SP 800-53) vice separate departmental instructions. DoD and the Director of National Intelligence (DNI) agreed to have CNSS publish an instruction (CNSSI 1253, *Security Categorization and Control Selection for National Security Systems*) that provides the security control requirements (baselines and overlays) for NSS that use and point to an expanded NIST SP 800-53 as the controls catalogue. [8]

[5] To maintain consistency across the Department, DoD applies the NSS requirements across all DoD systems.

DoD has the ability to influence regulations and policies associated with risk management as chair of CNSS and as a member of the Joint Transformation Task Force (JTTF).[6]

D. Department of Defense Directives and Instructions

In 2016, as a result of the changes made in FISMA, DoD replaced the DoD Information Assurance (IA) Certification and Accreditation Process (DIACAP) with the Risk Management Framework to manage the lifecycle cybersecurity risk to DoD IT in accordance with NIST SP 800-53A and DoD Directive (DoDD) 8000.01, *Management of the Department of Defense Information Enterprise (DoD IE)*. NIST SP 800-53A provides the procedures for risk management. DoDD 8000.01 directs that investments in information solutions be managed through a capital planning and investment control process that "provides for analyzing, selecting, controlling, and evaluating investments, as well as assessing and managing associated risks." [9]

Referencing Presidential guidance, CNSS policy instructions, and NIST standards and guidance, DoD updated the following instructions for RMF implementation:

- DoD Instruction (DoDI) 8500.01, *Cybersecurity*, specifies that DoD will use NIST SP 800-37 to address risk management and requires systems to obtain an Authority to Operate before being fielded or connected. [10] This requirement is derived from FIPS 200, which states that an organization will "authorize the operation of organizational information systems and any associated information system connections." [11]
- DoDI 8510.01, *Risk Management Framework for DoD Information Technology*, establishes policy, processes, and responsibilities for executing and maintaining the RMF. DoDI 8510.01 lays out an integrated enterprise-wide decision structure for cybersecurity risk management based on CNSSI 1253. [13]

Currently, five instructions (see Table 2-1) continue to reference DIACAP and should be updated to reflect DoDI 8510.01. In some cases, DIACAP processes are referenced directly in the instruction; two instructions should be modified to reference the appropriate DoD instruction rather than refer to specific processes and technology.

[6] The JTTF comprises NIST, DNI, and DoD. It does not meet; instead, it reviews requested changes to existing or new NIST publications.

Table 2-1. DoD Instructions that Refer to DIACAP

Instr. #	Office of Primary Responsibility	Title	Date	Description
8100.04+	ASD(NII)/ DoD CIO	DoD Unified Capabilities (UC)	12/09/2012	Establishes policy, assigns responsibilities, and prescribes procedures for test; certification; acquisition, procurement, or lease; effective, efficient, and economical transport; connection; and operation of DoD networks to support UC, as defined in the Glossary.
8260.03*	USD(P&R)	The Global Force Management Data Initiative (GFM DI)	02/19/2014	Mandates the GFM DI to develop standardized enterprise force structure data, available electronically in a joint hierarchical way, for integration and use throughout DoD.
8520.02*	ASD(NII)/ DoD CIO	Public Key Infrastructure (PKI) and Public Key (PK) Enabling	05/24/2011	Establishes and implements policy, assigns responsibilities, and prescribes procedures for developing and implementing a DoD-wide PKI and enhancing the security of DoD information systems by enabling these systems to use PKI for authentication, digital signatures, and encryption.
8581.01+	ASD(NII)/ DoD CIO	Information Assurance (IA) Policy for Space Systems Used by the Department of Defense	06/08/2010	Establishes IA policy and assigns responsibilities for all space systems used by DoD.
8550.01*	DoD CIO	DoD Internet Services and Internet-Based Capabilities	09/11/2012	Establishes policy, assigns responsibilities, and provides instructions for the establishment, operation, and maintenance of DoD internet services on unclassified networks to collect, disseminate, store, and otherwise process unclassified DoD information and the uses of internet-based capabilities (IbC) to collect, disseminate, store, and otherwise process unclassified DoD information.
*** References the previous version of DoDI 8510.01 + References DIACAP processes and procedures directly in the instruction**				

In addition, DoD updated acquisition directives to reflect the RMF requirement. Program managers (PM) must follow these directives and associated instructions when procuring urgent and emerging capabilities. This includes the following:

- DoDI 5000.02, *Operation of the DoD Acquisition System*, has been updated to include the RMF requirements, stating, "Cybersecurity RMF steps and activities…should be initiated as early as possible and fully integrated into the DoD acquisition process including requirements management, systems engineering, and test and evaluation." [12]
- DoDI 5200.39, *Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E)*, requires Components to secure DoD information technology storing, processing, or transmitting CPI in accordance with DoDI 8500.01 and DoDI 8510.01.

- DoDI 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems & Networks*, requires DoD systems to use impact level categorizations as defined in DoDI 8510.01.

3. DoD Risk Management Process 1992–2017

"Security control assessments and privacy control assessments are not about checklists, simple pass-fail results, or generating paperwork to pass inspections or audits—rather, such assessments are the principal vehicle used to verify that implemented security controls and privacy controls are meeting their stated goals and objectives."

National Institute for Standards and Technology Special Publication 800-53

A. Early Certification and Accreditation Efforts

DoD has been concerned about securing information systems (IS) for over three decades. As computers and networking became indispensable to the Department, a standard approach for accrediting IS was needed. In 1992, the Assistant Secretary of Defense for Command, Control, Computers, and Intelligence released the *Defense Information Systems Security Program (DISSP) Strategic Plan*.[ii] The plan laid out standard requirements and processes for accrediting computers systems and networks to meet the policies defined in DoDD 5200.28, *Security Requirements for Automated Information Systems (AISs) (1988)*; the *Computer Security Act of 1987*;[iii] and OMB Circular No. A-130, *Management of Federal Information Resources (1985)*.[7] DoD Instruction 5200.40, *DoD Information Technology Security Certification and Accreditation Process (DITSCAP)*, was released in response to the plan, which provided a standardized approach for security certification and accreditation of information systems.[iv]

DITSCAP was intended to streamline the certification and accreditation process and ensure the use of standard conventions, criteria, and processes across DoD. Unlike the existing processes of the time, DITSCAP focused on the infrastructure, viewing systems and networks as components of the infrastructure. However, DITSCAP concentrated only on certification and risk assessment of systems, with few considerations for life-cycle development, and implementation varied from Component to Component.

B. Shift to Life-Cycle Certification and Accreditation – DIACAP

Desiring improvements in the security of information systems within the Federal Government, Congress passed FISMA 2002 as part of the E-Government Act of 2002, which

[7] Circular A-130 was first issued in December 1985 to meet the information resource management requirements in the Paperwork Reduction Act (PRA) of 1980. This circular has been updated several times since then; the most recent update was released in 2016. (https://obamawhitehouse.archives.gov/blog/2016/07/26/managing-federal-information-strategic-resource)

directed Federal agencies to develop, document, and implement an organization-wide program to provide information assurance (IA). In response to this mandate, DoD issued DoDD 8500.01, *Information Assurance (IA)*, in 2002 to establish policy and assign responsibilities to achieve DoD IA, [10] and DoDI 8500.02, *Information Assurance (IA) Implementation*, in 2003 to define the security controls required to ensure that the confidentiality, integrity, and availability of an information system were being met, monitored, and managed.[v]

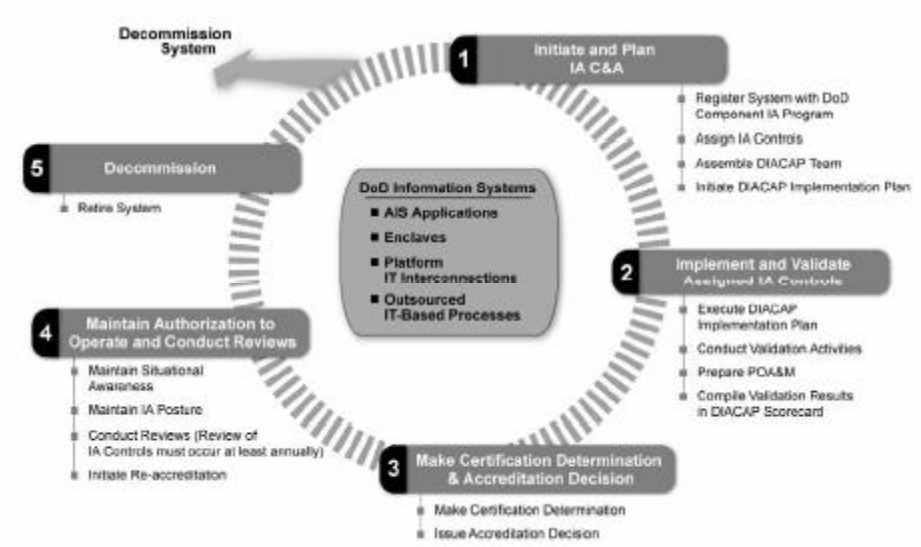
In 2007, DoDI 5200.40 (DITSCAP) was cancelled and replaced by DoDI 8510.01, *DoD Information Assurance Certification and Accreditation Process (DIACAP)*. DoDI 8510.01 established "a [certification and accreditation] C&A process to manage the implementation of IA capabilities and services and provide visibility of accreditation decisions regarding the operation of DoD ISs, including core enterprise services– and Web services–based software systems and applications." [13] DIACAP was supported by an automated IA controls-based C&A workflow, implemented through the Enterprise Mission Assurance Support Service (eMASS).[vi]

Unlike DITSCAP, DIACAP paralleled the system life cycle, and its activities were initiated at the start of a new system or a major system modification. DIACAP consisted of five major activities (see Figure 3-1):

1. *Initiate and Plan IA C&A.* This included "registering the system with the governing DoD Component IA program, assigning IA controls based on Mission Assurance Category (MAC) and Confidentiality Level (CL), identifying the DIACAP Team for the IS, and initiating the IS's DIACAP Implementation Plan (DIP)." [13]
2. *Implement and Validate Assigned IA Controls.* This included executing the DIP, conducting validation activities, preparing the IT Security Plan of Actions and Milestones (POA&M), and compiling the validation results in the DIACAP Scorecard. [13]
3. *Make Certification Determination and Accreditation Decision.* The certification determination was based on actual validation results. It considered impact codes, associated severity categories, expected exposure time (i.e., the projected life of the system release or configuration minus the time to correct or mitigate the IA security weakness), and cost to correct or mitigate (e.g., dollars, functionality reductions). An accreditation decision was applied to a specifically identified DoD IS and considered the tradeoff between mission or business need, protection of personal privacy, protection of the information being processed, and protection of the information environment. A certification determination was required before an accreditation decision could be made. An accreditation decision had four outcomes: an Authorization to Operate (ATO), an Interim ATO (IATO), an Interim Authorization to Test (IATT), or a Denial of an ATO (DATO). Systems were considered unaccredited prior to an accreditation decision. [13]

4. *Maintain Authorization to Operate and Conduct Reviews.* A continued ATO was contingent on the sustainment of an acceptable IA posture. The DoD IS IA Manager was responsible for maintaining situational awareness and initiating actions to improve or restore IA posture. [13]

5. *Decommission.* Prior to decommissioning, any inheritance relationships were reviewed and assessed for impact. Once a system was decommissioned, the System Identification Profile (SIP) was updated to reflect the IS decommissioned status and information on it was removed from all tracking systems. [13]



Source: DoDI 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP), November 28, 2007.

Figure 3-1. DIACAP Activities

PMs were required to develop two C&A packages for DIACAP: (1) a comprehensive package containing all information connected with the certification of the IS, and (2) an executive package containing the minimum information for an accreditation decision. The Designated Accrediting Authority (DAA) determined what information was necessary to make an accreditation decision. The package was "developed through implementing the activities of the DIACAP and maintained throughout a system's life cycle. Information from the package [is used] to support an accreditation or other decision such as a connection approval." [13] The following documents were included in the package.

- *System Identification Profile (SIP).* The SIP identifies the data requirements for registering an IS with the governing DoD Component IA program. It is generated during the DIACAP registration process.
- *DIACAP Implementation Plan (DIP).* The plan contains the IA controls (inherited and implemented), the implementation status, responsible entities, resources, and estimation completion data for each IA control. Not required for the executive package.

- *Supporting Certification Documentation.*[8] The documentation includes the actual validation results, the artifacts associated with implementation of IA controls, and any other documentation that is deemed necessary. Not required for the executive package.
- *DIACAP Scorecard.* A summary report that succinctly conveys information on the IA posture of a DoD IS in a format that can be exchanged electronically. It documents the designated accrediting authority (DAA) accreditation decision,[9] as well as the results of the implementation of required baseline IA controls and additional IA controls.
- *IT Security POA&M.* A POA&M is required for any accreditation decision that requires corrective action and is also used to document non-compliant (NC)[10] or not applicable (NA)[11] IA controls that have been accepted by the responsible DAA.

C. The Move to Life-Cycle Risk Management – RMF

In 2014, DoDI 8510.01 was reissued and renamed *Risk Management Framework (RMF) for DoD Information Technology (IT).* It replaced DIACAP with RMF and established the associated cybersecurity policy for the Department. NIST developed the RMF to provide a disciplined and structured process for integrating information security and risk management activities into the system development life cycle. RMF focuses on the information system level but is informed by the organizational and mission and business process levels.

Similar to DIACAP, risk management in RMF begins early in the system development life cycle to shape the security capabilities of the information system. RMF comprises the following six steps (see Figure 3-2):

Step 1. **Categorize** the information system and the information processed, stored, and transmitted by that system based on an impact analysis. Security categories are based on "potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to

---

[8] Certification is defined as the "comprehensive evaluation of the technical and non-technical security features of an IS to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements." (CNSSI 4009, *National Information Assurance (IA) Glossary,* revised May 2003, https://www.ecs.csus.edu/csc/iac/cnssi_4009.pdf.)

