Integrating Cybersecurity into NAVAIR OTPS Acquisition

Thomas Combass
AIR 4843
Fleet Readiness Center Southeast
Jacksonville, FL

Arthur Shilling
AIR 4843
Fleet Readiness Center Southeast
Jacksonville, FL

***Abstract*—Assessment of cybersecurity vulnerabilities and associated risks is a prevalent and escalating requirement for the Operational Test Program Set (OTPS) acquisition and development communities. In August of 1992, the Defense Information Systems Agency (DISA) developed the Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP); an assessment process for all Department of Defense (DoD) information systems. The accreditation and requirements process was service-specific and system-centric. In July 2006, the DoD Information Assurance Certification and Accreditation Process (DIACAP) was distributed. DIACAP implemented enterprise-wide Information Assurance (IA) through a standardized set of IA controls with continuous monitoring and annual reviews of the system's security posture. The current process, implemented in May 2014, is the Risk Management Framework (RMF). RMF is a more dynamic and integrated process than its predecessors.**

Instead of DoD defined security controls, RMF uses the Committee on National Security Systems Instructions (CNSSI) and National Institute of Standards and Technology (NIST) publications for its risk assessment guidelines and security control references respectively. Under RMF, all Information Technology (IT) is placed into four broad categories. These categories are Information Systems (IS), Platform IT (PIT), IT services and IT products. Fundamentally, all DoD IT assets must be categorized, security controls tailored, and implemented for the specific asset. Operational Test Program Sets (OTPS) mainly fall into the category of PIT. However, there may be circumstances where OTPSs fall into the category of an IS or any number of ambiguous areas. Since only generic high-level guidance is provided to evaluate PIT, guidelines for evaluating PIT OTPSs will be summarized. Also, since not all OTPSs are PIT and it may not be immediately clear which system category an OTPS falls, guidelines will be created to define these systems for proper evaluation. For the majority of OTPSs during the acquisition lifecycle; risk categorization, control selection, and assessment will occur. Case studies of OTPSs will be analyzed and discussed; OTPS PIT, OTPS IS, and ambiguous examples. In each of these cases, the question of task dependence versus the definition of what makes a particular OTPS a PIT or IS will be explored.

Keywords—cybersecurity, risk, NAVAIR, OTPS, RMF,

I. Introduction

With the increasing number of cyber-attacks from external adversaries and insider threats, implementing risk reduction strategies for damage or theft of information to defense and national security assets becomes a necessity. Most consider 'hacking' as being associated with a personal computer or corporate network commonly used for everyday information exchange and storage. In reality, any Information Technology (IT) asset able to contain, process, transmit or receive information could be attacked. Objects such as embedded systems can be vulnerable. For example, an Operational Test Program Sets (OTPS) containing random access memory or field programmable gate arrays could be susceptible to virus injection resulting in stack overflows and loss of capabilities.

A risk reduction solution to cyber-attacks was developed in 1992 by DISA. This process was labeled the Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) [1]. DITSCAP consisted of four phases; definition, verification, validation and post accreditation. It was independent of the life cycle of the asset. DITSCAP was designed for incorporation into any product life cycle, independent of the cycle phase. The DoD Information Assurance Certification and Accreditation Process (DIACAP) was established by DISA in July of 2006. DIACAP introduced Information Assurance (IA) and its concepts. DIACAP is similar to DITSCAP in its implementation with the exception of IA controls instead of unique system security requirements. The security controls within DIACAP have a broader scope compared to DITSCAP. These controls were standardized at the DoD level and apply to all DoD IT assets versus being system-centric.

While risk reduction was involved in the two aforementioned processes, total risk management was not extensively emphasized as in the Risk Management Framework (RMF). DISA established RMF in March 2014 as a next step in the evolution of information security risk management. RMF assembles an encompassing cradle to grave concept into the acquisition lifecycle process providing standardized risk categorization and security controls at a national level.

