Cybersecurity Controls: Then and Now

Marco Mayor
U.S. Army PEO STRI
Orlando, FL
marco.mayor.civ@mail.mil

ABSTRACT

The phase out of the Department of Defense (DOD) Information Assurance Certification and Accreditation Process (DIACAP) is leading to a new process called Risk Management Framework (RMF). This new process was mandated by DOD Instruction 8500.01, which also mandated the adoption of the term "cybersecurity" to be used throughout DOD instead of the term "information assurance (IA)." RMF will follow a set of security controls inherited from the National Institute of Standards and Technology (NIST). These controls are specifically located in the Special Publication (SP) 800-53. The NIST SP 800-53 controls will replace the existing DOD Instruction (DODI) 8500.2 controls and have been updated to reflect the evolving technologies while addressing new cybersecurity threats. Given the transition, there are a number of implications for the training and simulation community for ensuring training systems comply with these new controls and maintain their information security posture. Guidance for the transition has been developing gradually and each of the DOD agencies are handling it individually at the implementation level. The Program Executive Office for Simulation, Training, and Instrumentation (PEO STRI) is following DOD and specifically Army guidance to ensure the NIST control implementation gets executed in the most efficient manner possible.

This paper will first provide some background on the legacy DOD 8500.2 controls and an overview of the transition to the NIST SP 800-53 controls. It will then discuss the formal requirements, new terminology, implementation and guidance driving this transition. This paper will analyze the framework of the NIST SP 800-53 RMF controls and how they compare to DIACAP controls. It will discuss the security control overlays, and the assessment procedures. To conclude, this paper will describe the transition impacts for PEO STRI stakeholders, which include DOD contractors, system users, and Project Managers (PM). This paper will layout the fundamental idea and challenges PEO STRI faced on a particular use case, while handling the transition from the DODI 8500.2 DIACAP controls to the NIST SP 800-53 RMF controls

ABOUT THE AUTHOR

Mr. Marco Mayor works as an Information Security Analyst for the Chief Information Office (CIO) in the U.S. Army Program Executive Office for Simulation, Training, and Instrumentation (PEO STRI). Mr. Mayor worked several years as a Cybersecurity Analyst and then transitioned to government civil service as a certifier. With more than 8 years of cybersecurity experience, Mr. Mayor is Security+, Certified Ethical Hacker (CE|H), and Information Systems Security Professional (CISSP®) certified. He holds a Bachelor of Science in Information Technology (IT) and a Master of Science in Modeling and Simulation both from the University of Central Florida.

Cybersecurity Controls: Then and Now

Marco Mayor
U.S. Army PEO STRI
Orlando, FL
marco.mayor.civ@mail.mil

INTRODUCTION

Since 2007, the DOD Information Assurance Certification and Accreditation Process (DIACAP) has been the certification and accreditation vehicle ensuring system owners that risk management is applied on their systems. On March 14, 2014, the DOD released guidance to supersede DIACAP with a new more streamlined and effective process, called Risk Management Framework (RMF). Driven by DOD Instruction 8500.01, this new process still applies to all DOD IT (DOD, 2014). Among the many changes associated with the transition, one was the adoption of the term "cybersecurity" which replaces "Information Assurance (IA)". The other change addressed in this paper, is the migration from DIACAP security controls to National Institute of Standards and Technology (NIST) security Controls. RMF will now follow the NIST controls located in the Special Publication (SP) 800-53. These controls will replace the existing DOD Instruction (DODI) 8500.2 controls and have more granularity than the former controls. Also, these new controls are more updated and align better with today's technologies. This paper will focus on the control transition requirements and implications as known at the date of publication. The DIACAP to NIST controls transition will take place incrementally, and the different agencies are handling individually in terms of implementation. The Program Executive Office for Simulation, Training, and Instrumentation (PEO STRI) is following DOD and specifically Army guidance to ensure the NIST control implementation gets executed in the most efficient manner possible.

