INSTITUTE FOR DEFENSE ANALYSES

Recommendations for Improving Agility in Risk Management for Urgent and Emerging Capability Acquisitions – Quick Look Report

Laura A. Odell, *Project Leader*

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

October 10, 2017

IDA Non-Standard
NS D-8798

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

About This Publication

This work was conducted by the Institute for Defense Analyses (IDA) under contract HQ0034-14-D-0001, Project AA-5-4077, "Cyber Technical Baseline Automated Assessment," for the 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, Christopher R. Pavlak

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

Recommendations for Improving Agility in Risk Management for Urgent and Emerging Capability Acquisitions – Quick Look Report

Summary

This paper provides the results of an analysis of statutory and DoD requirements for risk management levied on urgent and emerging capability acquisitions. The IDA team reviewed statutory language and DoD policies and regulations for meeting risk management requirements and interviewed subject matter experts to support the analysis.

Based on our analysis, the IDA team recommends the following actions to streamline the Risk Management Framework (RMF) process for urgent and emerging capabilities:

- Develop a tactical overlay to emphasize appropriate tailoring of core minimum security controls that are relevant to the operational environment.
- Consider reciprocity first—emphasizing performance and operational value over a checklist or compliance methodology.
- Allow an urgent and emerging capabilities off-ramp for the Authority to Operate (ATO) decision and Authorizing Official (AO) review when mission need demands that the solution not be "late to need."

Background

In a September 22, 2017, memorandum, the USD(AT&L) requested inputs on suggested legislative changes in the area of acquisition across DoD to begin to address the NDAA directive. This includes:

(1) Identifying process requirements in acquisition statutes that hinder agile acquisitions;

(2) Identifying obsolete statutes; and

(3) Recommending any related statutory changes that should be considered to simplify or improve the agility of the defense acquisition systems.

Statutory Requirements for Risk Management

No statutory changes are needed to simplify or improve the agility of the defense acquisition systems for urgent and emerging capability acquisitions. However, some programs are not developing security authorization packages (including the ATO decision) that accurately reflect the operational situation. Overly risk-adverse postures may minimize the appropriate tailoring permitted and expected in the RMF guidance. 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.

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.[3] 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.[4]

DoD, as the CNSS chair, worked with the CNSS members (including 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 (National Institute of Standard and Technology (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 1253, *Security Categorization and Control Selection for National Security Systems*) that provided the security control requirements (baselines and overlays) for NSS. CNSS Instruction 1253 uses and points to an expanded NIST SP 800-53 as the controls catalog.[6] DoD published DoD Instruction 8510.10, *Risk Management Framework (RMF),* for DoD Information Technology (IT) to establish 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 Authority 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]

Recommendations for Streamlining the RMF Process

The expansion into DoD acquisitions of cybersecurity practices, such as the Risk Management Framework (RMF), provides cybersecurity requirements for mission-critical acquisitions. However, the development of RMF core documents (required by CNSS Instruction 1254, *Risk Management Framework Documentation, Data Element Standards, and Reciprocity Process for National Security Systems*, and DoDI 8510.10, Enclosure 6, Section 4) has become a compliance- rather than a performance-focused process, resulting in significant delays and increased costs when deploying urgent and emerging capabilities.[10] The content of the documents is driven by requirements of

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

[2] 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.

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.[11]

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 over 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 items] 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.

Recommendation 1. 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."[5]. The baselines have been adopted with some modification by CNSS and DoD. Not all controls apply to every risk level,[4] 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. Baselines contain a set of controls determined by the level of impact of a system with respect to the focus areas; they are one way of reducing the number of controls used in the RMF process.

DoDI 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT)*, allows the tailoring of security controls within the baseline as necessary. 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 Information Security Officer or

[4] 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.

program manager. If a selected control is not implemented, then the rationale for not implementing the controls must be documented in the security plan and Plan of Action and Milestones (POA&M)]."[7] 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." [5, Appendix G] 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 communities of interest (COIs) to develop standardized overlays that address their specific needs and scenarios."[7]

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 would apply to systems, or portions of systems, being created for use in or to 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 1 lists examples of security controls that might not be relevant or require modification in an operational environment.