II. Risk Management Framework

RMF applies to all IT within all DoD service components (Navy, Army, etc.). DoD and RMF policies are depicted in Figure 1. Department of Defense Instruction (DoDI) 8500.01 [2], Cybersecurity (CS), supersedes the Information Assurance program and establishes the Cybersecurity program. DoDI 8510.01 [3], Risk Management Framework (RMF) for DoD Information Technology details the RMF process. Secretary of the Navy Instruction (SECNAVINST) 5239.3C [4], Department of the Navy Cybersecurity Policy, establishes CS policy consistent with the DoD. Chief of Naval Operations

978-1-5090-0790-5/16/$31.00 ©2016 IEEE

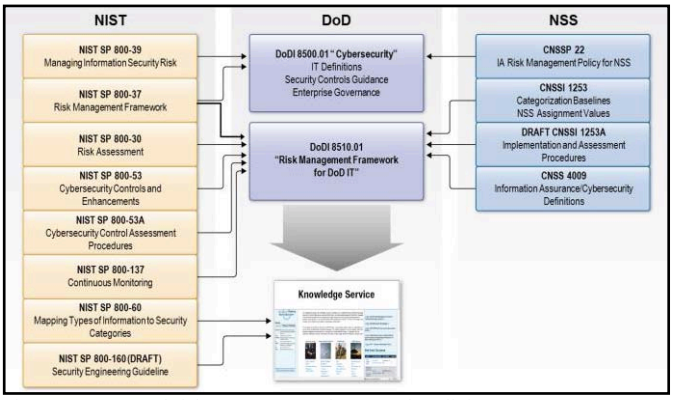


Figure 1. DoD and risk management framework policies

Instruction, OPNAVINST 5239.1D [5] will detail how RMF policy applies to the U.S. Navy. All DoD IT capable of transmitting, storing, receiving or processing information must abide by the full RMF process. Any exceptions will be analyzed on a case-by-case basis. Incorporating RMF early and robustly into an acquisition life cycle reduces the risk of a cybersecurity threat. It emphasizes risk awareness and resilience of the system as central. The RMF process has six steps, illustrated in the Figure 2.

RMF is designed for integration into the acquisition lifecycle from inception to termination of the product. RMF consists of six steps: 1) risk categorization, 2) control selection, 3) control implementation, 4) security control assessment, 5) authorization and 6) monitoring. The first step entails documenting personnel, business areas, a national security system determination, and information types. With this information, a security category and provisional risk impact values can be assigned. This information is entered into the Enterprise Mission Assurance Support Service (eMASS) system. Baseline control selection and tailoring of those controls occur next. A security plan and an Information System Continuous Monitoring (ISCM) are initiated as well as a Security Assessment Plan (SAP). Security controls selection is then evaluated. Security control implementation is documented and the Risk Assessment Report (RAR) is initiated. The fourth step involves a security control assessment. The assessment is documented within the

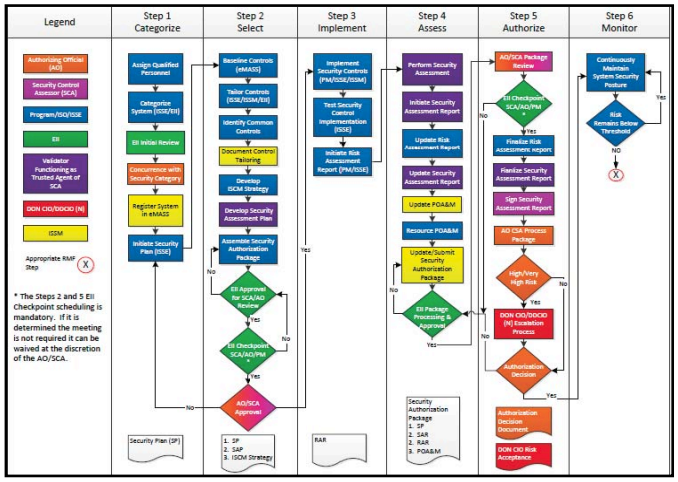


Figure 2. Risk Management Framework Process

Security Assessment Report (SAR) by a Security Control Assessor (SCA). Detailed conclusions of each control are then documented within a Plan of Action and Milestones (POA&M). Authorization involves review of the security package by the Functional Authorizing Official (FAO), resulting in an authority to operate (ATO), interim authority to test (IATT), or a disapproval of authority to operate (DATO). Finally, periodic observation of the asset for Cybersecurity policy compliance is imparted. The workflow for these steps is illustrated in the Figure 2.

III. OTPS RMF Overview

As avionics and its associated support equipment become more technically advanced, the information contained within this technology is increased both in quantity and complexity. A need to protect this information through the incorporation of the RMF process within OTPS acquisition arises. RMF integration starts with the mission gap analysis and continues throughout the acquisition lifecycle to include demilitarization. Procurement packages, programmatic, engineering, and logistical documentation should include verbiage to address cybersecurity and risk reduction strategy implementation in maturing system documentation.