This paper will first provide some background on the legacy DOD 8500.2 controls and an overview of the transition to the NIST SP 800-53 controls. It will then discuss the formal requirements, new terminology, implementation and guidance driving this transition. This paper will analyze the framework of the NIST SP 800-53 RMF controls and how they compare to DIACAP controls. It will discuss the assessment procedures and the security control overlays. To conclude, this paper will describe the transition impacts for PEO STRI stakeholders, which include DOD contractors, system users, and Program Managers (PM). This paper will layout the fundamental idea and challenges PEO STRI faced on a particular use case, while handling the transition from the DODI 8500.2 DIACAP controls to the NIST SP 800-53 RMF controls

BACKGROUND

DOD's IA control migration background began in an effort to consolidate and standardize certification and accreditation across the federal government (DISA, 2012). Prior to RMF, the DOD used DIACAP, and the security controls implemented, differed from other federal agencies. DIACAP implemented a total of 157 controls, and these were broken down into eight subject areas. The DOD controls outlined in DODI 8500.2, established fundamental cybersecurity requirements for DOD information systems in the form of two sets of graded baseline IA Controls. PMs were responsible for employing the sets of baseline controls appropriate to their programs. The baseline sets of IA controls were pre-defined based on the determination of the Mission Assurance Category (MAC) and Confidentiality Levels (CLs) as specified in the formal requirements documentation or by the User Representative on behalf of the information owner. IA Controls addressing availability and integrity requirements were entered to the system's MAC based on the importance of the information to the mission, particularly the warfighters' combat mission. Cybersecurity controls addressed confidentiality requirements based on the sensitivity or classification of the information. There were three MAC levels and three CLs with each level representing increasingly stringent cybersecurity requirements. Table 1, presents the first major component (MAC Level) that formed the first set baseline of the DIACAP controls. The levels varied based upon the high, medium or basic levels of integrity and availability (Defense Acquisition Guidebook, 2014, September 19, "Information Assurance", para. 7.5.7.1).

.

Table 1 - MAC Levels and Definitions

	Definition	Integrity	Availability
MAC I	These systems handle information that is determined to be **vital to the operational readiness of mission effectiveness of deployed and contingency forces** in both content and timelines.	High	High
MAC II	These systems **handle information that is important to the support of deployed and contingency forces.**	High	Medium
MAC III	These systems handle information that is necessary for the conduct of day-to-day business, but **does not materially affect support to deployed or contingency forces in the short-term.**	Basic	Basic

Table 2, displays the other major component that formed the baseline set for these DIACAP controls, the confidentiality level. DOD has defined three levels of confidentiality that line up with the sensitivity of the information associated with the information system.

Table 2 – Confidentiality Levels

	Definition
Classified	Systems processing classified information.
Sensitive	Systems processing sensitive information as defined in DOD Directive 8500.01E, to include any unclassified information not cleared for public release.
Public	Systems processing publicly releasable information as defined in DOD Directive 8500.01E (i.e., information that has undergone a security review and been cleared for public release)

The combination of these two components defined the total amount of DIACAP controls that an information system was required to comply with. Table 3, illustrates the different MAC/CL combinations mapped to the required amount of controls. Notice how the most stringent levels (MAC I and MAC II, Classified) require the most controls and the less stringent (MAC III, Public) requires least.

Table 3 – Total Amount of Controls Required Based on MAC and CLs

MAC Level	Confidentiality Level	Total Amount of DIACAP Controls
MAC I	Classified	110
MAC I	Sensitive	106
MAC I	Public	81
MAC II	Classified	110
MAC II	Sensitive	106
MAC II	Public	81
MAC III	Classified	105
MAC III	Sensitive	100
MAC III	Public	75

The DIACAP to NIST control transition moved the entire federal government under one set of controls resulting in improved information security, a stronger risk management process and reciprocity among federal agencies. Moving to a common process and set of controls will also reduce costs related to the activities associated with system authorization. For example a system purchased by the DOD for their Military Treatment Facilities, as well as by the Veterans Administration (VA) for use in their hospitals, would have required two separate processes: a Certification and Accreditation (C&A) utilizing DIACAP for the DOD and a system authorization based on NIST for the VA hospitals. Because of the common Assessment and Authorization (A&A) processes, the cost for purchasing and deploying that system has now considerably decreased. The transition goal is to accomplish reciprocity by ensuring that all Federal information systems are authorized under the same RMF process, and meet the same NIST 800-53 baseline set of controls (Onuskanich, 2011).

RMF REQUIREMENTS AND GUIDANCE

In 2013, DOD guidance for the RMF transition was released. Unlike DIACAP which was made up of five phases, RMF is composed of six steps, and each step is mapped to different Federal Information Processing Standards (FIPS) and NIST Special Publications (SP). Table 4 aligns these guidelines with their corresponding step within the RMF (NIST, 2014).

