Strategy Research Project

Effectiveness of the Department of Defense Information Assurance Accreditation Process

by

Mr. Joseph Luis Valladares
Department of the Army Civilian

United States Army War College
Class of 2013

DISTRIBUTION STATEMENT: A
Approved for Public Release
Distribution is Unlimited

This manuscript is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*
xx-03-2013

2. REPORT TYPE
STRATEGY RESEARCH PROJECT

3. DATES COVERED *(From - To)*

4. TITLE AND SUBTITLE
Effectiveness of the Department of Defense Information Assurance Accreditation Process

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Mr. Joseph Luis Valladares
Department of the Army Civilian

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Mr. Brian A. Gouker
Department of Military Strategy, Planning and Operations

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

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

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Approved for Public Release. Distribution is Unlimited.

13. SUPPLEMENTARY NOTES
Word Count: 6334

14. ABSTRACT

For many years, the Department of Defense (DoD) has used very formalized processes for authorizing the operation of its information systems. This authorization process, known as accreditation within the DoD, has always been based on certification testing of those systems and an assessment of the risks associated with operating those systems on the DoD's Global Information Grid (GIG). Despite using these various costly and process-intensive methods for certification and accreditation (C&A), it is questionable whether or not these processes have actually improved the security of DoD systems and networks commensurate with the cost and effort involved. Further, given current advances in systems security technologies, recent changes in DoD's strategy for operating in cyberspace, and even the very structure of the DoD's enterprise networks in the near future, should (or even can) the DoD continue to test and authorize information systems using these same methodologies? This paper addresses this question and proposes other ways the DoD can more effectively assess its systems and networks to better ensure their security over time.

15. SUBJECT TERMS
Certification & Accreditation (C&A), Assessment & Authorization (A&A), INFOSEC, Risk Assessment

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT UU	**b. ABSTRACT** UU	**c. THIS PAGE** UU	UU	34	**19b. TELEPHONE NUMBER** *(Include area code)*

USAWC STRATEGY RESEARCH PROJECT

Effectiveness of the Department of Defense Information Assurance Accreditation Process

by

Mr. Joseph Luis Valladares
Department of the Army Civilian

Mr. Brian A. Gouker
Department of Military Strategy, Planning and Operations
Project Adviser

This manuscript is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Abstract

Title:	Effectiveness of the Department of Defense Information Assurance Accreditation Process
Report Date:	March 2013
Page Count:	34
Word Count:	6334
Key Terms:	Certification & Accreditation (C&A), Assessment & Authorization (A&A), INFOSEC, Risk Assessment
Classification:	Unclassified

For many years, the Department of Defense (DoD) has used very formalized processes for authorizing the operation of its information systems. This authorization process, known as accreditation within the DoD, has always been based on certification testing of those systems and an assessment of the risks associated with operating those systems on the DoD's Global Information Grid (GIG). Despite using these various costly and process-intensive methods for certification and accreditation (C&A), it is questionable whether or not these processes have actually improved the security of DoD systems and networks commensurate with the cost and effort involved. Further, given current advances in systems security technologies, recent changes in DoD's strategy for operating in cyberspace, and even the very structure of the DoD's enterprise networks in the near future, should (or even can) the DoD continue to test and authorize information systems using these same methodologies? This paper addresses this question and proposes other ways the DoD can more effectively assess its systems and networks to better ensure their security over time.

Effectiveness of the Department of Defense Information Assurance Accreditation Process

For many years, the Department of Defense (DoD) has used very formalized processes for authorizing the operation of its information systems. This authorization process, known as accreditation within the DoD, has always been based on certification testing of those systems and an assessment of the risks associated with operating those systems on the DoD's Global Information Grid (GIG). Despite using these various costly and process-intensive methods for certification and accreditation (C&A), it is questionable whether or not these processes have actually improved the security of DoD systems and networks commensurate with the cost and effort involved. Further, given current advances in systems security technologies, recent changes in DoD's strategy for operating in cyberspace, and even the very structure of the DoD's enterprise networks in the near future, should (or even can) the DoD continue to test and authorize information systems using these same methodologies. This paper addresses this question and proposes other ways the DoD can more effectively assess its systems and networks to better ensure their security over time.