With the DIACAP process, all cybersecurity requirements were contained within the Program Protection Plan (PPP) as an appendix. An initial programmatic assessment still occurs with the PPP, but in a NAVAIR OTPS acquisition a Cybersecurity Plan (CSP) directly addresses cyber threats. Created by the government acquisition Integrated Product Team (IPT), the CSP denotes typical items found in the IA section of the PPP; conceivable system threats, potential resolution strategies, and risk reduction. A Cybersecurity Implementation Plan (CSIP) shall be created by the OTPS development team to address cybersecurity risks. This document shall expand in maturity and detail as the total system design develops.

The integration of RMF will take place throughout the entire NAVAIR OTPS procurement, development, and sustainment process. RMF within the U.S. Navy consists of two processes, the Centralized Authorizing Official route (CAO) and the Functional Authorizing Official (FAO) route. Defense business systems or highly visible, DoD Information Network (DoDIN) connected systems are processed by the CAO approval process. Systems not connected to the DoDIN and considered Platform IT (PIT) are administered through the FAO process. NAVAIR OTPSs fall under the FAO process.

For RMF integration into the OTPS acquisition process, each of the process steps should coincide or be iterated with a system engineering technical review (SETR) or audit. Figure 3 suggests an alignment of acquisition milestone events with RMF process steps.

Before proceeding, feasibility of applying the RMF process to OTPS development should be considered. If the system does not transmit, receive, store, or process information, it may constitute a suspension and the process could cease at this point. Otherwise, OTPSs that transmit, process, store, or receive information must proceed through the entire RMF process.

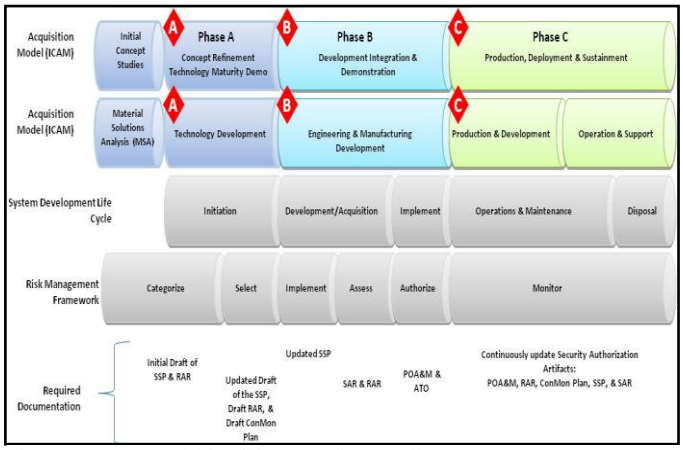


Figure 3. DoD acquisition lifecyce and RMF alignment

ID	TITLE	Confidentiality			Integrity			Availability		
		L	M	H	L	M	H	L	M	H
AC-1	Access Control Policy and Procedures	X	X	X	X	X	X	X	X	X
AC-2	Account Management	X	X	X	X	X	X			
AC-2(1)	Account Management | Automated System Account Management		X	X		X	X			
AC-2(2)	Account Management | Removal of Temporary / Emergency Accounts		X	X		X	X			
AC-2(3)	Account Management | Disable Inactive Accounts		X	X		X	X			
AC-2(4)	Account Management | Automated Audit Actions	+	X	X	+	X	X			
AC-2(5)	Account Management | Inactivity Logout							+	+	X
AC-2(6)	Account Management | Dynamic Privilege Management									
AC-2(7)	Account Management | Role-Based Schemes	+	+	+	+	+	+			
AC-2(8)	Account Management | Dynamic Account Creation									
AC-2(9)	Account Management | Restrictions on Use of Shared Groups / Accounts	+	+	+	+	+	+			
AC-2(10)	Account Management | Shared / Group Account Credential Termination	+	+	+	+	+	+			
AC-2(11)	Account Management | Usage Conditions									
AC-2(12)	Account Management | Account Monitoring / Atypical Usage	+	+	X	+	+	X			
AC-2(13)	Account Management | Disable Accounts For High-Risk Individuals	+	+	X	+	+	X			
AC-3	Access Enforcement	X	X	X	X	X	X			

Figure 4. Security controls baseline example

A. OTPS Risk Management Framework: Step One

Step one of the RMF process is categorization. System categorization is a significant step in the RMF and is required at system inception. System categorization influences the controls to be applied later. Categorization consists of documenting RMF personnel, business mission areas, operational impacts, and information types processed. Also, a National Security System (NSS) determination, selection and review of provisional impact values, security category assignments, category concurrence, and eMASS registration occur. This step aligns with the System Requirements Review One (SRR-I) acquisition milestone. SRR-I is primarily held for internal Government concurrence with all requirements prior to the release of the Request for Proposal (RFP). The eMASS record containing the initial CSP and description of the security category will be initiated. All information from this step will reside on the system categorization form. As with all acquisition efforts, intricacies of entrance and exit criteria should be tailored according to program scope and detailed within the Systems Engineering Plan (SEP).