Table 4 – FIPS and SP Guidelines Mapped to RMF Steps

RMF Step	Number	Name
Step 1 – Categorize Information Systems	FIPS 199	Standards for Security Categorization of Federal Information and Information Systems
	SP 800-60	Guide for Mapping Types of Information and Information Systems to Security Categories (Volumes I and II)
Step 2- Select Security Controls	FIPS 200	Minimum Security Requirements for Federal Information and Information Systems
	SP 800-53	Security and Privacy Controls for Federal Information Systems and Organizations
Step 3 – Implement Security Controls	SP 800-70	National Checklist Program for IT Products – Guidelines for Checklist Users and Developers
Step 4 – Assess Security Controls	SP 800-53A	Guide for Assessing the Security Controls in Federal Information Systems and Organizations
Step 5 – Authorize Information Systems	SP 800-37	Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
Step 6 – Monitor Security Controls	SP 800-37	Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
	SP 800-53A	Guide for Assessing the Security Controls in Federal Information Systems and Organizations
	SP 800-137	Information Security Continuous Monitoring for Federal Information Systems and Organizations

In steps 2, and 4, SP 800-53 and SP 800-53A play an important role in their implementation and assessment. Both publications specifically address the NIST controls implementation. SP 800-53 establishes guidelines for assigning security controls with the purposes of achieving secure operations of information systems. It addresses security from both a functionality perspective (the strength of security functions and mechanisms provided) and an assurance perspective (the measures of confidence in the implemented security capability). SP 800-53A provides procedures for conducting the assessment for applicable security controls and privacy controls for a given system. In collaboration with NIST, the Committee on National Security Systems (CNSS) released the instruction (CNSSI 1253) to ensure that NIST SP 800-53 contained the necessary security controls which met the security requirements across the U.S. Federal Government. This instruction also provided information system categorization, as a guideline to tailor and potentially expand the amount of controls depending on the category of the system. Table 5 provides a comprehensive list of instructions related to the overall execution of RMF. Their goal is to ensure agencies, contractors, and other stakeholders implement RMF effectively, therefore minimizing the cyber threat to systems (NIST, 2013).

Table 5 – RMF Instructions

Number	Name	Summary
DODI 8500.01	Cybersecurity	Provides the foundation for establishing a DOD cybersecurity program for defense of networks, systems and IT to include definitions of terms, security controls guidance, and enterprise governance.
DODI 8510.01	Risk Management Framework	Establishes a policy governing cybersecurity, addresses reciprocity, assigns responsibilities, and details execution of the RMF process.
CNSSI 1253	Security Categorization and Control Selection for National Security Systems	Provides a foundation for selecting and applying security controls from NIST SP 800-53 for implementation on a National Security System.
CNSSI 1253A	Implementation and Assessment Procedures	Establishes a guideline for assessing compliance with applicable security controls on a National Security System.
CNSS 4009	National Information Assurance Glossary	Documents a detailed glossary of Information Assurance related terms in an effort to minimize differences in terminology to ensure consistency and standardization.

FUNDAMENTALS OF RMF CONTROLS

To develop these controls, NIST consults other federal agencies and the private sector to ensure an integrated security framework for the federal government is met. These controls are policy and technology-neutral, this means that the controls focus only on the safeguards and countermeasures necessary to protect data while is in-transit or at rest. On the other hand, this does not mean the controls are policy and technology-unaware. Staying updated with policy and technology ensures that the security controls stay relevant and meaningful.