Evolution of DoD's Accreditation Process

In 1972, the DoD published DoD Directive 5200.28, Security Requirements for Automated Information Systems, which it later updated in 1988. Along with DoD Directive 5200.28-STD, also known as the "Orange Book," which was released in 1983, these directives formed the basis for the testing and accreditation of systems within DoD. These directives left room for interpretation with regard to process, which resulted in each of the military services specifying in its own regulations similar, but separate, accreditation processes to be used within that service. From the beginning, the accreditation processes used within the DoD focused on discrete, individual systems as the target of testing and accreditation.

In 1997, the DoD published DoD Instruction 5200.40, DoD Information Technology Security Certification and Accreditation Process (DITSCAP). The objective of this new regulation was “to establish a DoD standard infrastructure-centric approach that protects and secures the entities comprising the Defense Information Infrastructure (DII). The set of activities presented in the DITSCAP standardized the C&A process for single information technology (IT) entities that leads to more secure system operations and a more secure DII. The process considers the system mission, environment, and architecture while assessing the impact of operation of that system on the DII.”[1] This effort to synchronize the certification and accreditation process across the entire DoD, and to begin assessing risks in terms of the enterprise was a step in the right direction, but even the DITSCAP still focused on discrete, individual systems as the target of testing and accreditation.

In 2006, the DoD replaced the DITSCAP with the DoD Information Assurance Certification and Accreditation Process (DIACAP), as published interim guidance, and later (2007) finalized in DoD Instruction 8510.01. Ostensibly, this change was made to “address the paradigm shift in IA security from an individual information system-level approach to a DoD-wide enterprise approach of securing information systems in a net-centric environment and for supporting the implementation of IA security during a system’s life cycle”[2] This sounds a lot like what the DITSCAP was intended to do, but the DIACAP still tested and accredited individual systems and discrete enclaves (e.g., local area networks) that could be tested and accredited as one “system.”

Currently, the DoD is transitioning, along with the rest of the federal government, to the use of the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) as specified in NIST Special Publication (SP) 800-37, and the NIST-developed set of controls published in NIST SP 800-53. In fact, the current DIACAP aligns closely with the intent of and process called out in the NIST RMF. The most significant changes the DoD will have to adjust to will be the new RMF-related language (e.g., “Authorizing Official” under the RMF versus “Designated Approving Authority” under the DIACAP) and, more significantly, the new set of controls in NIST SP 800-53.

Despite what would seem a limited change to how the DoD historically conducted C&A, there are significant benefits offered by the RMF. One of these is to enable reciprocity between Federal agencies, including the DoD. It forces all Federal agencies to one common authorization process, common security controls, common testing activities and outcome assessment, as well as a common lexicon. Using one standardized process will also reduce costs related to the activities associated with system authorization. “A great example would be a medical system that has been purchased by the DoD for their Military Treatment Facilities (MTF), as well as by the Veterans Administration (VA) for use in their hospitals. Under the current situation, this new system would be required to undergo two separate processes: a C&A utilizing DIACAP for the DoD and a system authorization based on NIST guidelines for the VA hospitals. The cost for purchasing and deploying that system has now significantly increased as a consequence of the requirement for distinctly separate processes."[3]

Clearly, the DoD has placed significant emphasis on C&A processes over the last three decades, but what does C&A really get you? Many outside the information systems security field do not realize that C&A is just an *assurance* process that does not in and of itself provide any security. It provides only a level of confidence (i.e., assurance) that the system/network in question is compliant with the security requirements levied against it, and attempts to quantify the risks associated with any security weaknesses identified by the testing. Ultimately, an approving authority uses this risk information to decide whether or not the system/network in question will be allowed to operate for the next three years. There are inherent problems with C&A as the DoD has been performing it for decades; problems that will persist even using the NIST RMF.