Detailing the process of RMF Step I; the Program Manager (PM) is responsible for assigning personnel to appropriate roles. All assigned personnel must adhere to DoD and U.S. Navy training requirements [6]. Assignments include a PM, Information System Owner (ISO), Information System Security Manager (ISSM), Information System Security Officer (ISSO), User Representative, eMASS Information System Security Engineer (ISSE), Functional Security Control Assessor (FSCA) Liaison, FSCA Representative and the FAO Cybersecurity Analyst (CSA). All roles may or may not be assigned and personnel may occupy more than one role. The business or mission area of an OTPS is positioned in the Warfighting Mission Area (WMA) as it supports a weapons system. This information will later be used to assess risk and categorize the system. A NSS determination is required for the OTPS. This classification constitutes a higher risk category and application of more stringent security controls. The criteria questions for NSS determination are listed on the RMF Knowledge Service (KS) [7]. If 'Yes' is answered to any question listed, the system is NSS. If the system is deemed classified for any reason, then it is automatically a NSS. Operational impact is also used to determine categorization. It describes the processes if data were lost and the resulting level of impact to the OTPS.

Documenting what types of information are processed aids in determining system category and risk level. Information types at the Navy level can be researched on the Navy Information Types Baseline (NITB) [7] on the RMF KS at the DoD level or within the NIST SP 800-60, Volumes 1 & 2 [8], at the national level. Information types within the NITB are derived from the NIST SP 800-60 [8]. Multiple information types are possible and probable within an OTPS. Three security objectives are to be assessed when selecting provisional impact values. These objectives are confidentiality, integrity, and availability (C, I, & A). Impact values are measured as low, moderate, and high. Baseline impact values for each of the security objectives can be found in the NITB or can be found at a generic level within the NIST SP 800-60, Volumes 1 & 2 [8]. The impact levels should be reviewed and adjusted based on system security, personnel access, and specific informational requirements. Risk levels within the NITB are only baseline recommendations and should be adjusted to risk or mission needs. A security category is chosen by selecting the highest rating from the three security objective ratings seen from the information baseline. If multiple information types will be used within an OTPS, the highest of each of the categories are used to determine an aggregate risk level. For example (Figure 3), if information types were labeled as follows; $[C,I,A]1 = [L,M,L]_1$, $[C,I,A]_2 = [L,M,M]_2$, and $[C,I,A]_3 = [H,L,L]_3$, the aggregate risk level (ARL) is $[C,I,A]_{ARL} = [H,M,M]ARL$. Receiving concurrence from the FAO CSA and registering the system within eMASS concludes step one.

Figure 5. Three-tiered common control model

B. OTPS Risk Management Framework: Step Two

Security controls are safeguarding instructions for an information system. Controls selection involves the information previously gathered about information types and risk levels. DoD level controls are selected, tailored, and overlays applied, if one exists for the system. Overlays are a set of pre-tailored controls used for a specific type of system. Currently, there is no overlay written for OTPSs. A generic overlay is in development by the NAVAIR Generic OTPS Request for Proposal (NGOR) Integrated Product Team (IPT) with Cybersecurity subject matter expert (SME) assistance. Since there is not an overlay, the controls selected must be tailored in their entirety. The number of controls is determined by the security categorization. Naturally, low level categorizations result in fewer controls, while higher categorizations increase controls.

Security controls provide a consistent process throughout an organization. How the controls are interpreted and implemented is determined by the individual organization. Within RMF there are three levels of common security controls; DoD, Component, and Organization. These levels are illustrated in Figure 4. Controls for all federal agencies originate from NIST SP 800-37 [9].

The DoD has established a set of common controls from this publication. These controls can be found on the RMF KS [7]. The Department of the Navy (DON) level controls are currently in the process of being published. System baseline controls are based upon the security category chosen from the RMF KS in the security control explorer. Selection is accomplished by identifying the C, I, & A rating assigned to the information type selected from the NITB. Because the controls are from RMF KS, the controls selected are all DoD-level controls. Overlays can help tailor a control set or add needed security for a system. The overlay being developed will provide increased control granularity for OTPSs. Other software assurance processes such as digital signing, hash checking, and encryption are being considered to reduce risk.