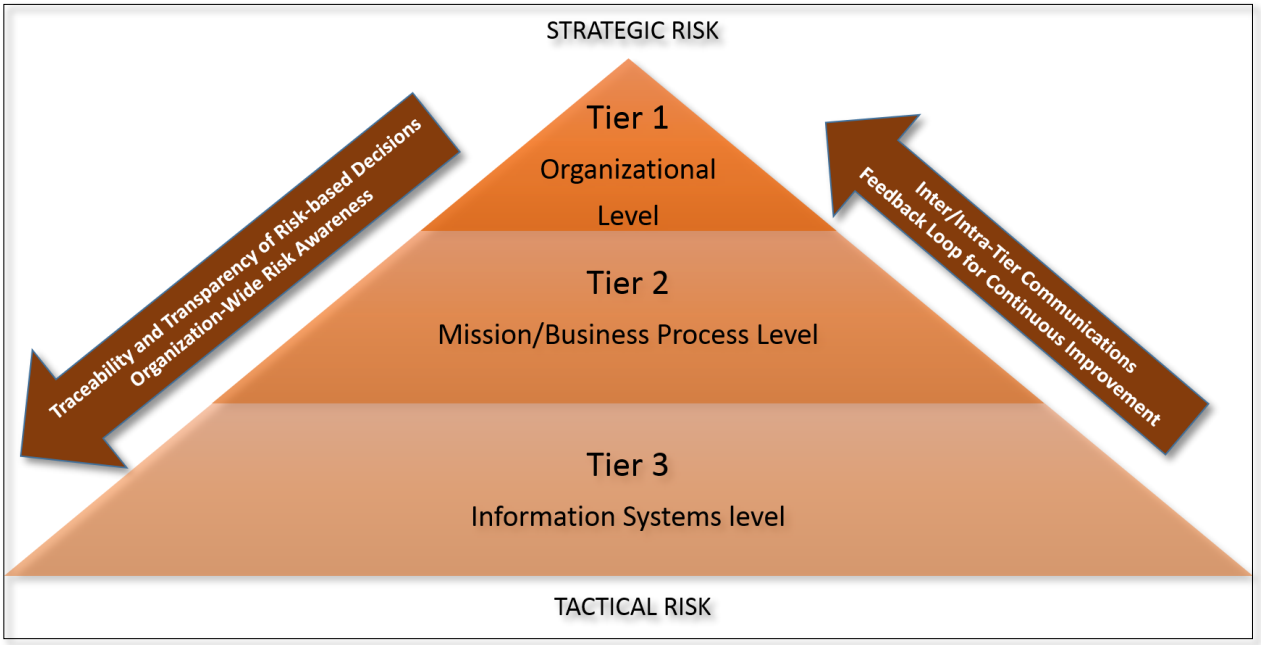

Figure 1 – Three-Tiered Risk Management Approach

Selection

The selection of the NIST controls for an information system is a three-tiered risk management process. Figure 1 illustrates this approach. Tier 1 starts with stakeholders prioritizing organizational missions and business functions.

Tier 2 defines the mission and business processes, the security category, the security requirements, and the enterprise architecture required to support the organizational mission/business functions. Tier 3 defines the implementation of these at the information system level. The feedback loop is encouraged in order to make continuous improvements.

The first step in the control selection, is determining the security categorization of the system. In other words, determining the potential adverse impact for organizational systems. The FIPS 199 guideline requires organizations to categorize systems in a low, medium, and high-impact fashion in terms of their confidentiality, integrity, and availability. For example: if a system is considered low confidentiality, low integrity, and low availability, then is a low–impact system. Once the impact level is determined, one of the three security control baselines from appendix D of the SP 800-53 publication, is selected. These security control baselines are the starting point from which RMF practitioners may tailor (add or remove controls) as needed. Today, NIST is working with DOD agencies to refine a tailoring process referred to as overlays that will serve as a baselines or starting points for specific types of systems. For example, several PEO STRI systems are simulation trainers which reside in stand-alone and closed-restricted networks.

Structure

Compared to DIACAP, the RMF controls are much more granular, the SP 800-53 revision 4 contains more than 850 controls. These have been organized into 18 families and three classes: Management Operational, and Technical controls. All controls within the respective family are related to the general category of the family. These families are identified by a two-character identifier, for example: AC (Access Control). Table 6, displays all the security control identifiers, their corresponding family names, their classes, and an examples on how these classes of controls are typically implemented.

Table 6 – Control Identifiers, Families, Classes and Examples

ID	Family	Class	Examples
AC	Access Control	Technical	Access controls, Authentication Mechanisms, and Encryption, Sign-in Sheets, Rosters, Privilege Access Agreements, Acceptable Use Policies, Appointment Orders, Security Technical Implementation Guides (STIGs), etc.
AU	Audit and Accountability	Technical	
IA	Identification and Authentication	Technical	
SC	System and Communications Protection	Technical	
AT	Awareness and Training	Operational	Awareness training, Configuration Management Plan, Incident response Plan, Contingency Plan, Continuity of Operations Plan, Physical Security Plan, Approved Hardware and Software, Alternate Site/Storage, Emergency Power, Fire Protection, Nondisclosure Agreements, etc.
CM	Configuration Management	Operational	
CP	Contingency Planning	Operational	
IR	Incident Response	Operational	
MA	Maintenance	Operational	
MP	Media Protection	Operational	
PE	Physical and Environment Protection	Operational	
PS	Personnel and Security	Operational	
SI	System and Information Integrity	Operational	
CA	Security Assessment and Authorization	Management	Policies, Procedures, Rules of Behavior, Security Concept of Operations, Penetration Testing, Cybersecurity Vulnerability Management, etc.
PL	Planning	Management	
PM	Program Management	Management	
RA	Risk Assessment	Management	
SA	System and Services Acquisition	Management	

The control content is written at a high level, leaving the most appropriate implementation in the hands of the organization. The goal of these controls is to promote a cost-effective, risk-based information security for organizations in any sector, any technology, and in any operating environment. Figure 2 describes in detail the anatomy of the AU-3 control. These can be found in appendix F of the SP 800-53.