[9] A formal statement by a designated accrediting authority (DAA) regarding acceptance of the risk associated with operating a DoD information system (IS) and expressed as an authorization to operate (ATO), interim ATO (IATO), interim authorization to test (IATT), or denial of ATO (DATO). [13]

[10] IA controls are those for which one or more of the expected results for all associated validation procedures are not achieved. Not achieving expected results for all validation procedures does not necessarily equate to unacceptable risk.

[11] IA controls are those that do not impact the IA posture of the IS as determined by the DAA.

be used in conjunction with vulnerability and threat information in assessing the risk to an organization." [14]

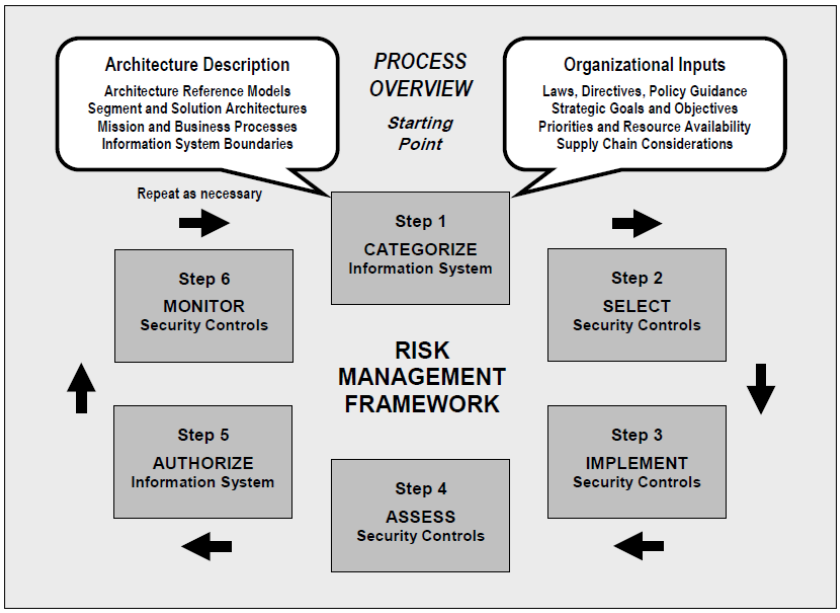
Step 2. **Select** an initial set of baseline security controls for the information system. The initial set of security controls for a system "is selected on the basis of either its baseline security categorization or its designated control profile." [15] The security control baseline can be tailored and supplemented as needed based on an organizational assessment of risk and local conditions.

Step 3. **Implement** the security controls and describe how the controls are employed within the information system and its environment of operation. "The implementation of any security control is intended to mitigate a risk, and the level of its implementation is set to the level of mitigation required to meet documented risk-tolerance thresholds." [15]

Step 4. **Assess** the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. "The conduct of security control assessments is the primary responsibility of information system owners and common control providers with oversight by their respective authorizing officials." [16]

Step 5. **Authorize** information system operation based on a determination of "the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable." [19]

Step 6. **Monitor** the security controls in the information system in accordance with the Information Security Continuous Monitoring strategy. [16] This includes assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.



Source: NIST SP 800-37 (Rev 1), Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, February 2010.

Figure 3-2. Risk Management Framework

Organizations use the RMF process to identify and mitigate risk to receive an ATO from the AO. CNNS, NIST, and DoD provide instructions and guidance (see Table 3-1) for each step in the process.

Table 3-1. Associated Guidance for RMF Process

Step	Guidance
Categorize	CNSSI 1253 FIPS 199 NIST SP 800-30, 800-59, 800-60
Select	CNSSI 1253 FIPS 199, 200 NIST SP 800-30, 800-53, 800-137
Implement	CNSSI 1253 FIPS 200 NIST SP 800-30, 800-53, 800-53A
Assess	NIST 800-30, 800-53A
Authorize	NIST SP 800-30, 800-39, 800-53A
Monitor	CNSSI 1253 FIPS 199 NIST SP 800-30, 800-39, 800-53, 800-53A, 800-137

Source: *NIST SP 800-37 (Rev 1), Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach, February 2010.*

The RMF core documents consist of:[12]

1. Security Authorization Package. Used by authorizing officials to make risk-based authorization decisions. The package includes:

   a. *System Security Plan (SSP).* Provides "an overview of the security requirements for a system and describes the security controls in place or plans for meeting those requirements, including the supporting rationale for control selection decisions, and any NSS use restrictions." [15]

   b. *Security Assessment Report (SAR).* Provides "evidence about the effectiveness of implemented controls; an indication of the quality of the risk management processes employed within the organization; and information about the strengths and weaknesses of information systems which are supporting organizational missions and business functions in a global environment of sophisticated and changing threats." [16]

   c. *Plan of Action and Milestones (POA&M).* Identifies tasks that need to be accomplished, the resources needed, and milestones with completion dates. Most importantly, the plan "describes the specific tasks that are planned: (i) to correct any weaknesses or deficiencies in the security controls noted during the assessment; and (ii) to address the residual vulnerabilities in the information system." [17]

2. *Risk Assessment Report (RAR).* Documents the results of the risk assessment or the formal output from the process of assessing risk. The authorizing official or designated representative, in collaboration with the senior information security officer, is responsible for assessing the security authorization package, which includes the current security state of the system or the common controls inherited by the system and the recommendations for addressing any residual risks. [17a]

3. *Authorization Decision Document*. This document "conveys the final security authorization decision from the Authorizing Official (AO) to the Information System Owner (ISO) or common control provider, and other organizational officials, as appropriate." [17b] A DoD authorization decision is expressed as an ATO, an IATT, or a DATO. An IS or platform IT (PIT) system is considered unauthorized if an authorization decision has not been made.

The RMF core documents represent the minimum information necessary for the acceptance of an information or platform information technology system by a receiving organization. [18]

[12] The RMF core documents are identified in CNSSI 1254 and DoDI 8510.01 and described in NIST 800-53A and 800-37.

D. DIACAP vs. RMF

It is important to understand the differences between DIACAP and RMF since these differences often create confusion when implementing RMF. Many organizations built the RMF process on top of the existing DIACAP process. For example, eMASS was first built for DIACAP and then modified for RMF. This is not surprising, since DIACAP and RMF have similar activities (see Table 3-2) and documentation. *However, DIACAP was primarily a compliance-oriented process, whereas RMF is a risk management-oriented process.* Both begin at the initiation of a new system or modification to a major system. The difference lies in how to begin the process. DIACAP begins fresh with each new system or major modification, whereas RMF is designed to build upon the work of other programs and systems, using reciprocity to the greatest extent possible. This allows the PM to streamline RMF efforts by using previous system information and ATO decisions to determine impact and risk.

Table 3-2. Comparison of DIACAP and RMF Activities

DIACAP	RMF
Initiate and Plan	Categorize
	Select
Implement and Validate	Implement
	Assess
Certification Determination/Accreditation Decision	Authorize
Maintain Authorization	Monitor
Decommission	

Security categorization changed under RMF. DIACAP categorization was based on availability and integrity (MAC levels) and confidentiality (CL levels). RMF categorization is based on three security objectives (Confidentiality, Integrity, and Availability) and impact levels (Low, Moderate, and High). In addition, the number of required security controls increased under RMF.

RMF streamlined the DIACAP process by reducing the documentation to be maintained and submitted to the AO for authorization (see Table 3-3). DIACAP's SIP and DIP were merged into a single document, the SSP, for RMF. Similarly, DIACAP's validation results and the DIACAP Scorecard were merged into the SAR for RMF. Lastly, the DIACAP Executive Package is no longer required since the RMF security authorization package fulfills both its function and the function of the DIACAP Comprehensive Package.

Table 3-3. Comparison of RMF Security Authorization Package and the DIACAP Package

DIACAP	RMF
System Identification Profile (SIP)	System Security Plan (SSP)
DIACAP Implementation Plan (DIP)	
oSupporting Certification Documentation	Security Assessment Report (SAR)
DIACAP Scorecard	
IT Security Plan of Actions and Milestones (POA&M)	Plan of Actions and Milestones (POA&M)

Another aspect of the RMF process is the implementation of continuous monitoring. The DIACAP accreditation decision had four possible outcomes: ATO, IATO, IATT, and DATO. RMF, on the other hand, has only three options: ATO, IATT, and DATO. The RMF ATO authorization decision "must specify an Authorized Termination Date (ATD) that is within three years of the authorization date unless the IS or PIT system has a system-level continuous monitoring program compliant with DoD continuous monitoring policy as issued." [19] This requirement means that an IATO is no longer needed; a system can have an ATO for 90 days, six months, or longer. The requirement for continuous monitoring ensures that patches are up to date and vulnerabilities due to the age of the system are mitigated. This is particularly important since many DoD systems remain in operation for years longer than originally planned, sometimes exceeding the vendor support period.

E. Challenges for Urgent and Emerging Capabilities

The IDA team interviewed several organizations with responsibility for developing and fielding urgent or emerging capabilities. The following challenges for the RMF process were identified.

1. *Improving the process means overcoming institutional inertia.* There is a perception that the PM is feeding the bureaucracy with information that adds no value. As one interviewee noted, "No one gets fired for saying 'I have concerns and need more artifacts.'"[13] The recent Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, which places more emphasis on accountability, has only solidified this view point. [18] This approach adds a lot of work/rework to the approval process.
2. *Reciprocity is not invoked enough and when invoked the results are inconsistent.* Reciprocity can streamline the RMF process; however, in reality reciprocity is difficult

[13] IDA interview.

to achieve. For example, one organization IDA interviewed has been trying to get an extension for a local ATO for over a year. The ATO still has not been granted. Both CNSSI 1254 and DoDI 8510.01 provide guidance on reciprocity, but neither provides guidelines for preparing and reviewing a security authorization package with respect to reciprocity. The original security authorization package reflects that the network environment of the originating organization and the system may have different titles, different configurations, different naming conventions, or may be an element of a larger suite of systems that have an ATO. Review time of the package is based on how capable the PM, AO, or the AO's representative is in translating the information from the original network environment to the receiving network environment.

3. *Obtaining qualified IA personnel remains a problem.* Since all IT capabilities are going through the RMF process, there has been an increase in demand for qualified IA personnel. As a result, organizations often end up with under-experienced personnel handling the RMF process or, in some cases, personnel for whom this is not their main job/priority. Also, IA personnel shortfalls are usually solved by using contractors without any contract incentives to improve the process. There are many questions about the cottage industry that has evolved to address the RMF process and whether the benefits assumed have actually materialized. Personnel capacity and talent issues add delays and additional activities to the process. This results in additional work/rework if the AO is reluctant to accept any level of risk to the receiving organization's environment.

4. *Sufficiency and completeness of needed artifacts may not meet RMF requirements.* While artifacts are sufficient for the contract that they were developed for, they often are not sufficient or complete for the activities that rely upon them outside of the contract (e.g., the RMF process). In addition, personnel developing the artifacts are still transitioning from the DIACAP process to the RMF process. As a result, it can be time-consuming and costly to get artifacts to a level appropriate for the RMF since the contractor provided a sufficient product for requirements under the contract. For example, one organization submitted a security authorization package to the AO five times due to insufficiency of artifacts before it was accepted. If design changes are made as a result of the rework, it is an indication that RMF requirements were not considered during the initial design of the system.

5. *The information required for the security authorization package differs across organizations.* The required contents of the package are determined by the AO. Also, each Military Service has its own set of guidelines for and limits to the risk its willing to tolerate. Interviewees indicated that some organizations receive an ATO with a much lighter package (i.e., 40 to 50 pages in length). Is there less content in those packages or do thicker packages (i.e., 600+ pages) contain unnecessary or irrelevant content? Only three documents are required to be submitted to the AO: the SSP, the SAR, and the

POA&M. Supporting documentation is available in eMASS and can be pulled by the AO as needed.

6. *Many organizations have built their RMF process on top of the existing DIACAP process.* This is resulting in unintended burden on staff, driving up the cost of RMF processes and increasing the amount of time the process takes. DIACAP starts as a green field process, where each control is documented and reviewed. But RMF uses common overlays and reciprocity. This means that documentation already exists and is readily available for many of the controls. The PM's effort should focus primarily on the differences between the inherited controls and overlays and the controls for the IS or PIT.

7. *The early involvement of the AO is a critical success factor for expediting systems through the RMF process.* Organizations that are successful in quickly moving an IS through the RMF process involve the AO, or AO's representative, as early as possible in the process. The AO, or AO's representative, can review security controls and identify ones that need to be addressed in the receiving environment. The goal is to ensure that AO concerns are addressed throughout the development process before requesting an ATO.

Distribution authorized to U.S. Government agencies only; Administrative or Operational Use 27 Mar 2018.
Other requests for this document shall be referred to OSD/A&S/DASD (C3CB).

4. Recommendations for Streamlining the RMF Process for Urgent and Emerging Capabilities

Cybersecurity practices and requirements for mission-critical acquisitions have been incorporated into DoD acquisition process documentation, such as the RMF. However, the development of RMF core documents (required by CNSSI 1254, *Risk Management Framework Documentation, Data Element Standards, and Reciprocity Process for National Security Systems* [24], and DoDI 8510.10, Enclosure 6, Section 4 [18]) has become a compliance-based rather than a performance-focused process, resulting in significant delays and increased costs when deploying urgent and emerging capabilities. The content of the documents is driven by the requirements of DoDI 8510.01, the guidelines of the organization, and the expectations of the AO; the more detail requested by the organization or AO, the larger the document becomes. In addition, ATO decisions are being made in a risk-adverse environment resulting from the recent Executive Order for strengthening the cybersecurity of federal networks and critical infrastructure, which places greater accountability on Agency Heads. [20]

The IDA team recommends the following actions to streamline the RMF process for urgent and emerging capabilities.