C&A presents only a "snapshot" of the system's compliance when the system was tested. System and network administrators generally have too much to do and have to deal with many competing priorities. If keeping the system/network secure is not at the top of their list of priorities, administrators may put off their security related duties (e.g., patching and proper configuration management) until a certification test is imminent. Then they will "surge" to clean up the security posture of their system/network just for the test. This has been a common scenario identified by US Army Information Systems Engineering Command (USAISEC) certification testers. The result of this type of paradigm is systems and networks that remain in a poor state of security until just before a certification test takes place. After testing is completed the system/network may once again fall out of compliance and its security posture will be significantly reduced. Of course, the authorizing official has no way of knowing this when he/she is making the authorization decision, or afterwards as the system is being operated over time. The poor state of a system's security might never be known to those responsible for its approval until (at best) it is up for retesting and reaccreditation some time later, or (at worst) it is compromised in some way as a result of the vulnerabilities its administrators allowed to creep into the system over time.

C&A within the DoD has been an expensive endeavor. As surprising as it may seem, neither the individual services nor the DoD comprehensively track the costs associated with accomplishing the DIACAP process.[4] Nevertheless, previous experiences at the U.S. Army Information Systems Engineering Command's Information Assurance Directorate allow for a rough estimate of C&A costs for the average system and network. Since the implementation of the DIACAP in 2006, the Information Systems Engineering Command's certification testing costs for a small-to-moderate sized system (i.e., several servers along with associated devices) averaged approximately $30,000. The certification costs for a moderate sized campus area network (i.e., an installation of approximately 15,000 users) averaged over $150,000. The development and use of automated tools and increasingly efficient processes allowed for cost reductions over time, but only on the order of 10-20%. Even very small systems consisting of only one or two servers were rarely charged less than $20,000 due to the amount certification work (testing, analysis, reporting) required by the DIACAP regardless of the size and scope of the system. Given these average costs, extrapolated over the entire DoD and repeated every three years (or *more* often in cases where systems changed enough to require early reaccreditation), it is easy to see that the DoD spends many millions of dollars each year just performing certification testing on its information systems and networks. Further, this rough estimate covers only certification testing/reporting and does not even include the other costs associated with performing the DIACAP process such as system owners preparing the documentation required and maintaining their Plan of Action and Milestones (POA&M) as they address weaknesses found by testing. When these other costs are added in, it becomes even more clear that C&A within the DoD has been a hugely expensive requirement.

DoD's C&A processes continue to focus on testing and accrediting discrete individual systems/enclaves. Why is this a problem? It is a problem because systems and networks do not run themselves. Systems and networks are built and operated by people. When we focus on testing and accrediting only the system or network, that is akin to issuing a driver's license to an automobile instead of the driver responsible for operating that automobile. While completing over 700 certification tests on information systems and networks of all types and sizes, time and time again USAISEC certification testers observed that organizations that had mature security processes, and made them a part of their day-to-day operations (i.e., *operationalized* them), maintained secure systems and did well during certification testing. Conversely, organizations that did not operationalize their security processes invariably had poorly secured systems and did poorly during certification testing. The lesson is, test the people and the security processes they have in place, not just the systems and devices, for a more accurate picture of the long term security posture of that organization.

The C&A process as currently required by DoD takes too long to be effective. In a speech in 2009, General Peter Chiarelli, then U.S. Army Vice Chief of Staff, discussed the rapid development and deployment of the Command Post of the Future (fielded in 2005) and the Tactical Ground Reporting System (fielded in 2008), which provided U.S. forces in Iraq with important new capabilities.

> He [GEN Chiarelli] had a major hand in bringing these systems to the field *without going through the traditional IA certification process*. (italics and underlining added for emphasis) Both were developed by the Defense Advanced Research Projects Agency outside of the DoDI 5000 acquisition process. In justifying the reasons for this, General Chiarelli characterized the IA certification process as broken and stated that, if the Army had had to put these systems through the traditional IA certification process, Command Post of the Future would only now be reaching troops in the field, in 2009. And, even though the Tactical Ground Reporting System completed initial development in 2008, by the end of 2009, more than 19 brigade combat teams will be equipped with this new information system (IS).[5]

The C&A process, as currently implemented, is not compatible with the rapid rate of change that systems and networks undergo constantly. "The GIG is a constantly changing and growing network of networks. In addition, the advent of Web services and service-oriented architectures (SOAs) has further increased the interconnectivity of DoD and federal ISs. SOAs are becoming the standard design paradigm for new and emerging DoD ISs."[6] Further, the DoD Strategy for Operating in Cyberspace, published July 2011, ups the ante on our current C&A processes. Strategic Initiative Five in the document calls upon the DoD's acquisition process for information technology to become much more dynamic and agile. It will do this by adopting five principles:

- Speedier fielding processes
- Employing incremental development and testing
- Sacrificing or deferring customization when possible

- Applying differing levels of oversight based on prioritization of critical systems
- Focusing on the security of the systems that DoD buys, including software and hardware

The strategy calls for the rapid movement of concepts from an innovative idea, to pilot program, to scaled adoption across the DoD enterprise. In short, “DoD’s cyberspace acquisition programs will reflect the adaptive nature of cyberspace; it will emphasize agility, embrace new operating concepts, and foster collaboration across the scientific community and the U.S. government as a whole.”[7] The current highly structured, process-intensive, and time-consuming C&A process the DoD relies upon is not a good fit for the fast moving and rapidly changing environment described in the strategy document.

Federal Information Security Management Act of 2002

In 2002, Title III of the E-Government Act, commonly referred to as the Federal Information Security Management Act (FISMA) was passed by Congress and signed into law by the President. FISMA requires federal agencies, to include the DoD, to “develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.”[8]

Unfortunately, as often happens, the original good intentions of a requirement like FISMA gets corrupted over time, and those who have to meet the requirement eventually focus more on the process and less on the goodness that the requirement was intended to promote in the first place. Consequently, for many federal organizations, FISMA resulted in a focus on compliance (i.e., checking the blocks) and not on risks; on reporting rather than actual security. Four years after FISMA was enacted, well regarded security experts were criticizing FISMA as a “well-intentioned but fundamentally flawed tool. 'A lot of your money is being thrown away,' Alan Paller, director of research for the SANS Institute, told an audience at the (2006) RSA IT security conference. The 2002 act mandates security planning for agencies, requiring a risk analysis of IT systems, and certification and accreditation of those systems. 'FISMA wasn't written badly, but the measuring system they are using is broken,' Paller said. 'What we measure now is, 'Do you have a plan?' Not whether the plan actually improves security.'”[9]

Fortunately, this issue has not been lost on the information systems security practitioners in government or our lawmakers. On April 26, 2012, The U.S. House of Representatives passed a proposed update to the FISMA called the Federal Information Security Amendments Act of 2012. This update calls for the implementation of automated and continuous (i.e., realtime) monitoring “when possible.”[10] The inclusion of the qualifier “when possible” could be problematic later but this is a step in the right direction; assuming this concept is eventually signed into law. Unfortunately, this update still misses the mark in its reporting requirement, which is that federal agencies must submit “an annual report on the adequacy and effectiveness of information security policies, procedures and practices, and compliance with the requirement of this subchapter.”[11] It seems, despite changes in the way the Federal Information Security Management Act is being implemented, the emphasis is still on reporting rather than on actual security posture. As a result, “the new FISMA looks a lot like the old FISMA.”[12]

Still, FISMA did heighten awareness of systems security across the federal government and at least began to hold agencies accountable for the security of their information systems and networks.

How Does the Commercial/Private Sector Handle C&A?

In general, there are no mandated information systems security requirements or C&A process in the commercial/private sector that are comparable to the DoD's security controls and C&A process. One exception is the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which protects the privacy of individuals' personal health information, establishes certain patient rights, and specifies a series of administrative, physical, and technical safeguards that "covered entities" (such as insurance companies and health care providers) must use to assure the confidentiality, integrity, and availability of electronic protected health information.[13] However, while HIPAA levies privacy and security requirements, it does not mandate any certification & accreditation mechanism. It only specifies implementation of the safeguards and requires covered entities to make proof of implementation available to the Federal Government upon request.