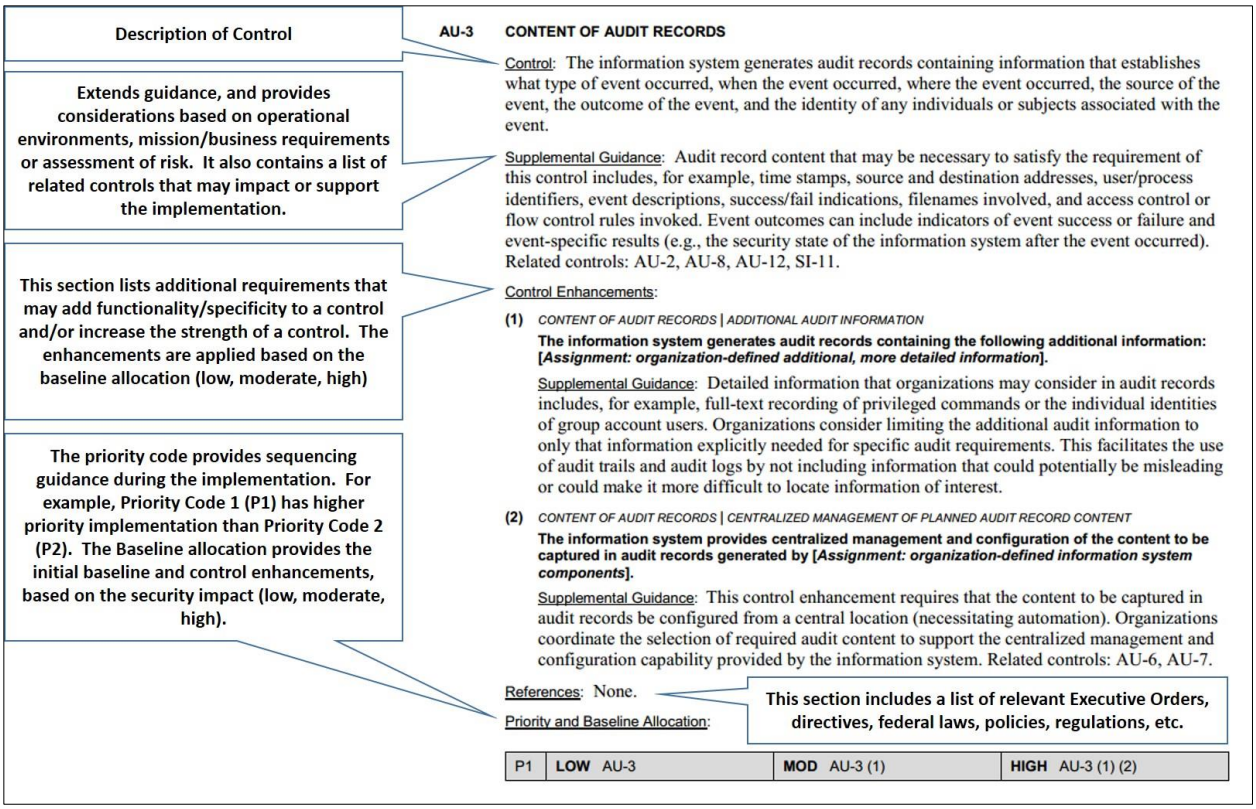

Figure 2 – Anatomy of the NIST Controls

In figure 2, under the control enhancements section, the two requirements (1) and (2), contain text in brackets stating assignment statements pointing to organization-defined requirements. At the time this research was done, the PEO STRI cybersecurity office used Army specific guidance, STIGs and/or Security Requirements Guides provided by DISA to define organization-specific parameters. As the RMF process evolves within the DOD, these requirements will be better delineated, but always keeping in mind that the agency may explicitly make these requirements more stringent. At the very bottom of figure 2 is the Priority and Baseline allocation section. In this example, if the system has a high security impact, the first and second control enhancements are selected, making the control designation AU-3(1)(2). This means that the system owner must comply with both requirements (NIST, 2013).

CONTROL CUSTOMIZATION AND OVERLAYS

One of the many challenges DOD is facing in the DIACAP-to-RMF transition, is ensuring that the adequate NIST controls are selected for the diverse pool of information systems (e.g. weapons systems, simulation trainers, enclaves, stand-alone, etc.) As discussed earlier, DIACAP based their security requirements on the determination of the system's MAC and CL. In the case of the Army, there were DIACAP Implementation Plan templates for connected and stand-alone environments with a different number of controls and different levels of stringency. NIST on the other hand, introduced a tailoring process utilized by RMF that achieves cost-effective, risk-based baselines called overlays. Overlays are essentially a set of security controls that can be tailored to meet specific sectors, communities of interest, information technologies or environment of operations, etc. Organizations then have the flexibility to apply a baseline, and tailor this baseline with security controls that further align with their mission, business requirements and environments of operation.