1. Develop a tactical overlay to emphasize appropriate tailoring of core minimum security controls that are relevant to the operational environment.
2. Consider reciprocity first—emphasizing performance and operational value over a checklist or compliance methodology.
3. Allow an urgent and emerging capabilities off-ramp for the ATO decision and AO review when the mission need demands that the solution not be "late to need."
4. Provide guidelines for expediting urgent and emerging capabilities through the RMF process.

A. Develop a tactical overlay to emphasize appropriate tailoring of core minimum security controls that are relevant to the operational environment.

One of the contributors to the length and complexity of the RMF process is the proliferation of security controls. Each control requires documentation, and the effort required to complete the RMF process grows as controls are added. CNSSI 1253 identifies over 600 security controls, which are categorized by three primary focus areas (confidentiality, integrity, accountability) and are binned into three levels of impact within each category. To mitigate this problem, NIST provides a set of control baselines. "A control baseline is a collection of controls…specifically

assembled or brought together to address the protection needs of a group, organization, or community of interest." [19] Baselines contain a set of controls determined by the level of impact of a system with respect to a focus area. They are one way of reducing the number of controls used in the RMF process. The baselines have been adopted with some modification by CNSS and DoD. But not all controls apply to every risk level,[14] and it can be difficult for organizations to select the most appropriate controls for a system. However, the baselines are designed to be only a starting point. It is assumed that they will be further tailored by overlays and customization.

DoDI 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT),* allows the tailoring of security controls within the baseline as necessary. [13] Tailoring can be handled on a case-by-case basis, through pre-approved RMF overlays, or through a combination of both. "Tailoring decisions must be aligned with operational considerations and the environment of the [information system] or [Platform IT] PIT system and should be coordinated with mission owner(s) and [user representatives]. … Tailoring decisions, including the specific rationale (e.g., mapping to risk tolerance) for those decisions, are documented in the security plan for the system. Every selected control must be accounted for either by the organization or the ISO or PM/SM. If a selected control is not implemented, then the rationale for not implementing the controls must be documented in the security plan and POA&M." [21] In other words, the security document describes the rationale behind the tailoring effort that resulted in the elimination/modification of any security controls in the selected baseline.

An overlay addresses the needs of specialized sets of controls for communities of interests. "Overlays complement the initial control baselines by providing the opportunity to add or eliminate controls." [22] Overlays allow for a reduction in duplicated efforts by limiting the scope of the security controls to the most relevant and by addressing common concerns once rather than for each system individually. "Overlays reduce the need for ad hoc or case-by-case tailoring by allowing COIs to develop standardized overlays that address their specific needs and scenarios." [21]

DoD Components have developed a set of control overlays that cover different scenarios, including those involving personally identifiable information, space, and intelligence. A tactical overlay was envisioned for the RMF that modified controls for the tactical environment, but it was never finalized. The tactical overlay was intended to apply to systems, or portions of systems, that are being created for use in or will be deployed to tactical environments. While many controls from the baselines apply to tactical environments, their implementations vary because of differences in risk and in both technical and operational constraints. Table 4-1 lists examples of security controls that might not be relevant or that might require modification in an operational environment.

[14] As a result of the RMF, controls are being codified in contract language. For example, the Department of Navy has a 900-page document of recommended Request for Proposal (RFP) statements aligned to RMF controls.

Table 4-1. Examples of Security Controls for Possible Removal or Modification

ID	Control Title	Description	CNSSI-1254 Cite/NIST SP800-53 Cite
AC-22	PUBLICLY ACCESSIBLE CONTENT	a. Designate individuals authorized to post information onto a publicly accessible system; b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information; c. Review the proposed content of information prior to posting onto the publicly accessible system to ensure that nonpublic information is not included; and d. Review the content on the publicly accessible system for nonpublic information [Assignment: organization-defined frequency] and remove such information, if discovered.	D-6/46
AU-11	AUDIT RECORD RETENTION	Retain audit records for [Assignment: organization-defined time-period consistent with records retention policy] to provide support for after-the-fact investigations of security and privacy incidents and to meet regulatory and organizational information retention requirements.	D-8/64
CM-10	SOFTWARE USAGE RESTRICTIONS	a. Use software and associated documentation in accordance with contract agreements and copyright laws; b. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and c. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.	D-11/91
CP-6	ALTERNATE STORAGE SITE	a. Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information; and b. Ensure that the alternate storage site provides security controls equivalent to that of the primary site.	D-11/99
MA-6	TIMELY MAINTENANCE	Obtain maintenance support and/or spare parts for [Assignment: organization-defined system components] within [Assignment: organization-defined time-period] of failure.	D-18/140
PE-9	POWER EQUIPMENT AND CABLING	Protect power equipment and power cabling for the system from damage and destruction.	D-20/157
PE-12	EMERGENCY LIGHTING	Employ and maintain automatic emergency lighting for the system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.	D-20/159
PE-13	FIRE PROTECTION	Employ and maintain fire suppression and detection devices/systems for the system that are supported by an independent energy source.	D-20/159
PE-14	TEMPERATURE AND HUMIDITY CONTROLS	a. Maintain temperature and humidity levels within the facility where the system resides at [Assignment: organization-defined acceptable levels]; and b. Monitor temperature and humidity levels [Assignment: organization-defined frequency].	D-20/160
PE-15	WATER DAMAGE PROTECTION	Protect the system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.	D-20/160
SC-19	VOICE OVER INTERNET PROTOCOL	a. Establish usage restrictions and implementation guidelines for Voice over Internet Protocol (VoIP) technologies; and b. Authorize, monitor, and control the use of VoIP technologies within the system.	D-29/244
SC-36	DISTRIBUTED PROCESSING AND STORAGE	Distribute [Assignment: organization-defined processing and storage components] across multiple physical locations.	D-30/252

New overlays can be developed. The RMF Technical Advisory Group (TAG) (formerly known as the DIACAP TAG) "provides implementation guidance for the RMF by interfacing with the DoD Component cybersecurity programs, cybersecurity communities of interest (COIs), and other entities (e.g., Defense Information Assurance Security Accreditation Working Group (DSAWG) to address issues that are common across all entities, by: … (b) Recommending changes to security controls in [NIST SP 800-53], security control baselines and overlays in [CNSSI 1253], DoD assignment values, and associated implementation guidance and assessment procedures to the DoD CIO." [8] DoD CIO would have the authority to approve changes to the cybersecurity risk management processes. CNSS approval would be required for NSS since it has the authority to develop policies and procedures.

The IDA team recommends the development of a tactical overlay for DoD. The RMF TAG should establish a working group, chaired by the USD(AT&L) and with membership including the appropriate members of the Military Departments, to develop a tactical overlay for urgent and emerging capabilities. The tactical overlay would reduce the amount of tailoring that may be required for urgent and emerging capabilities, thus streamlining the RMF process. It has the added benefit of reducing the time in the review process since any changes in the control set due to the overlay would have been approved by CNSS.

B. Consider reciprocity first—emphasizing performance and operational value over a checklist or compliance methodology.

An urgent or emerging capability may already be in use on a DoD network but with a different configuration, data flow, or use case. When RMF core documents and artifacts have been reviewed and have received authorization to operate, CNSS encourages the reciprocal use of the RMF core documents and ATO decision whenever possible. CNSS Instruction 1254, *Risk Management Framework Documentation, Data Element Standards, and Reciprocity Process for National Security Systems*, defines reciprocity as "the mutual agreement among participating organizations to share and/or reuse existing data and information included within the RMF core documents in support of authorization and risk management decisions." [24]

"Deploying systems with valid authorizations (from a DoD organization or other federal agency) are intended to be accepted into receiving organizations without adversely affecting the authorizations of either the deployed system or the receiving enclave or site. Deploying system information security officers (ISOs) and program managers (PMs) must coordinate system security requirement with receiving organizations or their representatives early and throughout system development." [25] The PMs "[e]nsure each program acquiring an information system (IS) or PIT system has

an assigned IS security engineer and that they are fully integrated into the systems engineering process." [23]

Reciprocity does not prevent an organization from developing RMF core documents and artifacts for their specific instance. "An authorization decision for IS or PIT system cannot be made without completing the required assessments and analysis, as recorded in the security authorization package. Deploying organizations must provide the complete security authorization package to receiving organizations. PMs/ISOs deploying systems across DoD Components will post security authorization documentation to Enterprise Mission Assurance Support Service (eMASS) or other electronic means to provide visibility of authorization status and documentation to planned receiving sites." [25] There is an underlying assumption that the system meets the requirements of DoDI 8500.01 and has been tested prior to placing it in the operational environment.

DoDI 8510.01 accounts for a situation in which a system has been given ATO approval and another DoD organization wants to use it as a separately owned, managed, and maintained system. In this situation, the receiving organization becomes the system owner and must use the RMF process to receive an ATO. However, "[t]he receiving enclave or site will maximize reuse of the existing authorization documentation to support the authorization by the receiving AO." [25]

Existing CNSS guidance leaves the final determination on whether to accept the request for reciprocal system authorization to the AO. CNSSI 1253 states that "[o]rganizations have the right to refuse participating in reciprocity with another organization, if the system's RMF core documentation is not considered complete enough to provide an informed understanding of potential or existing risks, or there would be excessive risk to the system or site, as determined by the system or site AO." [24] This language is replicated almost word for word in DoDI 8510.01. This allows risk-adverse AOs to deny ATO requests if they feel the risk is not acceptable, potentially holding up deployment of the urgent or emerging capability and requiring an appeal to the Information Security Risk Management Committee (ISRMC).

The IDA team recommends that for any urgent or emerging capability with an existing ATO on a DoD network, reciprocity be actively pursued as a first step. RMF is designed to build upon the work of other programs and systems, using reciprocity to the greatest extent possible Reciprocity minimizes duplication of effort and potentially decreases time to deployment. In addition, the PM should provide a roadmap as part of the reciprocity request that maps the boundaries and controls of the system being submitted for ATO to the boundaries and controls of the system that currently has an ATO. This roadmap should specify name changes and page numbers, provide a detailed justification of why reciprocity should be considered, and identify any deltas between the reciprocal system controls and the controls for the target environment. This is particularly important when the requesting organization is not the same as the receiving organization

since the AO will likely have no knowledge of the capability being requested if it is not already in operation in the target environment.

The IDA team recommends adding text analytics to eMASS to expedite user friendly search capabilities to identify systems, or system components, which currently hold an ATO. In eMASS the user has the ability to search on a system name to find information. However, many systems are made up of sets of software and hardware packages specific to the system. An AO, or AO's representative, is not able to search the document repository in eMASS for software or hardware that might be a component of a larger system. There is no indexing system that allows the user to search on a component and get a list of all systems containing that component. Reciprocity is difficult if the PM cannot search for the system he is using. For example, Naval System X, with an ATO, may comprise several tools (e.g., Tool A, Tool B, and Tool C). If Army System Y contains Tool A, there is no mechanism in eMASS that allows the Army PM to identify Naval System X as a candidate for possible reciprocity. The DoD should add a search capability to eMASS using natural language processing to help PMs identify possible reciprocity opportunities.

The IDA team recommends providing AOs with greater access to security authorization packages within common functional and technical areas that may not be within their direct organization. Even if a search capability were available in eMASS, only AOs can provide exposure of information about systems in their areas of responsibility in eMASS at their discretion. The intent is to reduce the possibility of insider threat. However, this approach hinders the ability to make greater use of reciprocity. For example, if an Army PM wants to use reciprocity based on a Navy system that already has an ATO, the PM must contact the appropriate office in the Navy to obtain a copy of the security authorization package. However, as part of the ATO process, all documents associated with a security authorization package are uploaded to eMASS. PMs should be allowed to contact their AOs to obtain information about any system loaded into eMASS. This would improve the PMs' ability to find opportunities for reciprocity and gain much quicker access to the documentation.

C. Allow an urgent and emerging capabilities off-ramp for the ATO decision and AO review when the mission need demands that the solution not be "late to need."

DoDI 8510.01 applies to "all Information Systems that receive, process, store, display, or transmit." [20] DoD Instruction 5000.02, *Operation of the DoD Acquisition System,* Enclosure 13, explicitly states that "Information technology (IT), including National Security Systems (NSS), provided in response to an urgent need require an Authority to Operate in accordance with DoD Instruction 8510.01." [26] DoD systems

must receive an ATO before they are deployed. The AO is responsible for making the ATO decision, and the RMF provides an approach to risk acceptance.

Comments from organizations indicate that this approach has become a time-consuming process. In the case of urgent and emerging capabilities, the need for a mechanism that allows the system owner to streamline procedures that introduce delay in receiving an ATO decision is indicated. There is an option to escalate the ATO request to a higher body, the DoD Information Security Risk Management Committee (ISRMC), formerly the Defense Information Systems Network (DISN)/Global Information Grid (GIG) Flag Panel.

The DoD ISRMC "performs the DoD Risk Executive Function as described in [NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*]. The panel provides strategic guidance to Tiers 2 and 3; assesses Tier 1 risk; authorizes information exchanges and connections for enterprise ISs, cross-Mission Area (MA) ISs, cross security domain connections, and mission partner connections." [23] The Commander, U.S. Strategic Command, chairs the ISRMC. The committee is supported by the DSAWG, and chaired by the Defense Information Systems Agency (DISA). The DSAWG is the community forum for reviewing and resolving authorization issues related to the sharing of community risk. The DSAWG develops and provides guidance to the AOs for IS connections to the DoD Information Enterprise. [2] This follows CNSSI 1253 guidance referencing NIST SP 800-39, which describes a tiered-approach for risk management and roles and responsibilities.