For the most part, commercial/private entities make their own internal assessments as to how much security their systems and networks require, and implement security safeguards accordingly. In these cases, security requirements are generally not well documented nor is there any formal process in place for testing safeguards or authorizing the operation of systems. In certain cases commercial entities do recognize the importance of the confidentiality, integrity and availability of their corporate information and take concrete steps to protect their systems and networks. Typically, this type of scenario would involve the development of internal company policies, procedures and standards for systems and information security based on recognized best practices; pre-deployment configuration and testing of information systems/devices on the corporate network; independent auditing of business critical systems; and establishment of an internal security review process to ensure ongoing compliance. These duties and responsibilities are typically split between the information technology (IT) department and the security department.[14] Some companies may even find it advantageous to take their systems security efforts to the next level and implement a recognized standard such as the International Organization for Standards (ISO) 27000 Series of standards, which provides an overall framework for an organization's information systems security program. The organization can be independently certified as meeting the requirements of ISO 27001, Information Security Management System. ISO 27002 provides "security techniques" or best practices that can be implemented by an organization as part of their certification effort.[15] Most likely, the main motivation a company would have for achieving an ISO 27001 certification would be to increase their stature and marketability, and separate themselves from their competitors. IT or security service providers and networking and communications companies would be prime examples. An ISO 27001 certification demonstrates to potential customers that the organization has mature security processes that have been verified by an independent third party. This certification would be a feather in their corporate cap and, therefore, worth the effort and expense. What lesson might the DoD draw from this corporate example? That it may be more useful and efficient to focus on an organization's process maturity than it is to focus just on testing and approving its systems. Technology is temporary, while organizational maturity endures.

NIST Risk Management Framework

In 2007, the NIST, the Intelligence Community (IC), the DoD, academia, and commercial industry collaborated to develop and implement a more standardized, streamlined and effective certification and accreditation process. The result is the NIST Risk Management Framework (RMF) as specified in NIST Special Publication (SP) 800-37. The RMF has already been adopted by all other Federal agencies, and the DOD has begun its initial steps in its transition from the DIACAP.[16] As mentioned earlier in this paper, the current DIACAP already aligns closely with the RMF in both process and intent. Noteworthy differences include a new lexicon and changes in some of the roles associated with the new "assessment and authorization" process (formerly known as certification and accreditation under the DIACAP).

Additionally, the RMF puts significantly more emphasis on "Continuous Monitoring" activities that take place after a system is granted its authorization to operate. Continuous Monitoring is addressed in more detail below.

Finally, the most significant impact of the NIST/IC/DoD collaboration is the new set of security controls specified in NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations. "DIACAP practitioners will find the NIST library more substantial in quantity, yet more granular and specific within the scope of each control. Technical practitioners will find the text of NIST control descriptions and validation procedures more clear and concise, since they were written by their technical peers and contain less of the FISMA influenced legal bent often attributed to the DIACAP controls."[17] NIST also intends to revise the controls every 18 months based on new threats, attack trends and other factors.

Will the DoD's transition to the NIST RMF and NIST Security Controls make certification and accreditation (or rather, assessment and authorization) within the DoD more effective and efficient? This question can only be answered after some time has passed and a significant amount of study and analysis have been done. The only thing we can say now is that two of the *anticipated* benefits of this Government-wide standardization in the RMF process and the controls used are reciprocity and the cost savings that should result from this reciprocity.

SANS Top 20 Critical Controls

A collaborative effort between the National Security Agency, the Center for Internet Security, the Systems Administration, Networking and Security (SANS) Institute, and several other organizations during 2008 and 2009 produced a set of 20 "critical controls" that addressed the most prevalent computer/network attacks experienced by government and commercial organizations. The premise was that organizations rarely have the resources to do everything that the numerous formal requirements, such as FISMA, levy upon them. They also do not have the resources to protect their systems and networks from every possible security threat that exists on the net. As such, it makes good sense to use available limited resources to focus on addressing the most prevalent and potentially damaging threats currently being faced. Also, as threats evolve, new threats emerge, and old threats disappear, a system owner's focus and efforts must shift accordingly in order to remain effective. For this reason the critical controls themselves, as well as the accompanying implementation guidance, are updated as time passes and threats change. For example, as zero-day attacks increased and advanced persistent threats became more prevalent, new sub-controls were added to address the need for more rapid detection and prevention of attacks. As of this writing, SANS has released Version 4 of the 20 Critical Controls.[18] Since its inception, the SANS Top 20 Critical Controls/Consensus Audit Guidelines (as they are now known) have proven very successful in helping organizations to achieve effective security and reduce their exposure (and resulting risk). The U.S. State Department was one of the first and most diligent organizations in adopting the use of the 20 critical controls and consensus audit guidelines. During 2009, it established a risk identification and mitigation program leveraging automated monitoring tools wherever possible, and successfully reduced its security risk level on its unclassified networks by 90 percent in overseas sites and 89 percent in domestic sites. The State Department's risk level has remained relatively stable since then, as well.[19]