Identifying control inheritance is a fundamental stage of applying the RMF. Inherited controls originate from systems already possessing an ATO. The system seeking authorization shall pursue communication with the authorized system. Usually, a memorandum of agreement (MOA), memorandum of understanding (MOU) or an interconnection agreement with written concurrence from both entities is established for founded controls usage. Not all inherited controls are applicable. However, sufficient justification for non-applicability should exist. Since all OTPSs interact with ATE, the OTPS will inherit some of the ATEs' security controls. Thus, an MOA must be established through Program Management Air (PMA) 260, Common Aviation Support Equipment Program Office, and the weapons system platform PMA. Tailoring the common set of controls for the specific system is vital. Tailoring involves analyzing the controls to determine which are relevant in risk reduction. Justification must be provided for those controls chosen as not applicable. Also, these controls should be translated into requirements for the systems integrator.

The ISCM is drafted and approved during this step to detail controls use monitoring, roles, and responsibilities. Most system monitoring transpires automatically through existing, approved software, or annually if manual monitoring is required. The FCSA evaluates the security control selections in the CSIP and verifies accuracy and non-applicability justification. A SAP is then developed by the FSCA with input from the ISSM and ISSE. The SAP contains the procedures and tools used to assess the controls. The FAO CSA reviews, comments, concurs/denies, and signs the SAP. The CSIP is updated with all relevant information.

C. OTPS Risk Management Framework: Step Three

Security controls implementation engages the chosen controls. Initiation begins with translating controls into verifiable requirements for developer design application. Preliminary controls testing shall be conducted during OTPS development. Controls are monitored for progress and re-evaluation during design and development. Testing may reveal fault or vulnerabilities prior to formal test. A RAR shall document all non-compliant controls unable to be corrected or mitigated preceding the formal assessment. Control implementation shall be documented in the CSIP.

D. OTPS Risk Management Framework: Step Four

Security controls Assessment is formal assessment of all determined controls. An FSCA performs the security control assessment and records the results, including any peculiarities. All controls are assessed as compliant (C), non-compliant (NC), or not applicable (NA). Noncompliant controls shall be annotated in the SAR which also records the results of the assessment and risk of NC controls. NC and NA controls are not only notated in the SAR, but the POA&M will also record deficiencies, compliance, and overall status of the security controls of the system. It will later be used for the cybersecurity lifecycle management of the system. The FSCA creates an Executive Summary Report recording the system risk and recommended corrections.

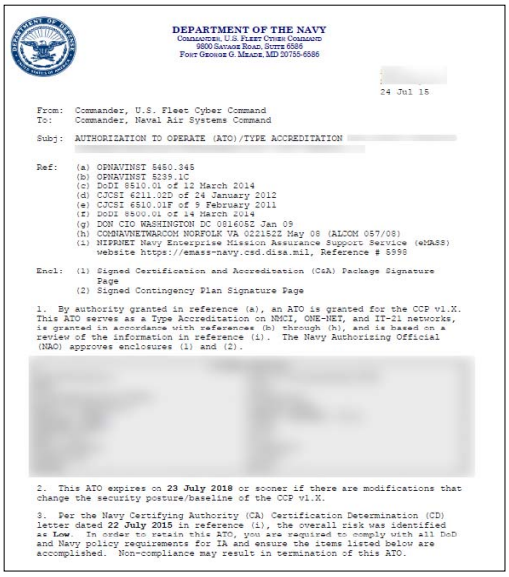
After the FSCA evaluates the OTPS a SAR is created. All conformance and non-compliance of controls are documented within a POA&M. The ISSE with assistance from the FSCA will then formulate a way to mitigate the risks from the controls outlined in the POA&M. Then, the FSCA presents their recommendation and accompanying security assessment package to the AO for an ATO.

E. OTPS Risk Management Framework: Step Five

Authorization consists of a Security Assessment Package review, the decision, and the authorization document. This package is reviewed by the FAO culminating in an authorization decision. The FAO determines if the system has acceptable cyber risks. The authorization decision will come in one of three forms; an ATO, an IATT, or a disapproval. ATOs are commonly issued if all risks and controls are within normal parameters. IATTs are issued when the system under review needs to begin testing with an authorized system. Disapprovals are issued when cyber risk is unacceptable.