DoD ISRMC "may make an enterprise level risk acceptance determination for authorized enterprise systems, which will satisfy the requirements of the first three elements of paragraph 1d of this enclosure."[15] "If the DoD ISRMC accepts the risk on behalf of the DoD Information Enterprise, the receiving organization may not refuse to deploy the system."[25] When the ISRMC was previously the DISN/GIG Flag Panel, ATO decisions were made at the Flag Level during operations in Iraq and Afghanistan.

The following recommendations could streamline the ATO decision process for urgent and emerging capabilities.

1. Agreed upon timelines for the ATO decisions that satisfy operational need. Once the RMF core documents and artifacts are submitted for an ATO decision, they are reviewed[16] for any risks that have not been addressed. The RMF core

[15] The first three elements of the enclosure are: (1) review the complete security authorization package, (2) determine the security impact of connecting the deploying system within the receiving enclave or site, and (3) determine the risk of hosting the deploying system within the enclave or site.

[16] DoDI 8510.01 requires DoD Component Heads to "[e]nsure a trained and qualified AO is appointed in writing for all DoD IS and PIT systems, operating within or on behalf of the DoD Component in

documents should be based on a minimum set of controls defined in a tactical overlay. Depending on the level of complexity and the workload of the reviewers, it may take months before an ATO decision is made. This is unacceptable if operational commands are dependent on the capability. Urgent and emergent capabilities need an ATO decision no later than four (4) weeks after submittal.

2. Submit the RMF to the ISRMC in parallel with submittal to the AO. Submitting to the ISRMC in parallel allows the DSAWG to review the RMF in parallel with the AO. If the ATO does not make a decision in a timely manner, the decision can be escalated to the ISRMC for review and ATO decision.

3. For urgent capabilities that require short, non-enduring[17] ATO decisions, submit the request for ATO directly to the ISRMC. The ISRMC has the ability to make decisions out of cycle, and those decisions will be binding on the AO. A temporary ATO can be authorized with a requirement to meet AO security requirements if the capability becomes an enduring need. If this step is taken, the system owner will need to go through the DSAWG review process.

D. Provide guidelines for expediting urgent and emerging capabilities through the RMF process.

Section 806 of Public Law 107-314 provides the authority to streamline acquisition and deployment procedures. Procedures have been put in place on the acquisition side (i.e., Course of Action Analysis instead of Analysis of Alternatives) but they seemingly are not being leveraged effectively for deployment procedures (i.e., RMF).

DoD Directive 5000.71, *Rapid Fulfillment of Combatant Commander Urgent Operational Needs*, defines the types of acquisitions that qualify as urgent operational needs and dictates how components should expedite processes.[vii] However, this directive does not specifically address which processes (i.e., ATO and IATT) senior leaders should act on swiftly.

Regarding urgent and emerging capabilities, DoDI 5000.02, *Operation of the DoD Acquisition System*, [10] explicitly states in Enclosure 13 that "Information technology (IT), including National Security Systems (NSS), provided in response to an urgent need require an Authority to Operate in accordance with DoD Instruction 8510.01." [26]

---

accordance with DoDI 8500.01... [with] Relevant PIT expertise must be a factor in the selection and appointment of AOs responsible for authorizing PIT systems."

[17] Non-enduring requests are ATO requests for systems that have a limited life-span on the network. Many times, systems are given a temporary ATO but continue to be used beyond the period of authorization. This is intended to ensure that urgent needs are met, but long-term solutions must go through the RMF process for AO review.

Although the enclosure further directs the services that "DoD Component Chief Information Officers will establish processes consistent with DoD Instruction 8510.01 for designated approval authorities to expeditiously make the certification," it is unclear whether such processes have been implemented. [26]

DoD Components have policies that address both RMF and urgent needs, but there is no evidence of policies that relate the two. Air Force Instruction (AFI) 17-101, *Risk Management Framework for Air Force Information Technology*, [27] provides Air Force-level processes for completing the RMF and gaining an ATO that are aligned to DoD policy and tailored for the Air Force. Air Force Pamphlet 63-128, *Integrated Life Cycle Management*, defines Quick Reaction Capabilities (QRC) as a designation to meet urgent needs. This policy states that schedule is paramount when executing a QRC program, and both cost and performance should be traded off respectively: "The MDA must have a higher risk tolerance for QRC programs and be willing to leverage all regulatory/statutory authorities to field a rapid solution."[viii] There is guidance for the MDA to streamline, tailor, and have a higher tolerance for risk, but there is nothing that guides how to streamline or tailor the RMF for urgent needs. The Army similarly has disconnected the authorization process from the rapid acquisition process.

The IDA team recommends that guidelines for expediting urgent and emerging capabilities through the RMF process be developed as an annex to DoDI5000.71, *Rapid Fulfillment of Combatant Commander Urgent Operational Needs*. DoDI 8510.01 allows tailoring of the RMF core documents and provides off-ramps for quicker decision-making. However, there are no clear guidelines for identifying a capability as urgent or emerging, nor associated timelines that allow the Services to react to operational needs.

Lessons Learned: Using DevOps to streamline the ATO process

*The Joint Improvised–Threat Defeat Organization (JIDO) has a long history of responding to JUONS for combat forces. To achieve mission success, JIDO created a high-trust, high-collaboration, and secure Agile **DevOps** environment to ensure mission capabilities are delivered faster and more secure. This environment leverages principles from the Agile Software Development Life Cycle, integrates them with best practices from Information Technology Infrastructure Library (ITIL) Release and Operations Management, creates workflows to automate repeatable processes, and leverages many open source tools to rapidly and efficiently deliver mission capability using the NIST RMF.*

However, the JIDO approach requires several pre-conditions to be present for success. These are:

- *An organizational culture that is comfortable with making risk-based decisions.*
- *A mature organization whose processes operate at CMMI level-3 or higher. (This should not be an assertion, but independently verified by an outside organization.)*
- *Sufficient lead time to implement a technology platform and analytic tool suite based on NSA's Ghost Machine Cloud Reference Architecture (estimated to be 1 year).*

*If these conditions can be met, then organizations should consider a balanced approach of People, Processes and Technology to create an operational, secure **DevOps** environment patterned around the JIDO Concept of Operations.*

Reference: SecDevOps Concept of Operations, JIDO, 2017.

Most organizations do not normally operate in the high-tempo environment that supports combat missions and, consequently, do not have highly automated, agile processes that can respond to urgent requirements. Guidelines are needed for expediting urgent requests through the RMF process. However, for any set of guidelines to work efficiently, the following preconditions must be met.

1. *Provide acknowledgement that the organization submitting the urgent requirement has already completed a trade space analysis of mission need, timeliness, and affordability and has determined a desired delivery date.* The purpose of organizations tasked to satisfy the urgent requirement by the required delivery date is to operationalize the desired solution while minimizing risk to the DoD enterprise. The receiving organization must make every effort to support the required delivery data by expediting urgent requests in their processes.
2. *Create and maintain a system architecture for the baseline environment to include a tactical overlay*. The system architecture provides a starting point for any solution that will be placed in the network environment. It clearly shows the inherited controls for a solution, which can reduce the effort needed to prepare

the SSP. See Figure 4-1, below, for a notional architecture. For each system/subsystem in this architecture view, a matrix should be developed to allocate security controls by impact level (see Table 4-2).

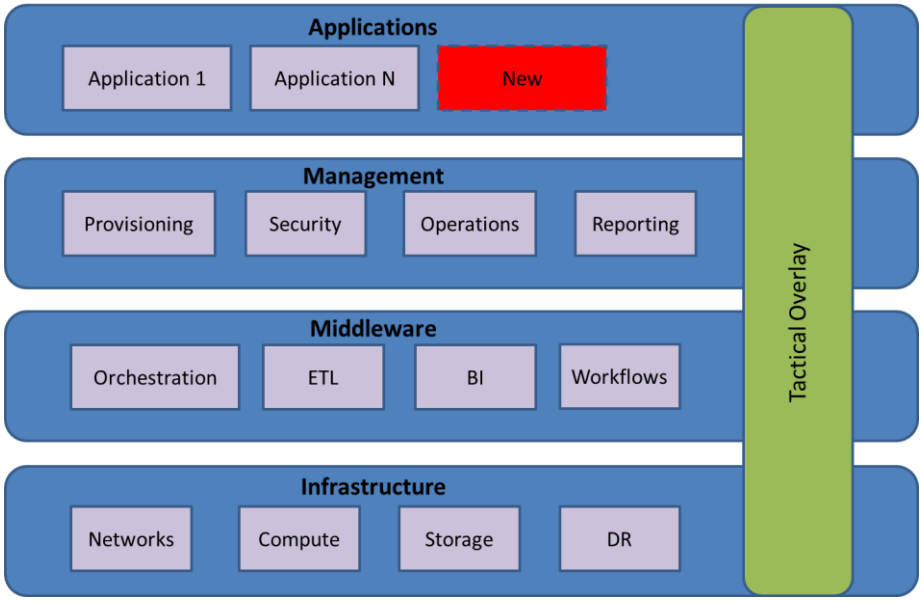


Figure 4-1. Notional Systems Architecture

Table 4-2. Allocation of Controls by System and Impact Level

Target Capability		Impact Level		
		Low	**Medium**	**High**
Existing ATO	AS-IS target environment by Infrastructure by Middleware by Management by Application	List controls	List controls	List controls
	Tactical Overlay by system layer	List controls	List controls	List controls
New ATO	Proposed application solution adds	Delta Controls	Delta Controls	Delta Controls

3. *Whenever practical, type-accredit all supporting IT infrastructure systems/subsystems to minimize the work required in developing the submitting organization's supporting SSP.* As part of this type-accreditation, make clear what security controls are allocated within the boundaries of these systems/subsystems. If a tactical overlay exists, add it to the AO's reference library.

4. *Create a quick reaction process with swim lanes and explicit timelines for each process and activity,* to include escalation procedures and swim lanes for each accountable organization and a dedicated swim lane for systems/technology used in the process. The processes should be optimized to grant an ATO for an urgent requirement within 30 days of receiving a request. The escalation process should describe the procedures and condition for escalating requests to the DoD ISRMC. Figure 4-2 provides a notional high-level swim lane.

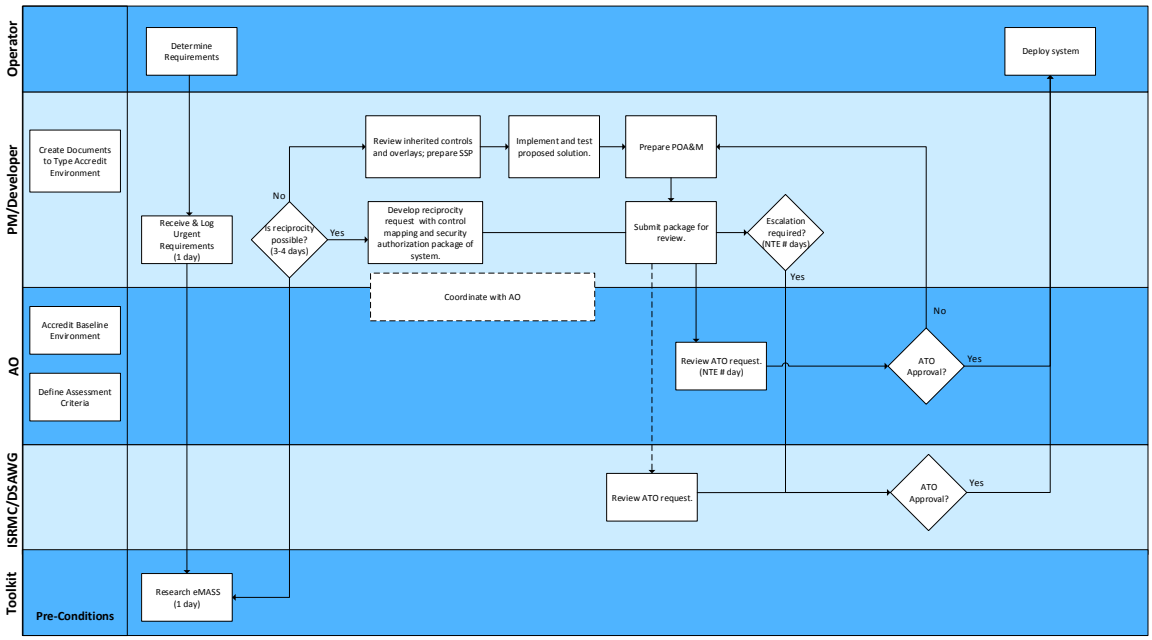


Figure 4-2. Notional High-Level Swim Lane and Process

5. *Define the assessment criteria and procedures to be used to determine that controls are implemented correctly and the solution is operating correctly*. Assessment criteria should be made available to PMs as part of a transparent approval process.

There are two scenarios in which an urgent or emerging capability requirement is invoked: (1) the submitting organization is the same as the receiving organization (intra-organizational ATO request) and (2) the submitting and receiving organization are different (inter-organizational ATO requests). For intra-organizational ATO requests, the IDA team proposes the following steps for completing the RMF process.

1. *Research eMASS and related sources to determine whether the proposed solution has been already deployed.*

   a. *If reciprocity is an option, request ATO reciprocity.* The PM should provide the AO with the security authorization package(s) for the system along with a

reciprocity request. The PM should make every effort to assist the AO staff by clearing mapping systems/subsystems boundaries in the proposed solution with the associated security controls to the same systems/subsystems in the already approved capability. In cases in which the impact level increases, mitigation steps should be clearly articulated. (See Recommendation B for suggested changes in eMASS to facilitate this step). Submit request to AO for review (step 6).

b. *If reciprocity is not an option, then superimpose the proposed solution onto the systems architecture (created in the preconditions listed above) and describe the controls that are inherited from the baseline or an overlay*, identifying all delta controls (i.e., controls whose impact level is greater than the inherited controls or controls that are not accounted for in the baseline). These delta controls must be addressed within the boundary of any proposed solution and should be the main focus of the AO's risk assessment. Prepare the SSP and have a preliminary discussion with the AO or AO's representative.