New overlays can be developed. The RMF Technical Advisory Group (TAG) (formerly known as the DIACAP (DoD Information Assurance Certification and Accreditation Process) 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 [Defense Information Assurance Security Accreditation Working Group]) 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 [Chief Information Officer]."[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 the DoD. The RMF TAG should establish a working group, chaired by the Office of the Under Secretary of Defense for Acquisition, Technology and Logistics and with appropriate members of the Military Departments, to develop a tactical overlay for urgent and emerging capabilities. The RMF process should begin with the development of a tactical overlay. This first step reduces 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 have been approved by the CNSS.

Table 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
AT-2	AWARENESS TRAINING	Provide basic security and privacy awareness training to system users (including managers, senior executives, and contractors).	D-6/51
AT-4	TRAINING RECORDS	Document and monitor individual system security and privacy training activities, including basic security and privacy awareness training and specific role-based system security and privacy training; and…Retain individual training records.	D-6/52
AU-4	AUDIT STORAGE CAPACITY	Allocate audit record storage capacity to accommodate [Assignment: organization-defined audit record retention requirements].	D-6/56
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-8	VISITOR ACCESS RECORDS	a. Maintain visitor access records to the facility where the system resides for [Assignment: organization-defined time-period]; and b. Review visitor access records [Assignment: organization-defined frequency].	D-20/157
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

ID	Control Title	Description	CNSSI-1254 Cite/NIST SP800-53 Cite
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
PE-17	ALTERNATE WORK SITE	a. Determine and document the [Assignment: organization-defined alternate work sites] allowed for use by employees; b. Employ [Assignment: organization-defined security and privacy controls] at alternate work sites; c. Assess the effectiveness of security and privacy controls at alternate work sites; and d. Provide a means for employees to communicate with information security and privacy personnel in case of security or privacy incidents or problems.	D-20/161
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

Recommendation 2. 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 an ATO, CNSS encourages the reciprocal use of the RMF core documents and ATO decision whenever possible. CNSS Instruction 1254 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."[10]

"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."[8] 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."[9]

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.[5] 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."[8] 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."[8]

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

[5] DoDI 8510.01, Enclosure 5, Section 1.c

or existing risks, or there would be excessive risk to the system or site, as determined by the system or site AO."[10] 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, holding up deployment of the urgent or emerging capability.

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. Reciprocity has the potential to prevent duplication of effort and decrease the time to deployment.

Recommendation 3. Allow an urgent and emerging capabilities off-ramp for the ATO decision and AO review when 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."[7] 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 requires an Authority to Operate in accordance with DoD Instruction 8510.01."[13] 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.

This approach has become a time-consuming bureaucratic 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 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 [information systems], cross-Mission Area (MA) ISs, cross security domain connections, and mission partner connections." Commander, U.S. Strategic Command chairs the ISRMC. The committee is supported by the DSAWG, chaired by the Defense Information Systems Agency. 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.[9] This follows CNSSI 1253 guidance referencing NIST 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."[6] "If the DoD ISRMC accepts the risk on behalf of the DoD Information Enterprise, the receiving organization may not refuse to deploy the system."[8] During operations in Iraq and Afghanistan, when the ISRMC was the DISN/GIG Flag Panel, ATO decisions were made at the Flag Level.

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[7] for any risks that have not been addressed. The RMF core documents should be based on a minimum set of controls defined in an 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 weeks after submittal.
2. Submit the RMF to the ISRMC in parallel with submittal to the AO. Submitting to the IRSMC 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 a short, non-enduring[8] ATO decision, 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.

[6] 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.

[7] DoD 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 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."

[8] 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.