Even after an overlay is defined, the organization may do a gap analysis, and decide to implement additional controls, substitute some with supplemental controls, and even select compensating/alternative controls. This tailoring process, while it looks sequential, may also have an iterative aspect. For example, organizations may establish some initial security control parameters, then face difficulties, which trigger the need for additional controls. (NIST 2014). PEO STRI is working closely with other Army organizations to develop a set of controls that apply to stand-alone systems.

DOD 8500.2 VS NIST SP 800-53 COMPARISON

Table 7 displays side-by-side characteristics for both types of controls. The comparison exhibits how flexible the NIST controls may be compared to the DOD 8500.2 controls, but it also shows how more granular they are. The increment of controls is a key concern among system owners, because even though the technical security aspect is the same, the validation process will take longer to implement. This normally translates to an adverse impact to cost and schedule.

Table 7 – DOD 8500.2 Controls vs. NIST 800-53 Comparison

DODI 8500.2 (Then)	NIST SP 800-53 (Now)
MAC and **CL** Levels	**Impact Levels**, (Confidentiality-Moderate, Integrity-Low, Availability-Low, etc.)
Fixed amount of controls based on **MAC** and **CL** Levels	**Variable** amount of controls based on **initial baselines, impact levels, overlays, control enhancements, additional tailoring requirements.**
157 Controls Total (not including sub-controls)	**958** Controls Total (not including Control Correlation Identifiers).
8 Subject Areas	**3** Classes divided in **18** families.

ASSESSMENT PROCEDURES AND CONTINUOUS MONITORING

In order to provide guidance on the assessment methods and procedures for determining security control effectiveness, NIST released the SP 800-53A rev4 publication. This publication contains procedures that are consistent with the security and privacy controls in the NIST 800-53 rev4. Unlike the DIACAP assessment procedures, these can be tailored in order to provide organizations with the flexibility to conduct security and privacy control assessments supporting an organization's overall risk management process. The main goals for these NIST assessment procedures are to provide organizations with evidence on the effectiveness of the implementation, provide an idea on how the organization stands in terms of the quality of their risk management process, and ultimately provide the strengths and weaknesses of information systems (NIST 2013). PEO STRI will be tailoring the assessment procedures by following Army specific guidance complemented with STIGs developed by the Defense Information Systems Agency (DISA).

Unlike DIACAP where the assessment procedures were checklist-based and more static in nature, RMF is modernizing the entire assessment process by implementing tools that promote automation and continuous monitoring. NIST developed the Security Content Automation Protocol (SCAP), with the intent to standardize the format in which configurations and security flaws are communicated. This standardization opened the door to automated system configuration assessments, patch compliancy verification, vulnerability assessments, and report aggregation, all between SCAP-enabled security tools (NIST 2013). DISA in conjunction with the NIST SCAP developed the Control Correlation Identifiers (CCIs), which decomposed a control or industry best practice into a single, actionable statement. CCIs are not specific to a product or a Common Platform Enumeration.

In order to provide training systems with near-real time cybersecurity situational awareness, emerging technologies such as Assured Compliance Assessment Solution (ACAS), Host Based Security System (HBSS), and the Continuous Monitoring Risk Scoring (CMRS), system were implemented. ACAS is a scalable suite of COTS applications, which has the ability to provide automated network vulnerability scanning, configuration assessment, application vulnerability scanning, device configuration assessment, STIG compliance, and network discovery (ACAS, 2014). HBSS is also a COTS suite of software applications that monitors, detects, and counters against acknowledged cyber-threats to DOD systems and networks (HBSS, 2014). CMRS is web-based system that visualizes and quantifies the cybersecurity risk of the DOD based on published asset inventory (provided by HBSS) and the compliance data (provided by ACAS), via usage of a dashboard. CMRS allows users to gather decision-making information, implement prioritized mitigation decisions, and ensure effectiveness of security controls in order to support their cybersecurity risk management duties (CMRS, 2014).