2. *Implement the proposed solution in the testing and development environment that models the target deployment environment*. Assess the security controls using assessment criteria (identified in the preconditions listed above), with the primary focus being on the delta between the controls identified in the target environment's system architecture and the solution. The results of this assessment are documented in the SAR.

3. *Coordinate with the AO, or the AO's representative, in the development of the SSP and SAR.* Early involvement of the AO is a critical success factor for streamlining the approval process. If the AO, or the AO's representative, is involved at the beginning of the RMF process, risks can be identified early and mitigated, making it less likely additional rework will be required when the request for ATO is submitted.

4. *Prepare POA&M describing the mitigation approach for reducing residual risks to an acceptable level.* The PO&AM describes actions to be taken to mitigate risks with timelines.

5. *Submit the SSP, SAR, and POA&M to the AO for an assessment of risk and the ATO determination.* As noted in Recommendation C, for urgent capabilities that require short, non-enduring ATO decisions, ATO requests should be submitted directly to the ISRMC. If this step is taken, the system owner will need to go through the DSAWG review process.

6. *The AO, or AO's representative, reviews the security authorization package, identifying any risks to the target environment.* If the risk is deemed acceptable, the AO authorizes the solution for deployment.
    a. *If the AO does not approve an authorization for deployment, then the PM is required to correct the gap(s),* returning to Step 4 in the process.
    b. *If an ATO decision in not made in a timely manner, the PM can escalate the decision to the Commander.* In the intra-organizational scenario, the network falls under the purview of the Commander, who can take responsibility for accepting the risks of the JUON/JEON on the network.
7. *Deploy solution to target environment and continuously monitor the effectiveness of the controls throughout the life of the system* in accordance with the information security continuous monitoring strategy. Any significant changes to the target solution should be identified in the change management processes. Go to Step 4 in the process.

The same process can be followed for an inter-organizational ATO request with modifications.

- Step 1: the PM should contact the AO of the target environment and coordinate with his staff to obtain the system architecture, the list of inherited security controls with associated impact levels, and the assessment criteria defined by the receiving organization prior to beginning the urgent and emerging capability RMF process.
- Step 5: the security authorization package for an emerging and urgent need should be submitted to both the AO and the DSAWG at the same time. If the AO does not provide a timely decision (i.e., within a period of time not to exceed a predetermined threshold) in Step 6.b, then the ATO request should be sent to the ISRMC. The ISRMC receives input from the DSAWG and makes the ATO decision.

Coordination, early and often, is a critical success factor for moving quickly through the RMF process. By leveraging overlays, inherited controls, and reciprocity, the PM can reduce the amount of time needed in the RMF process by shifting the focus from all controls, to only those controls that affect the target environment. While the target environment may be unknown when the requirement for an urgent or emerging capability is identified, once the target environment is identified, the PM should work closely with the AO, or AO's representative to gather knowledge of inherited security controls and discuss mitigation strategies for controls that exceed the impact level of the environment. Early coordination builds a better understanding of the solution in the receiving

organization and increases the confidence of the AO in the submitting organization's ability to meet security requirements.

Last, if the target deployment environment is a cloud service provider, then DoD should leverage the FedRAMP Agency Playbook[18] for specific steps and templates for creating the SSP, SAR, and POA&M.

[18] Federal Risk and Authorization Management Program (FedRAMP) streamlined the provisional authorization process for cloud service providers (CSP) to obtain an ATO. FedRAMP published a comprehensive guide to the authorization process. The FedRAMP Agency Authorization Playbook identifies best practices and tips in a 21-page document that outlines a step-by-step process for issuing an initial FedRAMP authorization. (https://www.fedramp.gov/introducing-the-new-agency-authorization-playbook/)

Distribution authorized to U.S. Government agencies only; Administrative or Operational Use 27 Mar 2018.
Other requests for this document shall be referred to OSD/A&S/DASD (C3CB).

Appendix A
References

Ref. #	Authority	Type	Topic	Excerpts
[1]	Title 44, Chapter 35, Subchapter II § 3551 (referred to as the Federal Information Security Modernization Act of 2014)	U.S. Code	Information Security - Purpose	Provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets.
[2]	Title 40, Chapter 113, Subchapter III, § 11331	U.S. Code	Responsibilities for Federal information systems standards	(1) In general.— (A) Requirement.—Except as provided under paragraph (2), the Director of the Office of Management and Budget shall, on the basis of proposed standards developed by the National Institute of Standards and Technology pursuant to paragraphs (2) and (3) of section 20(a) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(a)) and in consultation with the Secretary of Homeland Security, promulgate information security standards pertaining to Federal information systems. (B) Required standards.—Standards promulgated under subparagraph (A) shall include— (i) standards that provide minimum information security requirements as determined under section 20(b) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(b)); and (ii) such standards that are otherwise necessary to improve the efficiency of operation or security of Federal information systems.

Ref. #	Authority	Type	Topic	Excerpts
[3]	Title 44, Chapter 35, Subchapter II § 3553	U.S. Code	Information Security - Authority and functions of the Director and the Secretary	(a) DIRECTOR.—The Director shall oversee agency information security policies and practices, including— (1) developing and overseeing the implementation of policies, principles, standards, and guidelines on information security, including through ensuring timely agency adoption of and compliance with standards promulgated under section 11331 of title 40; (2) requiring agencies, consistent with the standards promulgated under such section 11331 and the requirements of this subchapter, to identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of— (A) information collected or maintained by or on behalf of an agency; or (B) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency; (e) DEPARTMENT OF DEFENSE AND INTELLIGENCE COMMUNITY SYSTEMS.— (1) The authorities of the Director described in paragraphs (1) and (2) of subsection (a) shall be delegated to the Secretary of Defense in the case of systems described in paragraph (2) and to the Director of National Intelligence in the case of systems described in paragraph (3). (2) The systems described in this paragraph are systems that are operated by the Department of Defense, a contractor of the Department of Defense, or another entity on behalf of the Department of Defense that processes any information the unauthorized access, use, disclosure, disruption, modification, or destruction of which would have a debilitating impact on the mission of the Department of Defense. (3) The systems described in this paragraph are systems that are operated by an element of the intelligence community, a contractor of an element of the intelligence community, or another entity on behalf of an element of the intelligence community that processes any information the unauthorized access, use, disclosure, disruption, modification, or destruction of which would have a debilitating impact on the mission of an element of the intelligence community.

Ref. #	Authority	Type	Topic	Excerpts
[4]	Title 44, Chapter 35, Subchapter II, § 3553	U.S. Code	Information Security - Authority and functions of the Director and the Secretary	(a) DIRECTOR.—The Director shall oversee agency information security policies and practices, including— (5) coordinating Government-wide efforts on information security policies and practices, including consultation with the Chief Information Officers Council established under section 3603 and the Director of the National Institute of Standards and Technology; (c) REPORT.—Not later than March 1 of each year, the Director, in consultation with the Secretary, shall submit to Congress a report on the effectiveness of information security policies and practices during the preceding year, including— (1) a summary of the incidents described in the annual reports required to be submitted under section 3554(c)(1), including a summary of the information required under section 3554(c)(1)(A)(iii); (2) a description of the threshold for reporting major information security incidents; (3) a summary of the results of evaluations required to be performed under section 3555; (4) an assessment of agency compliance with standards promulgated under section 11331 of title 40; and (5) an assessment of agency compliance with data breach notification policies and procedures issued by the Director. (d) NATIONAL SECURITY SYSTEMS—Except for the authorities and functions described in subsection (a)(5) and subsection (c), the authorities and functions of the Director and the Secretary under this section shall not apply to national security systems.
[5]	National Security Directive No. 42	Executive Directive	National Policy for the Security of National Security Telecommunications and Information Systems	5. The National Security Telecommunications and Information Systems Security Committee (NSTISSC) (redesignated the Committee on National Security Systems (CNSS) in 2001) b. The NSTISSC shall: (1) Develop such specific operating policies, procedures, guidelines, instructions, standards, objectives, and priorities as may be required to implement this Directive; (2) Provide systems security guidance for national security systems to Executive departments and agencies;
[6]	CNSSP 22	CNSS Policy	Cybersecurity Risk Management	FOREWARD The CNSS intends to adopt National Institute of Standards and Technology (NIST) issuances where applicable. Additional CNSS issuances will occur only when the needs of NSS are not sufficiently addressed in a NIST document. Annex B identifies the guidance documents, which includes NIST Special Publications (SP), for establishing an organization-wide risk management program.
[7]	CNSSI 1254	CNSS Instruction	Risk Management Framework Documentation, Data Element Standards, and Reciprocity Process for National Security Systems	SECTION I - PURPOSE 1. This Instruction creates a standard for data elements within RMF core documents to establish consistency and to facilitate reciprocity across the NSS community. 2. This Instruction derives the required RMF documents and standard data elements from NIST Special Publications 800-30, 800-37, 800-39, 800-53, and 800-53A.

Ref. #	Authority	Type	Topic	Excerpts
[8]	CNSSI 1253	CNSS Instruction	Security Categorization and Control Selection for National Security Systems	CHAPTER ONE 1. The National Institute of Standards and Technology (NIST) created NIST Special Publication (SP) 800-53, "Recommended Security Controls for Federal Information Systems and Organizations," to establish a standardized set of information security controls for use within the United States (U.S.) Federal Government. NIST collaborated with the Intelligence Community (IC), Department of Defense (DoD), and the Committee on National Security Systems (CNSS) to ensure NIST SP 800-53 contains security controls to meet the requirements of National Security Systems (NSS).2 As a result of these collaborative efforts, the Director of National Intelligence and the Secretary of Defense have directed that the processes described in NIST SP 800-53 (as amended by this Instruction) and the security and programmatic controls contained in Appendices F and G, respectively, shall apply to NSS within the National Security Community. This means NIST SP 800-53 now provides a common foundation for information security controls across the U.S. Federal Government.
[9]	DoDD 8000.01	DoD Instruction	Management of the Department of Defense Information Enterprise (DoD IE)	3. POLICY. It is DoD policy that: (g) (2) Provides for analyzing, selecting, controlling, and evaluating investments, as well as assessing and managing associated risks.
[10]	DoDI 8500.01	DoD Instruction	Cybersecurity	2. APPLICABILITY a. This instruction applies to: (1) OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the DoD, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this instruction as the "DoD Components"). (2) All DoD IT. (3) All DoD information in electronic format. (4) Special access program (SAP) information technology, other than SAP ISs handling sensitive compartmented information (SCI) material. 2. RISK MANAGEMENT a. Cybersecurity Risk Management. Managing cybersecurity risks is a complex, multifaceted undertaking that requires the involvement of the entire organization, from senior leaders planning and managing DoD operations, to individuals developing, implementing, and operating the IT supporting those operations. Cybersecurity risk management is a subset of the overall risk management process for all DoD acquisitions as defined in Reference (av), which includes cost, performance, and schedule risk associated with the execution of all programs of record, and all other acquisitions of DoD. The risk assessment process extends to the logistics support of fielded equipment and the need to maintain the integrity of supply sources. (1) DoD will use NIST SP 800-37 (Reference (ch)), as implemented by Reference (q), to address risk management, including authorization to operate (ATO), for all DoD ISs and PIT systems.

Ref. #	Authority	Type	Topic	Excerpts
[11]	FIPS 200	Federal Information Processing Standards	Minimum Security Requirements for Federal Information and Information Systems	Certification, Accreditation, and Security Assessments (CA): Organizations must: (i) periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.
[12]	DoDI 5000.02	DoD Instruction	Operations of the DoD Acquisition System	6. CYBERSECURITY a. Cybersecurity Risk Management Framework (RMF). Cybersecurity RMF steps and activities, as described in DoD Instruction 8510.01 (Reference (bg)), should be initiated as early as possible and fully integrated into the DoD acquisition process including requirements management, systems engineering, and test and evaluation. Integration of the RMF in acquisition processes reduces required effort to achieve authorization to operate and subsequent management of security controls throughout the system life cycle.

Ref. #	Authority	Type	Topic	Excerpts
[13]	DoDI 8510.01 (2007)	DoD Instruction	DoD Information Assurance Certification and Accreditation Process (DIACAP)	1. PURPOSE 1.4. Establishes a C&A process to manage the implementation of IA capabilities and services and provide visibility of accreditation decisions regarding the operation of DoD ISs, including core enterprise services- and Web services-based software systems and applications. 6. PROCEDURES 6.3.1. Initiate and Plan IA C&A. This activity includes registering the system with the governing DoD Component IA program, assigning IA controls based on Mission Assurance Category (MAC) and Confidentiality Level (CL), identifying the DIACAP Team for the IS, and initiating the IS's DIP. 6.3.2. Implement and Validate Assigned IA Controls. This activity includes executing the DIP, conducting validation activities, preparing the IT Security POA&M, and compiling the validation results in the DIACAP Scorecard. 6.3.3. Make Certification Determination and Accreditation Decision 6.3.4. Maintain Authorization to Operate and Conduct Reviews. Continued ATO is contingent on the sustainment of an acceptable IA posture. The DoD IS IAM has primary responsibility for maintaining situational awareness and initiating actions to improve or restore IA posture. 6.3.5. Decommission. When a DoD IS is removed from operation, a number of DIACAP-related actions are required. Prior to decommissioning, any inheritance relationships should be reviewed and assessed for impact. Once the system has been decommissioned, Lines 8, "DIACAP Activity," and 9, "System Life Cycle Phase," of the SIP should be updated to reflect the IS decommissioned status. Concurrently, the DIACAP Scorecard and any POA&Ms should also be removed from all tracking systems. Other artifacts and supporting documentation should be disposed of according to its sensitivity or classification. Data or objects in IA infrastructures that support the GIG, such as key management, identity management, vulnerability management, and privilege management, should be reviewed for impact. ENCLOSURE 2 - DEFINITIONS E2.22. DIACAP Package. The collection of documents or collection of data objects generated through DIACAP implementation for an IS. A DIACAP package is developed through implementing the activities of the DIACAP and maintained throughout a system's life cycle. Information from the package is made available as needed to support an accreditation or other decision such as a connection approval. There are two types of DIACAP packages: E2.22.1. The Comprehensive Package contains all of the information connected with the certification of the IS. It includes the System Identification Profile (SIP), the DIACAP Implementation Plan (DIP), the Supporting Certification Documentation, the DIACAP Scorecard, and the IT Security POA&M, if required. E2.22.2. The Executive Package contains the minimum information for an accreditation decision. It contains the SIP, the DIACAP Scorecard, and the IT Security POA&M, if required.
[14]	FIPS 199	Federal Information Processing Standards	Standards for Security Categorization of Federal Information and Information Systems	3 CATEGORIZATION OF INFORMATION AND INFORMATION SYSTEMS This publication establishes security categories for both information and information systems. The security categories are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization.