Continuous Monitoring

What might Information Security Continuous Monitoring (ISCM) offer? The DoD has and continues to implement ISCM technologies such as Host Based Security System and Assured Compliance Assessment Solution in order to monitor, essentially in *realtime*, the security posture of its systems and networks. ISCM is defined as "maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions."[20] The objective of a continuous monitoring program is to determine if the security controls applied to an information system (to include any inherited controls) continue to be effective over time even as changes to the system itself, as well as changes in the operating environment, threats, etc., occur.[21]

ISCM is a very good idea but there are currently problems with the concept. NIST itself relates in its main ISCM guidance document that “ISCM is most effective when automated mechanisms are employed where possible for data collection and reporting. While this document encourages the use of automation, it is recognized that many aspects of ISCM programs are not easily automated.”[22] Organizations face significant challenges with the technologies that enable automated monitoring. “Organizations typically use a diverse set of security products from multiple vendors. Thus it is necessary to extract security-related information (ideally in the form of raw system state data) from these tools and to normalize that data so that it is comparable.”[23] This type of work can be labor intensive, time consuming, and requires skilled analysts even when they are leveraging automated analysis tools.

Also, not all of the security controls that the DoD requires can be monitored in an automated fashion. An analysis commissioned by the Army’s Office of the Chief Information Officer (CIO)/G-6 in 2012 determined that only approximately 32% of the security controls embodied within the SANS Top 20 Critical Security Control Areas were automatable through continuous monitoring of information obtained from the machine to machine transfer of data from Network Operations and Continuous Monitoring tools. The other approximately 68% of controls, such as Incident Response and Data Recovery Capability, would have to be assessed using non-automated methods such as human reviews of policies, procedures and other documents, as well as onsite inspections and interviews. The analysis also determined that the SANS Top 20 controls actually only represented 287 out of the 617 security controls specified in NIST Special Publication 800-53.[24] Major control areas such as Program Management, Awareness and Training, and Physical and Environmental Protection are not addressed in the Top 20. The significance of these findings is that they demonstrate that purely automated monitoring can introduce some efficiency and timeliness into a Continuous Monitoring program, but automated monitoring alone, given the current state of the art, is not nearly enough.

Federal Risk and Authorization Management Program

In December 2011, the Federal Chief Information Officer (CIO) officially announced the kick-off of the Federal Risk and Authorization Management Program (FedRAMP), an assessment and authorization process exclusively for Cloud Service Providers (CSP). The FedRAMP is intended to provide a cost-effective, risk-based approach for Federal agencies' use of cloud services by:

- Standardizing security requirements (based on the NIST SP 800-53 controls) for the authorization and ongoing cyber-security of cloud services
- Implementing an assessment program capable of producing consistent independent, third-party assessments of security controls implemented by CSPs
- Standing up a Joint Authorization Board (JAB) consisting of security experts from the Department of Homeland Security (DHS), the DoD, and the General Services Administration (GSA) that will review all CSP authorization requests
- Standardizing contract language to help Executive departments and agencies integrate FedRAMP requirements and best practices into their acquisitions
- Maintaining a list of approved CSPs and a repository of authorization packages for cloud services that can be leveraged government-wide