Two additional RMF web-based resources, that play an important role in the DIACAP to NIST control transition, are the Enterprise Mission Assurance Support Service (eMASS) and the RMF Knowledge Site (KS). The eMASS includes all the reports required by the RMF process, and it will support the transition from the legacy DIACAP to the NIST 800-53 controls. The eMASS' main vision is to promote process automation, reduce cost, and provide system owners with near real-time enterprise-level visibility into cybersecurity activities, all in a secure fashion.

eMASS keeps track of all the compliant, not compliant, non-applicable, and inherited NIST controls. Users now have the capability to upload vulnerability scans to eMASS, and help generate a Plan of Actions and Milestones in an automated fashion.

The KS on the other hand, provides RMF users access to RMF policy and guidance on implementation methods, standards, and practices required to protect DOD systems. It provides access to the NIST security controls baselines, overlays, individual security controls and security control implementation guidance and assessment procedures. The KS website contains a library of tools, diagrams, process maps, etc. assisting users in the execution of the RMF process. Access to the eMASS and KS websites, is only available to users with a Common Access Card or with external DOD sponsorship, for example, DOD contractors without a CAC (Department of Defense, 2014).

TRANSITION IMPLICATIONS

Even though the DIACAP and NIST controls addressed similar security goals, there are a number of challenges the DOD community is facing as we make the transition. By DOD community I am referring to the stakeholders such as Government Project Managers, DOD cybersecurity workforce, and RMF validation testing teams. One of the main challenges associated with the transition for the DOD community is adequate training. The DOD has developed a number of RMF training packages, which are available to the cybersecurity workforce. This training includes the DIACAP to NIST control transition, but the training does not delve into this topic in detail as it will relate to DOD IT and PIT Systems. As RMF matures, more training opportunities will be available at the agency level for both government and industry personnel. Currently, PEO STRI is incorporating RMF language in all Requests For Proposals (RFPs) to ensure that PEO STRI meets RMF requirements for future systems going through the acquisition process. It is important that the DOD community understands the NIST control requirements, the security impact of their systems, and the overlays that should be implemented. Defining these will help outline the RMF requirements in RFPs for upcoming acquisitions, resulting in adequate planning for cost and schedule.

During the transition, PEO STRI recognizes the fact that the DOD community is concerned by the significant increment of controls required under NIST 800-53 guidance. At a glance this represents more requirements, resulting in higher project costs. In other words, the granularity of the NIST controls gives the perception that hundreds of new controls will need to be implemented under RMF. Table 8, provides one of the many cases where one DIACAP control can be mapped to multiple NIST 800-53 controls. So after researching the validation procedures in NIST 800-53A for the controls listed in the second column of table 8, and comparing them with the procedures from the DOD 8500.2 DIACAP guidance for the same control, we concluded that they both meet the same security goals (NIST, 2013).

Another transition implication is the adoption of eMASS as the default A&A tracking tool. The RMF transition requires the DOD cybersecurity community to implement eMASS as a central repository for all cybersecurity information. In the past, PEO STRI was required to manage all of its systems in the Army's C&A tracking database. Today, PEO STRI is engaged in eMASS training, so that they can gain access and start tracking their corresponding RMF activities. The time required to do a self-assessment on a system with low confidentiality, low integrity, and low availability, may take up to 40 hours. When this paper was written, self-assessment time metrics for higher confidentiality, integrity and availability levels, were not available.

Table 8 – DOD 8500.2 Controls to NIST 800-53 Mapping

Legacy DOD 8500.2 Control and Definition	NIST SP 800-53 Controls		NIST 800.53 Definition
ECLP-1 Least Privilege Access procedures enforce the principles of separation of duties and "least privilege." Access to privileged accounts is limited to privileged users. Use of privileged accounts is limited to privileged functions; that is, privileged users use non-privileged accounts for all non-privileged functions. This control is in addition to an appropriate security clearance and need-to-know authorization.	**AC-6**	**LEAST PRIVILEGE**	
	AC-6(1)	**LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS**	The organization explicitly authorizes access to [Assignment: organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information].
	AC-6(2)	**LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS**	The organization requires that users of information system accounts, or roles, with access to [Assignment: organization-defined security functions or security-relevant information], use non-privileged accounts or roles, when accessing non-security functions.
	AC-6(5)	**LEAST PRIVILEGE | PRIVILEGED ACCOUNTS**	The organization restricts privileged accounts on the information system to [Assignment: organization-defined personnel or roles].
	AC-6(7)	**LEAST PRIVILEGE | REVIEW OF USER PRIVILEGES**	The organization: (a) Reviews [Assignment: organization-defined frequency] the privileges assigned to [Assignment: organization-defined roles or classes of users] to validate the need for such privileges; and (b) Reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs.
	AC-6(8)	**LEAST PRIVILEGE | PRIVILEGE LEVELS FOR CODE EXECUTION**	The information system prevents [Assignment: organization-defined software] from executing at higher privilege levels than users executing the software.
	AC-6(9)	**LEAST PRIVILEGE | AUDITING USE OF PRIVILEGED FUNCTIONS**	The information system audits the execution of privileged functions.
	AC-6(10)	**LEAST PRIVILEGE | PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS**	The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