Ref. #	Authority	Type	Topic	Excerpts
[15]	CNSSI 1253	CNSS Instruction	Security Categorization and Control Selection for National Security Systems	3.2 SELECTING THE INITIAL SET OF SECURITY CONTROLS 28. The initial set of security controls for a system is selected on the basis of either its baseline security categorization or its designated control profile. 29. If a baseline security categorization is used, the initial control set is the aggregation of the controls identified in the tables provided in Appendix D and corresponds to the value determined for each security objective (confidentiality, integrity, and availability) of the system. 30. If a control profile is used, the initial set of security controls is identified in the profile. 3.3.2 Supplementing Controls 53. It is important for organizations to document the decisions made during the security control selection process, identifying the risk-based rationale for those decisions. This documentation is essential when assessing the overall security posture of information systems with respect to potential mission and/or business case impact. The implementation of any security control is intended to mitigate a risk, and the level of its implementation is set to the level of mitigation required to meet documented risk-tolerance thresholds. The resulting set of agreed-upon security controls, the supporting rationale for control selection decisions, and any NSS use restrictions must be documented in the SSP for the information system.

Ref. #	Authority	Type	Topic	Excerpts
[16]	NIST SP 800-53A	NIST Special Publication	Assessing Security and Privacy Controls in Federal Information Systems and Organizations	FORWARD Security control assessments and privacy control assessments are not about checklists, simple pass-fail results, or generating paperwork to pass inspections or audits—rather, such assessments are the principal vehicle used to verify that implemented security controls and privacy controls are meeting their stated goals and objectives. Special Publication 800-53A, Assessing Security and Privacy Controls in Federal Information Systems and Organizations, is written to facilitate security control assessments and privacy control assessments conducted within an effective risk management framework. The control assessment results provide organizational officials with: • Evidence about the effectiveness of implemented controls; • An indication of the quality of the risk management processes employed within the organization; and • Information about the strengths and weaknesses of information systems which are supporting organizational missions and business functions in a global environment of sophisticated and changing threats. 2.2 STRATEGY FOR CONDUCTING CONTROL ASSESSMENTS The conduct of security control assessments is the primary responsibility of information system owners and common control providers with oversight by their respective authorizing officials. The conduct of privacy control assessments is the primary responsibility of senior agency officials for privacy/chief privacy officers and privacy staff. There is also significant involvement in the assessment process by other parties within the organization who have a vested interest in the outcome of assessments. Other interested parties include, for example, mission/business owners, information owners/stewards (when those roles are filled by someone other than the information system owner), information security personnel, and designated privacy staff. It is imperative that information system owners and common control providers coordinate with the other parties in the organization having an interest in control assessments to help ensure that the organization's core missions and business functions are adequately addressed in the selection of security and privacy controls to be assessed. 2.1 ASSESSMENTS WITHIN THE SYSTEM DEVELOPMENT LIFE CYCLE Subsequent to the initial authorization, the organization assesses all implemented security controls on an ongoing basis in accordance with its Information Security Continuous Monitoring strategy.16 Privacy controls are also assessed on an ongoing basis to ensure compliance with applicable privacy laws and policies. The ongoing assessment and monitoring of security controls and privacy controls use the assessment procedures defined in this publication. The frequency of such assessments and monitoring is determined by the organization and/or information system owner or common control provider and approved by the authorizing official. Finally, at the end of the life cycle, security assessments are conducted to ensure that important organizational information is purged from the information system prior to disposal.

Ref. #	Authority	Type	Topic	Excerpts
[17]	NIST SP 800-37	NIST Special Publication	Guide for Applying the Risk Management Framework to Federal Information Systems	TASK 5-1: Prepare the plan of action and milestones based on the findings and recommendations of the security assessment report excluding any remediation actions taken. The *plan of action and milestones*, prepared for the authorizing official by the information system owner or the common control provider, is one of three key documents in the security authorization package and describes the specific tasks that are planned: (i) to correct any weaknesses or deficiencies in the security controls noted during the assessment; and (ii) to address the residual vulnerabilities in the information system. The plan of action and milestones identifies: (i) the tasks to be accomplished with a recommendation for completion either before or after information system implementation; (ii) the resources required to accomplish the tasks; (iii) any milestones in meeting the tasks; and (iv) the scheduled completion dates for the milestones. The plan of action and milestones is used by the authorizing official to monitor progress in correcting weaknesses or deficiencies noted during the security control assessment. All security weaknesses and deficiencies identified during the security control assessment are documented in the security assessment report to maintain an effective audit trail. Organizations develop specific plans of action and milestones based on the results of the security control assessment and in accordance with applicable laws, Executive Orders, directives, policies, standards, guidance, or regulations. Plan of action and milestones entries are not required when weaknesses or deficiencies are remediated during the assessment or prior to the submission of the authorization package to the authorizing official.

Ref. #	Authority	Type	Topic	Excerpts
[17a]	NIST SP 800-37	NIST Special Publication	Guide for Applying the Risk Management Framework to Federal Information Systems	RISK DETERMINATION TASK 5-3: Determine the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation. The authorizing official or designated representative, in collaboration with the senior information security officer, assesses the information provided by the information system owner or common control provider regarding the current security state of the system or the common controls inherited by the system and the recommendations for addressing any residual risks. Risk assessments (either formal or informal) are employed at the discretion of the organization to provide needed information on threats, vulnerabilities, and potential impacts as well as the analyses for the risk mitigation recommendations. The risk executive (function) also provides information to the authorizing official that is considered in the final determination of risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation and use of the information system. Risk related information includes the criticality of organizational missions and/or business functions supported by the information system and the risk management strategy for the organization. The risk management strategy typically describes: (i) how risk is assessed within the organization (i.e., tools, techniques, procedures, and methodologies); (ii) how assessed risks are evaluated with regard to severity or criticality; (iii) known existing aggregated risks from organizational information systems and other sources; (iv) risk response approaches; (v) organizational risk tolerance; and (vi) how risk is monitored over time. When making the final risk determination, the authorizing official or designated representative considers information obtained from the risk executive (function) and the information provided by the information system owner or common control provider in the security authorization package (i.e., security plan, security assessment report, and plan of action and milestones). Conversely, information system-related security risk information derived from the execution of the RMF is available to the risk executive (function) for use in formulating and updating the organization-wide risk management strategy. After risk determination, organizations can respond to risk in a variety of ways, including: (i) accepting risk; (ii) avoiding risk; (iii) mitigating risk; (iv) sharing risk; (v) transferring risk; or (vi) a combination of the above. Decisions on the most appropriate course of action for risk response include some form of prioritization. Some risks may be of greater concern than other risks. In that case, more resources may need to be directed at addressing higher-priority risks than at other lower-priority risks. This does not necessarily mean that the lower-priority risks are ignored. Rather, it could mean that fewer resources are directed at the lower-priority risks (at least initially), or that the lower-priority risks are addressed at a later time. A key part of the risk decision process is the recognition that regardless of the risk decision, there typically remains a degree of residual risk. Organizations determine acceptable degrees of residual risk based on organizational risk tolerance.

Ref. #	Authority	Type	Topic	Excerpts
[17b]	NIST SP 800-37	NIST Special Publication	Guide for Applying the Risk Management Framework to Federal Information Systems	TASK 5-4: Determine if the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation is acceptable. The *authorization decision document* conveys the final security authorization decision from the authorizing official to the information system owner or common control provider, and other organizational officials, as appropriate. The authorization decision document contains the following information: (i) authorization decision; (ii) terms and conditions for the authorization; and (iii) authorization termination date. The security authorization decision indicates to the information system owner whether the system is: (i) authorized to operate; or (ii) not authorized to operate. The terms and conditions for the authorization provide a description of any specific limitations or restrictions placed on the operation of the information system or inherited controls that must be followed by the system owner or common control provider. The authorization termination date, established by the authorizing official, indicates when the security authorization expires. Authorization termination dates are influenced by federal and/or organizational policies which may establish maximum authorization periods. Organizations may choose to eliminate the authorization termination date if the continuous monitoring program is sufficiently robust to provide the authorizing official with the needed information to conduct ongoing risk determination and risk acceptance activities with regard to the security state of the information system and the ongoing effectiveness of security controls employed within and inherited by the system.
[18]	DoDI 8510.01 Enclosure 6: Risk Management of IS and PIT Systems.	DoD Instruction	Risk Management Framework (RMF) for DoD Information Technology (IT)	4. SECURITY AUTHORIZATION DOCUMENTATION. The security authorization documentation consists of all artifacts developed through RMF activity. Security authorization documentation is maintained throughout a system's life cycle. The security authorization package consists of the security plan, SAR, POA&M, risk assessment report, authorization decision document, and is the minimum information necessary for the acceptance of an IS or PIT system by a receiving organization. Detailed information on the content of the security authorization package is available on the KS.
[19]	DoDI 8510.01 Enclosure 6: Risk Management of IS and PIT Systems.	DoD Instruction	Risk Management Framework (RMF) for DoD Information Technology (IT)	2. RMF STEPS e. Step 5 – Authorize System (4) Determine if the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation is acceptable. The product of this risk determination is the authorization decision. An authorization decision applies to a specifically identified IS or PIT system and balances mission need against risk to the mission, the information being processed, the broader information environment, and other missions reliant on the shared information environment. A DoD authorization decision is expressed as an ATO, an IATT, or a DATO. An IS or PIT system is considered unauthorized if an authorization decision has not been made. (a) If overall risk is determined to be acceptable, and there are no NC controls with a level of risk of "Very High" or "High," then the authorization decision should be issued in the form of an ATO. An ATO authorization decision must specify an ATD that is within 3 years of the authorization date unless the IS or PIT system has a system-level continuous monitoring program compliant with DoD continuous monitoring policy as issued.

Ref. #	Authority	Type	Topic	Excerpts
[20]	EXORD 13800	Executive Order	Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure	Section 1. Cybersecurity of Federal Networks. (c) Risk Management. (i) Agency heads will be held accountable by the President for implementing risk management measures commensurate with the risk and magnitude of the harm that would result from unauthorized access, use, disclosure, disruption, modification, or destruction of IT and data. They will also be held accountable by the President for ensuring that cybersecurity risk management processes are aligned with strategic, operational, and budgetary planning processes, in accordance with chapter 35, subchapter II of title 44, United States Code.
[21]	DoDI 8510.01 Enclosure 6: Risk Management of IS and PIT Systems.	DoD Instruction	Risk Management Framework (RMF) for DoD Information Technology (IT)	Enclosure 6 – Risk Management of IS and PIT systems 2(a)(2): All DoD IT that receive, process, store, display, or transmit DoD information. These technologies are broadly grouped as DoD IS, platform IT (PIT), IT services, and IT products. This includes IT supporting research, development, test and evaluation (T&E), and DoD controlled IT operated by a contractor or other entity on behalf of the DoD. 2(a)(2)(b). Nothing in this instruction alters or supersedes the existing authorities and policies of the Director of National Intelligence regarding the protection of sensitive compartmented information (SCI), as directed by Executive Order 12333 (Reference (l)) and other laws and regulations. The application of the provisions and procedures of this instruction to information technologies processing SCI is encouraged where they may complement or cover areas not otherwise specifically addressed. 2(b)(2)(b) Identifying overlays that apply to the IS or PIT system due to information contained within the system or environment of operation. Overlays may add or subtract security controls, or provide additional guidance regarding security controls, resulting in a set of security controls applicable to that system that is a combination of the baseline and overlay. The combination of baselines and overlays address the unique security protection needs associated with specific types of information or operational requirements. Overlays reduce the need for ad hoc or case-by-case tailoring by allowing COIs to develop standardized overlays that address their specific needs and scenarios. Access to the overlays, and guidance regarding how to determine which overlays may apply, are included in the KS. The KS is the authoritative source for detailed security control descriptions, implementation guidance and assessment procedures. 2(b)(2)(c) If necessary, tailor (modify) a control set in response to increased risk from changes in threats or vulnerabilities, or variations in risk tolerance. The resultant set of security controls derived from tailoring is referred to as the tailored control set. Tailoring decisions must be aligned with operational considerations and the environment of the IS or PIT system and should be coordinated with mission owner(s) and URs. Security controls should be added or removed only as a function of specified, risk-based determinations. Tailoring decisions, including the specific rationale (e.g., mapping to risk tolerance) for those decisions, are documented in the security plan for the system. Every selected control must be accounted for either by the organization or the ISO or PM/SM. If a selected control is not implemented, then the rationale for not implementing the controls must be documented in the security plan and POA&M. The tailoring process may include: 1. Applying scoping guidance to the initial set of security controls; 2. Selecting or specifying compensating controls to adjust the initial set of security controls to obtain an equivalent set deemed to be more feasible to implement; or 3. Specifying organization-defined parameters in the security controls via explicit assignment and selection statements to complete the definition of the tailored set of security controls.