Additionally, FedRAMP is intended to reduce duplicative efforts, inconsistencies and cost inefficiencies associated with the current security authorization process.[25] As the DoD moves towards a more consolidated, cloud based, enterprise level information environment for reasons of fiscal austerity, ease of management and standardization, the FedRAMP initiative aligns very well with this shift. Of course, cloud based computing is not without its own set of security risks but the Federal Government, with its FedRAMP effort, has gotten out in front and established what appears to be a well organized program to mitigate those risks, while allowing Federal agencies to take advantage of the benefits offered by cloud services sooner rather than later. Using the current DIACAP or NIST RMF assessment and authorization methodologies, with no recognition of and adjustment for the nature of cloud based computing, would take far too long and cost too much. That reality would simply stand in the way of necessary progress and slow (in some agencies, stop) the DoD's shift to the more consolidated, cloud based, enterprise level information environment it seeks. Currently, there are two CSPs approved under the FedRAMP process to provide cloud services. More than 80 CSPs have applied for FedRAMP authorization, and more than 50 companies have applied to third-party assessment organizations for review, with 16 being successfully tested to date.[26]

The DoD Joint Information Environment

Recognizing the benefits of cloud based computing, the DoD has made the shift to cloud based services an important part of its Joint Information Environment (JIE) concept. Along with providing common services at the enterprise (i.e., DoD) level, architectures shared across the services, and consolidation of servers into large scale data centers, the department will move toward cloud computing, which offers great efficiencies not only in hardware and software, but also in data sharing.[27] The move to a Joint Information Environment is intended to have positive security impacts as well. According to GEN Keith Alexander, U.S. Army, current Commander of the DoD's Cyber Command and Director of the National Security Agency:

> Our current information systems architecture in the Department of Defense was not built with security uppermost in mind, let alone with the idea of operationalizing it to enable military missions. Instead, we have seven million networked devices in 15,000 DoD network enclaves. Our vision is to fashion that architecture into an operational platform, not just a channel for communications and a place for data storage. To do so, our DoD cyber enterprise, with the Department's Chief Information Officers, DISA, and Cyber Command helping to lead the way, will build a common cloud infrastructure across the Department and the Services that will not only be more secure but more efficient--and ultimately less costly in this time of diminishing resources--than what we have today. Our operational objectives are to reduce the number of network enclaves to the minimum possible; to implement a common cloud-based infrastructure to improve security across all of DoD.[28]

Given the fast moving nature of the technology and the DoD's timeline, the move to a Joint Information Environment will require timely, adaptive and effective security processes to ensure the transition does not introduce unacceptable levels of risk. The DoD's current C&A process is not timely or adaptive enough to support this transition and provide the level of assurance that the DoD needs.

Conclusions

Have the approaches used by the DoD to test and approve its systems and networks over the years improved the DoD's security posture and lessened the DoD's risks? After over three decades of testing and accrediting our systems, you might assume our systems would be highly secure and successful intrusions would be rare. Unfortunately, this is not the case. The DoD's Strategy for operating in Cyberspace, published in July 2011 warns that "Foreign cyberspace operations against U.S. public and private sector systems are increasing in number and sophistication. DoD networks are probed millions of times every day, and successful penetrations have led to the loss of thousands of files from U.S. networks and those of U.S. allies and industry partners."[29] In one of the more well known incidents, code-named TITAN RAIN, hackers allegedly from China were able to penetrate "hundreds" of unclassified networks belonging to the DoD and other U.S. agencies.[30] Compounding the challenge for traditional C&A is the sheer size and complexity of the DoD's constantly changing networks. The "DoD operates over 15,000 networks and seven million computing devices across hundreds of installations in dozens of countries around the globe."[31] This paradigm makes almost every accreditation accomplished using current processes "OBE" ("overcome by events") almost as soon as it is completed.

Possible Alternative and/or Supplemental Approaches

One concept that has been discussed at the US Army Information Systems Engineering Command's Information Assurance Directorate is the certification and accreditation not of systems, but of the *organizations* that develop, manage and operate systems.[32] This organizational INFOSEC maturity approach is similar in concept to the ISO 27001 certification described earlier in this paper. The FedRAMP program, also described previosly, takes a step in this direction by focusing on the cloud service provider. Using an organizational maturity accreditation approach would work for any organization, no matter what type of information technology responsibilities it had. For example:

- Organizations that develop and field (and possibly provide lifecycle support to) new systems (e.g., Program Managers, rapid development programs, etc.)