USE CASE AND THE FUTURE OF THE TRANSITION

At the time this research was done, NIST control guidance for stand-alone systems had not been officially released. PEO STRI took the lead to define a set of NIST controls that will be used to assess and authorize stand-alone trainers. For the first system to undergo the RMF process in our organization, the PEO STRI Cybersecurity Office first identified all controls that met the low confidentiality, low integrity, low availability criteria. Then, did a comprehensive study of all the possible controls and removed those that dealt with remote access, network boundary, and automated reporting. After that, we did a comparison between the 32 DIACAP controls listed in the Army stand-alone C&A Best Business Practice, and the NIST controls crosswalk table located in the RMF KS. We noticed that some of the 32 controls did not meet the Low-Low-Low criteria, so we researched the SP 800-53 guidance, and found out that these controls were part of the moderate criteria. These extra controls were also added

to our pilot stand-alone template. The next step is to release the template to the NETCOM G6 organization, so that they can take advantage of our lessons learned, avoid duplicate efforts and gain the benefits of reciprocity.

Members of the PEO STRI Cybersecurity community will continue attending NIST control specific working group discussions, document lessons learned from the initial transition, and establish processes that will lay the path for an effective transition to RMF control implementation. After the initial system is accredited, there will be an opportunity at the PEO STRI level to refine processes. Additionally, future work will capture the evolution in the Risk Management Framework related tools.

ACRONYMS

Acronym	Name
A&A	Assessment and Authorization
ACAS	Assured Compliance Assessment Solution
AU	Audit and Accountability
BAM	Basic Accreditation Manual
C&A	Certification and Accreditation
CCI	Control Correlation Identifiers
CIO	Chief Information Office
CL	Confidentiality Level
CMRS	Continuous Monitoring Risk Scoring
CNSS	Committee On National Security Systems
CNSSI	Committee On National Security Systems Instruction
COTS	Commercial Off The Shelf
CSO	Cybersecurity Office
DIACAP	DOD Information Assurance Certification and Accreditation Process
DISA	Defense Information Systems Agency
DOD	Department of Defense
DODI	Department of Defense Instruction
eMASS	Enterprise Mission Assurance Support Service
FIPS	Federal Information Processing Standards
HBSS	Host Based Security System
IT	Information Technology
KS	Knowledge Service
MAC	Mission Assurance Category
NIST	National Institute of Standards and Technology
PEO STRI	Program Executive Office for Simulation, Training, and Instrumentation
PM	Program Manager / Program Management
RFP	Request For Proposal
RMF	Risk Management Framework
SP	Special Publication
STIG	Security Technical Implementation Guides

REFERENCES

Defense Information Systems Agency. (2014). *ACAS.* Retrieved on September 25, 2014, from http://www.disa.mil/Services/Information-Assurance/ACAS

Defense Information Systems Agency. (2014). *CMRS.* Retrieved on September 28, 2014, from https://east1.deps.mil/disa/cop/mae/netops/CMRS/SitePages/Home.aspx

Defense Information Systems Agency. (2014). *HBSS.* Retrieved on September 26, 2014, from http://www.disa.mil/Services/Information-Assurance/HBSS

Department of Defense. (2014). *Cybersecurity Instruction 8500.01*. Retrieved September 17, 2014 from http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf

Department of Defense. (2014). *Risk Management Framework (RMF) for DOD Information Technology (IT) Instruction 8510.01*. Retrieved October 15, 2014 from http://www.dtic.mil/whs/directives/corres/pdf/851001_2014.pdf

National Institute of Standards and Technology. (2014). *Risk Management Framework (RMF) 6 step Chart*. Retrieved October 23, 2014 from http://csrc.nist.gov/groups/SMA/fisma/Risk-Management-Framework/

National Institute of Standards and Technology. (2013). *Security and Privacy Controls for Federal Information Systems and Organizations Special Instruction 800-53r4*. Retrieved October 22, 2014, from http://csrc.nist.gov/publications/drafts/800-53a/sp800_53a_r4_draft.pdf

Onuskanish, R. (2011, December 12). Out With The DIACAP, In With the DIARMF. Retrieved September 21, 2014, from https://www.lunarline.com/sites/default/files/out with diacap in with diarmf - lunarline white paper_dec 11.pdf