Ref. #	Authority	Type	Topic	Excerpts
[22]	NIST SP 800-53 (Rev 5) Appendix G	NIST Special Publication	Recommended Security Controls for Federal Information Systems	
[23]	DoDI 8510.01 Enclosure 4: RMF Governance	DoD Instruction	Risk Management Framework (RMF) for DoD Information Technology (IT)	Enclosure 4 – RMF Governance 1(a) Tier 1 – Organization. For the purposes of the RMF, the organization described in Tier 1 is the OSD or strategic level, and it addresses risk management at the DoD enterprise level. The key governance elements in Tier 1 are: (1) DoD CIO. Directs and oversees the cybersecurity risk management of DoD IT. (2) Risk Executive Function (a) DoD Information Security Risk Management Committee (ISRMC) (formerly the Defense Information Systems Network (DISN)/Global Information Grid (GIG) Flag Panel). The DoD ISRMC performs the DoD Risk Executive Function as described in Reference (i). The panel provides strategic guidance to Tiers 2 and 3; assesses Tier 1 risk; authorizes information exchanges and connections for enterprise ISs, cross-MA ISs, cross security domain connections, and mission partner connections. (b) Defense IA Security Accreditation Working Group (DSAWG). The DSAWG, in support of the DoD ISRMC, is the community forum for reviewing and resolving authorization issues related to the sharing of community risk. The DSAWG develops and provides guidance to the AOs for IS connections to the DoD Information Enterprise. (5) The RMF TAG. The RMF TAG (formerly known as the DIACAP TAG) provides implementation guidance for the RMF by interfacing with the DoD Component cybersecurity programs, cybersecurity communities of interest (COIs), and other entities (e.g., DSAWG) to address issues that are common across all entities, by: (a) Providing detailed analysis and authoring support for the KS. (b) Recommending changes to security controls in Reference (f), security control baselines and overlays in Reference (e), DoD assignment values, and associated implementation guidance and assessment procedures to the DoD CIO. (c) Recommending changes to cybersecurity risk management processes to the DoD CIO. (d) Advising DoD forums established to resolve RMF priorities and cross-cutting issues. (e) Developing and managing automation requirements for DoD services that support the RMF. (f) Developing guidance for facilitating RMF reciprocity throughout the DoD. 1(c) Tier 3 – IS and PIT Systems (2) IS or PIT System Cybersecurity Program. The system cybersecurity program consists of the policies, procedures, and activities of the ISO, PM/SM, UR, ISSM, and IS security officers (ISSOs) at the system level. The system cybersecurity program implements and executes policy and guidance from Tier 1 and Tier 2, and augments them as needed. The system cybersecurity program is responsible for establishing and maintaining the security of the system, including the monitoring and

Ref. #	Authority	Type	Topic	Excerpts
				reporting of the system security status. Specific cybersecurity program responsibilities include: (a) ISOs must: 1. In coordination with the information owner (IO), categorize systems in accordance with Reference (e) and document the categorization in the appropriate JCIDS capabilities document (e.g., capabilities development document). 2. Appoint a UR for assigned IS and PIT systems. 3. Develop, maintain, and track the security plan for assigned IS and PIT systems. (Common security controls owner performs this function for inherited controls.) (b) PMs (or SM, if no PM is assigned) must: 1. Appoint an ISSM for each assigned IS or PIT system with the support, authority, and resources to satisfy the responsibilities established in this instruction. 2. Ensure each program acquiring an IS or PIT system has an assigned IS security engineer and that they are fully integrated into the systems engineering process. 3. Implement the RMF for assigned IS and PIT systems. 4. Ensure the planning and execution of all RMF activities are aligned, integrated with, and supportive of the system acquisition process. 5. Enforce AO authorization decisions for hosted or interconnected IS and PIT systems. 6. Implement and assist the ISO in the maintenance and tracking of the security plan for assigned IS and PIT systems. 7. Ensure POA&M development, tracking, and resolution. 8. Ensure periodic reviews, testing and assessment of assigned IS and PIT systems are conducted at least annually. 9. Provide the IS or PIT system description. 10. Register the IS or PIT system in the DoD Component registry. 11. Ensure T&E of assigned IS and IT system is planned, resourced, and documented in the program T&E master plan in accordance with DoDI 5000.02 (Reference (s)(r)).

Ref. #	Authority	Type	Topic	Excerpts
[24]	CNSSI 1254	CNSS Instruction	Risk Management Framework Documentation , Data Element Standards, and Reciprocity Process for National Security Systems	This Instruction creates a standard for data elements within RMF core documents to establish consistency and to facilitate reciprocity across the NSS community. a. RMF CORE DOCUMENTS - The following list of RMF core documents were collected from NIST SPs (see Foreword section) and consists of: 1) System Security Plan (SSP) is a formal document that provides an overview of the security requirements for a system and describes the security controls in place or plans for meeting those requirements; 2) Security Assessment Report (SAR) provides a disciplined and structured approach for documenting the findings of the assessor and recommendations for correcting any identified vulnerabilities in the security controls; 3) Risk Assessment Report (RAR) documents the results of the risk assessment or the formal output from the process of assessing risk. The risk assessment process is outlined in NIST 800-30; 4) Plan of Action and Milestones (POA&M) identifies tasks that need to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones1; and5) Authorization Decision Document conveys the final security authorization decision from the Authorizing Official (AO) to the Information System Owner (ISO) or common control provider, and other organizational officials, as appropriate Section 4 8(c): Reciprocity is the mutual agreement among participating organizations to share and/or reuse existing data and information included within the RMF core documents in support of authorization and risk management decisions. Annex D, 2(e): Organizations have the right to refuse participating in reciprocity with another organization, if the system's RMF core documentation is not considered complete enough to provide an informed understanding of potential or existing risks, or there would be excessive risk to the system or site, as determined by the system or site AO. Such decisions to refuse participation in reciprocity should be documented by the refusing AO, and provided, upon request, to the deploying organization's ISO or PM, AO, and organization Senior Information Security Officer (SISO), and to the refusing organization's Component SISO. Disputes should be resolved at the lowest possible level. Disputes that cannot be resolved will be raised to the next appropriate level.

Ref. #	Authority	Type	Topic	Excerpts
[25]	DoDI 8510.01 Enclosure 5: Cybersecurity Reciprocity	DoD Instruction	Risk Management Framework (RMF) for DoD Information Technology (IT)	Enclosure 5 – Cybersecurity Reciprocity 1.b Deploying systems with valid authorizations (from a DoD organization or other federal agency) are intended to be accepted into receiving organizations without adversely affecting the authorizations of either the deployed system or the receiving enclave or site. Deploying system ISOs and PMs must coordinate system security requirement with receiving organizations or their representatives early and throughout system development. 1.c. An authorization decision for IS or PIT system cannot be made without completing the required assessments and analysis, as recorded in the security authorization package. Deploying organizations must provide the complete security authorization package to receiving organizations. PMs/ ISOs deploying systems across DoD Components will post security authorization documentation to Enterprise Mission Assurance Support Service (eMASS) or other electronic means to provide visibility of authorization status and documentation to planned receiving sites. 2.a(2) (2) The DoD ISRMC, supported by the DSAWG, may make an enterprise level risk acceptance determination for authorized enterprise systems, which will satisfy the requirements of the first three elements of paragraph 1d of this enclosure. If the DoD ISRMC accepts the risk on behalf of the DoD Information Enterprise, the receiving organization may not refuse to deploy the system.
[26]	DoDI 5000.02	DoD Instruction	Operation of the Defense Acquisition System	• E11: 6.a. Cybersecurity RMF steps and activities, as described in DoD Instruction 8510.01 (Reference (bg)), should be initiated as early as possible and fully integrated into the DoD acquisition process including requirements management, systems engineering, and test and evaluation. • E11: 6.b. All acquisitions of systems containing IT, including NSS, will have a Cybersecurity Strategy. The Cybersecurity Strategy is an appendix to the Program Protection Plan (PPP) that satisfies the statutory requirement in section 811 of P.L. 106-398 (Reference (q)) for mission essential and mission critical IT systems. • E13: 3.a. MDAs and program managers will tailor and streamline program strategies and oversight. This includes program information, acquisition activity, and the timing and scope of decision reviews and decision levels. Tailoring and streamlining should be based on program complexity and the required timelines to meet urgent need capability requirements consistent with applicable laws and regulations. • E13: 4.c.(2) IT, including NSS, fielded under this enclosure require an Authority to Operate in accordance with DoD Instruction 8510.01 (Reference (bg)). DoD Component Chief Information Officers will establish processes consistent with DoD Instruction 8510.01 for designated approval authorities to expeditiously make the certification determinations and to issue Interim Authorization to Test or Authority to Operate.
[27]	AFI 17-101	Air Force Instruction	Risk Management Framework (RMF) for Air Force Information Technology	• AOs may issue an IATT, ATO, or an ATO with conditions for any risk not determined to be high or very high. (3.6.1) pg. 22 • If risk is determined to be high, then the SAF/CIO A6 is the only Air Force member who may grant IT to operate. There can be no delegation below the AF CIO. IT which are authorized by other DoD components connecting to AFIN require their component CIO approval and joint systems require DoD CIO approval. (3.6.2.1) pg. 22

Ref. #	Authority	Type	Topic	Excerpts
[28]	AFI 63-128	Air Force Instruction	Integrated Life Cycle Management	• Quick Reaction Capability (QRC) is specially designated by the MDA to urgent needs (UON, JUON, and Chief of Staff top-down direction). (15.22) • Rapid delivery – Schedule is paramount when executing a QRC program, and both cost and performance should be traded off respectively. Ideally, QRC programs should field an initial capability within 180 days of urgent need validation. (15.22) • MDA for ACAT II and III QRC programs is automatically delegated to the PEO. In addition, the process only specifies two formal MDA reviews: a MDD and a Capability Transition Review (CTR). (15.22) • The MDA must have a higher risk tolerance for QRC programs and be willing to leverage all regulatory/statutory authorities to field a rapid solution. The MDA needs build a strategy that manages risk within tight constraints. (15.22) • PMs must aggressively question requirements and deflect pressures to deliver more capability than is absolutely needed to mitigate the identified gap. Following initial fielding, there should be time to examine. The implementing command or Chief of Staff should endorse a course of action that extends beyond 180 days from urgent need validation to initial fielding. Long (>180 days) schedules should be the rare exception. (15.22) • QRC programs are tightly constrained by schedule and should likely use interim raw data to assess a capability's readiness for fielding. If the testing does not uncover critical issues that would preclude fielding, the lead command and PM should execute the fielding plan prior to receipt of final test reports. (15.22) • The AFROC has two decision-making responsibilities for Urgent/Emergent Needs in the QRC process. The AFROC is responsible for validating all UON requests, and the AFROC is responsible for providing an AF Corporate Review, through a Capabilities Transition Decision (CTD), for all UON/JUON/JEON fielded capabilities (7.3)

Distribution authorized to U.S. Government agencies only; Administrative or Operational Use 27 Mar 2018.
Other requests for this document shall be referred to OSD/A&S/DASD (C3CB).

Appendix B. Acquisition Instructions and Directives

In 2016, IDA completed an analysis identifying DoD Information Technology (IT) acquisition authorities using the IDA Text Analytics (ITA) capability. The capability ingested all available, machine-readable DoD issuances[19] (963) and analyzed and tagged the documents, sections, and paragraphs referencing IT acquisition authorities. The results provided a detailed understanding of how IT acquisition authority is spread and shared across the Department, to include the specific authoritative language for each office. Aspects of this analysis can be leveraged to inform the larger acquisition review needed.

The 2016 analysis provided an overview of the interconnections between DoD Instructions, Directives, and U.S. Code Title 10. Figure B-1 provides a visualization of these interconnections. The sheer number of issuances that could be affected by a Title 10 change informs the complexity of legislative adjustments and shows that manual reviews may no longer bepractical.

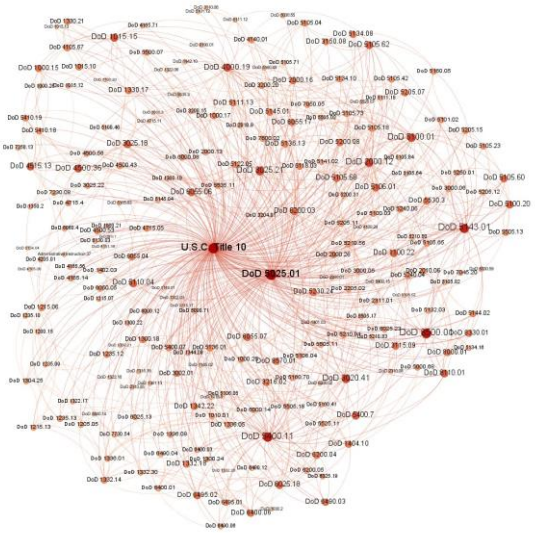


Figure B-1. Interconnections between U.S. Code Title 10 and DoD Issuances and Directives

[19] The tables and charts in this section are based on the data collected for a previous 2016 effort and do not reflect current data. Since the time of the analyses, 88 issuances have been updated and will need to be included in any future analysis.

The 2016 analysis revealed that many issuances are outdated and have not kept up with changes within the Department. Of the 963 issuances analyzed, 227 of them had not been updated in the last decade. Table B-1 provides a sample of the 227 issuances specific to acquisition policy, as well as the date they were last updated.