Authority 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 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
[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— (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.
[4]	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;
[5]	NIST 800-53	NIST Special Publication	Security and Privacy Controls for Information Systems and Organizations	This publication provides a catalog of security and privacy controls for federal information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats including hostile attacks, natural disasters, structural failures, human errors, and privacy risks.
[6]	DoDI 8500.01	DoD Instruction	Cybersecurity	Enclosure 3: 2 (a)(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. (p28)

Ref. #	Authority	Type	Topic	Excerpts
[7]	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
[8]	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.
[9]	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

Ref. #	Authority	Type	Topic	Excerpts
				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 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
[10]	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.
[11]	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.

Ref. #	Authority	Type	Topic	Excerpts
[12]	DoDD 5000.71	DoD Directive	Urgent Capability Acquisition	3. POLICY. It is DoD policy that: a(3) The solution must be rapidly executed, including completing any development (necessarily minimal, given the timeline), acquisition, identification and prioritization of funding, training, and fielding. (p2) e(2) Subject to statutes and regulation, UON processes will be optimized for speed and accept reasonable risk with regard to cost, performance and other doctrine, organization, training, materiel, leadership and education, personnel, and facilities considerations. Actions will be taken swiftly and senior leaders will ensure that staffing processes do not inordinately delay the fielding of critical capabilities. (p3) f. DoD Components will establish supporting policies and procedures, in accordance with Enclosure 2, for the expeditious identification, submission, evaluation, validation, and resolution of UONs and provide visibility to the Warfighter SIG of their efforts to resolve UONs. (p3)
[13]	DoDI 5000.02	DoD Instruction	Operation of the Defense Acquisition System	Enclosure 11: REQUIREMENTS APPLICABLE TO ALL PROGRAMS CONTAINING INFORMATION TECHNOLOGY (IT) 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. 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. Enclosure 13: RAPID ACQUISITION OF URGENT NEEDS 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. 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.

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE (DD-MM-YY) 10-10-17	2. REPORT TYPE Non-Standard	3. DATES COVERED (From – To)

4. TITLE AND SUBTITLE

Recommendations for Improving Agility in Risk Management for Urgent and Emerging Capability Acquisitions – Quick Look Report

5a. CONTRACT NUMBER

HQ0034-14-D-0001

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBERS

6. AUTHOR(S)

Laura A. Odell, Cameron E. DePuy, J. Corbin Fauntleroy, Tyler C. Rabren, Miranda G. Seitz-McLeese

5d. PROJECT NUMBER

AA-5-4077

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESSES

Institute for Defense Analyses
4850 Mark Center Drive
Alexandria, VA 22311-1882

8. PERFORMING ORGANIZATION REPORT NUMBER

NS D-8798

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Adam Nucci, C3 Cyber
OUSD AT&L
Room MC12E08, 4800 Mark Center Dr.

10. SPONSOR'S / MONITOR'S ACRONYM

OUSD AT&L

11. SPONSOR'S / MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

Project Leader: Laura A. Odell

14. ABSTRACT

This memorandum provides the results of an analysis of statutory and DoD requirements for risk management levied on Urgent and Emerging Capability Acquisitions. IDA reviewed statutory language and DoD policies and regulations for meeting risk management requirements and interviewed subject matter experts to support the analysis. Although no statutory changes are needed to simplify or improve the agility of the defense acquisition systems for urgent and emerging capability acquisitions, due to their risk-adverse posture, some programs are not taking advantage of the ability to tailor security authorization packages (including the ATO decision) to accurately reflect the operational situation. This memorandum recommends changes in DoD Instruction 8510.01 for streamlining the process for obtaining and authorization to operate (ATO) for urgent and emerging capability acquisitions.

15. SUBJECT TERMS

Risk Management, FISMA, ATO, Urgent and Emerging Capability Acquisition

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON Adam Nucci, C3 Cyber
a. REPORT Unclassified	b. ABSTRACT Unclassified	c. THIS PAGE Unclassified	Unlimited	16	19b. TELEPHONE NUMBER (Include Area Code) 703-695-7937