F. OTPS Risk Management Framework: Step Six

The ISCM strategy shall be implemented annually at a minimum. The FSCA reviews the strategy against the system and forwards the findings to the FAO and ISSM for review and compliance determination. If the system is not found to be compliant, the ATO, illustrated in Figure 6, may need to be downgraded or the system re-accredited. This is the final stage and is after the system has been approved to operate. Monitoring is a necessity for system risk reduction and to maintain authorized compliance.



DEPARTMENT OF THE NAVY
COMMANDER, U.S. FLEET CYBER COMMAND
9800 SAVAGE ROAD, SUITE 6586
FORT GEORGE G. MEADE, MD 20755-6586

24 Jul 15

From: Commander, U.S. Fleet Cyber Command
To: Commander, Naval Air Systems Command

Subj: AUTHORIZATION TO OPERATE (ATO)/TYPE ACCREDITATION

Ref: (a) OPNAVINST 5450.345
(b) OPNAVINST 5239.1C
(c) DoDI 8510.01 of 12 March 2014
(d) CJCSI 6211.02D of 24 January 2012
(e) CJCSI 6510.01F of 9 February 2011
(f) DoDI 8500.01 of 14 March 2014
(g) DON CIO WASHINGTON DC 091605Z Jan 09
(h) COMNAVNETWARCOM NORFOLK VA 022152Z May 08 (ALCOM 057/08)
(i) NIPRNET Navy Enterprise Mission Assurance Support Service (eMASS) website https://emass-navy.csd.disa.mil, Reference # 5998

Encl: (1) Signed Certification and Accreditation (C&A) Package Signature Page
(2) Signed Contingency Plan Signature Page

1. By authority granted in reference (a), an ATO is granted for the CCP v1.X. This ATO serves as a Type Accreditation on NMCI, ONE-NET, and IT-21 networks, is granted in accordance with references (b) through (h), and is based on a review of the information in reference (i). The Navy Authorizing Official (NAO) approves enclosures (1) and (2).

2. This ATO expires on **23 July 2018** or sooner if there are modifications that change the security posture/baseline of the CCP v1.X.

3. Per the Navy Certifying Authority (CA) Certification Determination (CD) letter dated **22 July 2015** in reference (i), the overall risk was identified as **Low**. In order to retain this ATO, you are required to comply with all DoD and Navy policy requirements for IA and ensure the items listed below are accomplished. Non-compliance may result in termination of this ATO.

Figure 6. Authorization to operate

IV. CONCLUSION

Integration of Cybersecurity into the OTPS acquisition and procurement process is streamlined following the Risk Management Framework. Cybersecurity risks cannot be eliminated in totality, but early implementation of the process should reduce cyber threats to acceptable levels. Cybersecurity controls can be transformed into requirements during the development phase and implemented during OTPS integration. Moving Cybersecurity consideration earlier in the development cycles will reduce systemic risk and deliver cyber hardened products to the Warfighter. Detailed information on the RMF process can be found at the Risk Management Framework Knowledge Service.

ACKNOWLEDGMENT

The authors would like to thank the following people for their technical expertise and overall support: Chris Dosch, PMA260, Patuxent River, Maryland; Dr. Christopher Heagney, AIR 4.0T, Jacksonville, Florida; David Rolke, AIR 4.5, Jacksonville, Florida; William Heyn, AIR 4.8, Jacksonville, Florida.

REFERENCES

[1] *DoD Information Technology Security Certification and Accreditation Process (DITSCAP),* DoD Instruction 5200.40, December 1997

[2] *Cybersecurity*, DoD I Instruction 8500.01, March 2014

[3] *Risk Management Framework (RMF) for DoD Information Technology (IT),* DoD Instruction 8510.01, 12 March 2014

[4] *Department of the Navy Cybersecurity Policy*, SECNAVINST 5239.3C, May 2016

[5] *Information Assurance*, OPNAVINST 5239.1D, unpublished

[6] *Cyberspace Workforce Management*, DoD Directive 8140.01, August 2015

[7] (2016) The Office of the Secretary of Defense website. Risk Management Framework Knowledge Service webpage [Online]. Available: https://rmfks.osd.mil/login.htm

[8] *Guide for Mapping Types of Information and Information Systems to Security Categories,* National Institute for Standards and Technology (NIST) Special Publication (SP) 800-60, Vol. 1 & 2, Rev 1, August 2008

[9] *Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach,* National Institute for Standards and Technology (NIST) Special Publication (SP) 800-37, Rev 1, June 2014