Table B-1. DoD Issuances without update in over a decade

Issuance	Date	S
DoDD5200.27	7-Jan-80	Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense
DoDD3230.3	14-Oct-86	DoD Support for Commercial Space Launch Activities
DoDD5505.5	30-Aug-88	Implementation of the Program Fraud Civil Remedies Act
DoDI6025.5	6-Jan-95	Personal Services Contracts (PSCs) for Health Care Providers (HCPs)
DoDI2015.4	7-Feb-02	Defense Research, Development, Test and Evaluation (RDT&E) Information
DoDD5000.01	12-May-03	The Defense Acquisition System
DoDD5134.3	3-Nov-03	Director of Defense Research and Engineering (DDR&E)
DoDI1015.13	11-Mar-04	DoD Procedures for Implementing Public-Private Ventures (PPVs) for Morale, Welfare and Recreation (MWR), and Armed Services Exchange Category C Revenue-Generating
DoDD4151.18	31-Mar-04	Maintenance of Military Materiel
DoDD1100.20	12-Apr-04	Support and Services for Eligible Organizations and Activities Outside the Department of Defense
DoDD8100.02	14-Apr-04	Use of Commercial Wireless Devices, Services, and Technologies in the Department
DoDI4165.71	6-Jan-05	Real Property Acquisition
DoDD5124.03	8-Jan-05	Armed Forces Tax Council
DoDD4270.34	12-Jan-05	Host Nation-Funded Construction Programs in the U.S. Pacific Command
DoDD4270.5	12-Feb-05	Military Construction
DoDD4275.5	15-Mar-05	Acquisition and Management of Industrial Resources
DoDD5500.20	28-Mar-05	Unified Legislation and Budgeting (ULB) Process
DoDI4165.69	6-Apr-05	Realignment of DoD Sites Overseas
DoDI4165.7	6-Apr-05	Real Property Management
DoDI2000.20	29-Aug-05	Cooperative Logistics Supply Support Arrangements
DoDI3210.1	16-Sep-05	Administration and Support of Basic Research by the Department of Defense
DoDI5134.04	27-Sep-05	Director of Small and Disadvantaged Business Utilization
DoDD8115.01	10-Oct-05	Information Technology Portfolio Management
DoDI2000.03	17-Jan-06	International Interchange of Patent Rights and Technical Information
DoDI8115.02	30-Oct-06	Information Technology Portfolio Management Implementation

The issuances in Table B-1 are good candidates to review for obsolete policy or outdated acquisition processes. Many outdated issuances exist department-wide and do not accurately reflect authority change. For example, as of 2016, more than 500 mentions of the Assistant Secretary of Defense for Networks and Information Integration ASD(NII) remain in more than 50 documents. More than 20 mentions of ASD(C3II), the office that preceded ASD(NII), remain. The ripple effect is not insignificant, and the inconsistency it presents, including the existence of disestablished offices throughout issuances, adds to the confusion across authorities and can add unnecessary layers to the bureaucracy.

New policy and guidance can often make past policy and guidance obsolete. During the IT acquisition authorities review, the IDA team was able to identify the sections within issuances that were likely obsolete and should be removed. Table

B-2 provides a summary of the obsolete passages identified with an associated citation and impacted authoritative office.

Table B-2. Proposed obsolete authorities in IT acquisition Issuances

Issuance	Office	Citation	S
DoDD 7045.20	AT&L	DoDD 7045.20 (2008), Enclosure 2, Table 1, pg 4	Capability portfolio management for Logistics, Protection, and Force application (shared with USD(P))
DoDD 8115.01	AT&L	DoDD 8115.01 (2005), para 5.2, pg 4.	Reviews, approves, and oversees the planning, design, acquisition, deployment, operation, maintenance, and modernization of the BMA portfolio of IT investments with the primary purpose of improving acquisition, logistics, or installation sn environment activities consistent with BMA guidance. Ensures policies for the IT PfM are incorporated into
DoDD 8115.01	AT&L	DoDD 8115.01 (2005), para 5.2.1.5, and .6, pg. 4	Participates in cross-Mission Area governance forum for the Enterprise portfolio. Participates in the WMA, DIMA, and
DoDD 8115.01	AT&L	DoDD 8115.01 (2005), para 5.2.1, pg 4	Coordinates with the DoD CIO, USD(C), and USD(P&R) to lead and manage the BMA portfolio
DoDD 8115.01	DCMO	DoDD 8115.01	Business Mission Area (BMA) portfolio management
DoDD 7045.20	DCMO	DoDD 7045.20 (2008), Enclosure 2, Table 1, pg 4	Capability Portfolio Manager for Corporate Management and Support Portfolio
DoDD 8115.01	DoD CIO (including as ASD(NII)	DoDD 8115.01	Enterprise Information Environment Mission Area (EIEMA) portfolio management lead
DoDD 8115.01	DoD CIO (including as ASD(NII)	DoDD 8115.01 (2005), para 5.1.1 through 5.1.3. pg 3	Establishes guidance for managing IT portfolios. Establishes and leads a cross-Mission Area governance for the Enterprise portfolio, identify opportunities for IT investments and resolve cross-Mission Area issues. Ensure that all mission area portfolio recommendations are based on architectures that comply with policy, Participates in the WMA, BMA and DIMA
DoDI 8580.	DoD CIO (including as ASD(NII)	DoDI 8580.1	Supports the Overarching Integrated Product Teams (OIPT) by ensuring that IA is included for consideration prior to all acquisition milestone decisions, program decision reviews, and
DoDI 8580.	DoD CIO (including as ASD(NII)	DoDI 8580.1	Establish and implement procedures for the review of Acquisition IA Strategies from programs acquiring mission
DoDD 3100.12	DoD CIO (including as ASD(NII)	DoDD 3100.12	Serves as the PSA and advisor to the SecDef and DepSecDef and focal point within the DoD for space support and related activities. Oversees the development pf space support, related architectures, and acquisition programs in support of USD(AT&L)
DoDI 8115.02	DoD CIO (including as ASD(NII)	DoDI 8115.02 (2006), para 5.3, pg 2-3.	Coordinates with USD(AT&L), USD(C), CJCS and Mission Area Leads to develop additional guidance for integration ot IT portfolio Management (PfM) activities in to the PPBS, Defense Acquisition System, and the JCIDs processes
DoDD 8115.01	USD(I)	DoDD 8115.01 (2005), para 5.5, pg 5	Mission area lead for Defense Intelligence Mission Area (DIMA). Establishes, issues guidance for managing the DIMA portfolio and designates responsibilities for management. Presents the DIMA portfolio recommendations to the proper officials in the DoD's decision support systems for
DoDD 8110.01	USD(I)	DoDD 8110.01 (2005), para 5.5.5. & 6, pg 6	Participates in cross-Mission Area governance forum for the Enterprise portfolio. Participates in the WMA, BMA, and EIEMA
DoDD 7045.20	USD(I)	DoDD 7045.20 (2008), Enclosure 2, Table 1, pg 4	Capability portfolio mgmt. for battlespace awareness Portfolio
DoDD 8115.01	USD(P&R)	DoDD 8115.01 (2005), para 5.4, pg 5	Participates in BMA governance forums with the goal of identifying commonality in BMA portfolio management processes and providing solutions that are in the best interest of the DoD. Review, approve, and oversee the planning, design, acquisition, deployment, operation, maintenance, and modernization of the BMA portfolio of IT investments with the primary purpose of improving human resource management

Issuance	Office	Citation	S
DoDD 7045.20	USD(P&R)	DoDD 7045.20 (2008), Enclosure 2, Table 1, pg 4	Capability portfolio manager for Force Support
DoDD 7045.20	USD(P)	DoDD 7045.20 (2008), Enclosure 2, Table 1, pg 4	Lead for Building Partnerships Capability Portfolio. Co-lead (with USD(AT&L)) for Force Application

This type of text analytics will help make sure that obsolete passages are identified and flagged for removal. Without eliminating these, officials could be taking action based on incorrect policy, and any recommended changes will not be based on accurate information. Although the removal of obsolete IT acquisition authorities is just a subset of the overall acquisition effort needed, it provides an initial list of actions that can be taken now.

Acronyms and Abbreviations

AIS	Automated Information System
AO	Authorizing Official
ASD(NII)	Assistant Secretary of Defense for Networks and Information Integration
ATO	Authorization to Operate
C&A	certification and accreditation
CNSSI	CNSS Instruction
CNSSP	CNSS Policy
COI	community of interest
CSP	cloud service providers
DAA	Designated Accrediting Authority
DATO	Denial of an Authorization to Operate
DIACAP	DoD Information Assurance Certification and Accreditation Process
DIP	DIACAP Implementation Plan
DISA	Defense Information Systems Agency
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DNI	Director of National Intelligence
DoD	Department of Defense
DoD IE	Department of Defense Information Enterprise
DoDD	Department of Defense Directive
DoDI	DoD Instruction
DSAWG	Defense Information Assurance Security Accreditation Working Group
eMASS	Enterprise Mission Assurance Support Service
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standards

FISMA	Federal Information Security Modernization Act
GFM DI	Global Force Management Data Initiative
IA	Information Assurance
IATO	Interim Authorization to Operate
IATT	Interim Authorization to Test
IC	Intelligence Community
IDA	Institute for Defense Analyses
IRSMC	Information Security Risk Management Committee
IS	information system
ISCM	Information Security Continuous Monitoring
ITA	IDA Text Analytics
ISO	Information System Owner
IT	Information Technology
ITIL	Information Technology Infrastructure Library
JIDO	Joint Improvised–Threat Defeat Organization
JTTF	Joint Transformation Task Force
JUON	Joint Urgent Operational Needs
NA	not applicable
NC	non-compliant
NIST	National Institute of Standard and Technology
NSD	National Security Directive
NSS	National Security Systems
OSD	Office of the Secretary of Defense
PIT	platform information technology
PK	Public Key
PKI	Public Key Infrastructure
PM	Program Manager
POA&M	Plan of Actions and Milestones
RAR	Risk Assessment Report

RFP	Request for Proposal
RMF	Risk Management Framework
SAR	Security Assessment Report
SIP	System Identification Profile
SP	Special Publication
SSP	System Security Plan
TAG	Technical Advisory Group
UC	Unified Capabilities
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology and Logistics
VoIP	Voice over Internet Protocol

Distribution authorized to U.S. Government agencies only; Administrative or Operational Use 27 Mar 2018.
Other requests for this document shall be referred to OSD/A&S/DASD (C3CB).

Bibliography

[i] Department of Defense Instruction 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT), Enclosure 6: Risk Management of IS and PIT Systems*, March 12, 2014.

[ii] Commons, D., "DITSCAP: DoD's Answer to Secure Systems," InfoSec Reading Room, SANS Institute, 2002, https://www.sans.org/reading-room/whitepapers/country/ditscap-dods-answer-secure-systems-669, Accessed January 26, 2018.

[iii] *Computer Security Act of 1987*, Pub. L. 100-235 (H.R. 145), January 8, 1988.

[iv] Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD(C3I)), DoDI 5200.40, *DoD Information Technology Security Certification and Accreditation Process(DITSCAP)*, December 30, 1997, http://www.acqnotes.com/Attachments/DoD%20Instruction%205200.40.pdf.

[v] DoDI 8500.02, *Information Assurance (IA) Implementation*, February 6, 2003, https://ia.signal.army.mil/docs/encl_4_i85002p.pdf.

[vi] DISA, Enterprise Mission Assurance Support Service (eMASS)," http://www.disa.mil/~/media/Files/DISA/Fact-Sheets/eMASS.pdf.

[vii] Joint Rapid Acquisition Cell (JRAC), DoD Directive 5000.71, *Rapid Fulfillment of Combatant Commander Urgent Operational Needs*, August 24, 2012.

[viii] Secretary of the Air Force/Acquisition, Air Force Pamphlet 63-128, *Integrated Life Cycle Management*, July 10, 2017.

Distribution authorized to U.S. Government agencies only; Administrative or Operational Use 27 Mar 2018.
Other requests for this document shall be referred to OSD/A&S/DASD (C3CB).

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE (DD-MM-YY)	2. REPORT TYPE	3. DATES COVERED (From – To)
00-03018	Final	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Streamlining the Risk Management Framework (RMF) Process for Urgent and Emerging Capabilities	HQ0034-14-D-0001
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBERS

6. AUTHOR(S)	5d. PROJECT NUMBER
Laura A. Odell, Cameron E. DePuy, J. Corbin Fauntleroy, Tyler C. Rabren, Miranda G. Seitz-McLeese	AA-5-4077
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESSES	8. PERFORMING ORGANIZATION REPORT NUMBER
Institute for Defense Analyses 4850 Mark Center Drive Alexandria, VA 22311-1882	D-8981

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR'S / MONITOR'S ACRONYM
Adam Nucci Cyber & Space Programs, DASD(C3CB), OUSD(AT&L) Rm. 5A924, Pentagon	DASD(C3CB)
	11. SPONSOR'S / MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution authorized to U.S. Government agencies only; Administrative or Operational Use 27 Mar 2018. Other requests for this document shall be referred to OSD/A&S/DASD (C3CB).

13. SUPPLEMENTARY NOTES

Project Leader: Laura A. Odell

14. ABSTRACT

The expansion of cybersecurity practices into Department of Defense (DoD) acquisitions, such as the Risk Management Framework (RMF), is intended to document and build cybersecurity into mission-critical acquisitions. Given that urgent and emerging capability acquisitions are granted rapid acquisition authorities because of a time-critical need, this report examines the question of whether the RMF process can be streamlined, adjudicated, or waived to meet the needed timely delivery to the warfighter. This report reviews statutory requirements and relevant policy and guidance for RMF implementation and makes recommendations for streamlining the RMF process for urgent and emerging capability acquisitions.

15. SUBJECT TERMS

Risk Management, JUON, JEON

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			John Garstka, Deputy Director
Unclassified	Unclassified	Unclassified	Unlimited	72	19b. TELEPHONE NUMBER (Include Area Code) 571-372-4973

Distribution authorized to U.S. Government agencies only; Administrative or Operational Use 27 Mar 2018.
Other requests for this document shall be referred to OSD/A&S/DASD (C3CB).

Distribution authorized to U.S. Government agencies only; Administrative or Operational Use 27 Mar 2018.
Other requests for this document shall be referred to OSD/A&S/DASD (C3CB).