- Organizations that operate large networks and/or enclaves on a daily basis (e.g., Army Network Enterprise Centers [NEC], data centers, Continuity of Operations/Disaster Recovery [COOP/DR] sites, etc.)
- Organizations that operate their own smaller networks and/or enclaves for internal business purposes
- Organizations that provide cloud based services (similar to the approach FedRAMP takes with cloud service providers)

All these organizations could be assessed in terms of the adequacy and maturity of their organizational security processes and be accredited on that basis.

This organizational accreditation approach resolves many of the issues associated with the current DoD C&A process previously identified in this paper. It resolves the issue of C&A being a “snapshot in time” approach because it is not focusing on the security posture of a system, network or device *today*, but on the ability of the organization to develop, manage and operate its systems in a secure manner over a period of time. It resolves the issue of current C&A not being agile and adaptive enough to accommodate the rapid pace of advancements in the information technology field. Since accreditation is not tied to the technology (i.e., the systems and devices), but to the organization itself, the organization is trusted to update its technology in a controlled and secure manner – no constant system re-certifications and reaccreditations required. The development and fielding of new systems can be accomplished much more rapidly because C&A, often the “long pole in the tent,” is no longer tied to the system itself. The Program Manager’s organization has already proven that it can develop and field a secure system, so system deployment can be accomplished without delay and the system carries with it the accreditation of the organization. Last but not least, an organizational accreditation approach will result in significant cost savings for the DoD. The number of organizations that would undergo the accreditation process is much smaller than the number of systems and networks that currently require accreditation thereby greatly reducing the expense of accomplishing and tracking accreditations across the enterprise. Lastly, the time period an organizational accreditation is good for could be increased from the current three year period, thereby introducing additional cost savings.

This shift in approach will not require a wholesale scrapping of previous work that has already been done to improve system/network security. Many, if not most, of the requirements embodied in the NIST SP 800-53 controls actually apply to organizational processes and are adaptable to organizational accreditations with little or no modification. Likewise, the NIST Risk Management Framework (NIST SP 800-37) can be adapted by the DoD if it chooses to accredit organizations rather than discrete systems.

Continuous monitoring as described earlier in this paper also holds great promise in lowering the level of risk to DoD systems. Continuous monitoring should not replace C&A but should augment it. It should not replace C&A because, as related above, there are controls that cannot be monitored in an automated fashion. Those controls can be assessed as part of a periodic C&A process, and even periodically reassessed thereafter, but to say they can be “continuously” monitored is not realistic. Whether used in the DoD’s current C&A paradigm or in an organizational accreditation approach, continuous monitoring serves as the “cop on the beat,” monitoring the neighborhood and addressing issues as they surface (i.e., in realtime). The sooner vulnerabilities can be identified and resolved or mitigated, the smaller the DoD's exposure will be (in time and footprint), and the lower the risk level will be. A continuous monitoring program "helps to ensure that deployed security controls continue to be effective and that operations remain within stated organizational risk tolerances in light of the inevitable changes that occur over time. Information collected through the program supports ongoing authorization decisions."[33]

The DoD's shift to a Joint Information Environment and the proliferation of cloud based and/or enterprise level services holds promise for the DoD as well. The more centralized these services can be, the easier and more cost effectively they can be managed, operated and possibly most importantly, secured. The flip side of that argument is that a compromise or disruption would have a much greater impact on the DoD than if services were decentralized. The reality is that larger service providers enjoy an economy of scale that smaller providers do not. They can resource their security efforts better, have fewer points of failure in aggregate, can afford greater redundancy, and are significantly more capable of keeping services secure and available. In fact, the FedRAMP process verifies the cloud service provider's security posture, or that service provider is not approved for use.

The DoD-wide adoption of the SANS Top 20 Critical Controls/Consensus Audit Guidelines would represent a significant augmentation to any C&A approach the DoD uses. As mentioned previously, organizations rarely have all the resources they need to dedicate to system/network security. During the next several years, looming budget cuts will only make this problem more acute. As such, the ability to prioritize security efforts so an organization is getting maximum “bang for the buck” will be critical. Focusing on the Top 20 Controls, which in turn address the top 80-90% of threats/risks, gives an organization the biggest return on its security investment. Of course, adopting the Top 20 Controls does not relieve an organization of responsibility for the other controls or the bottom 10-20% of risk they represent, but if (as mentioned) we can’t do *everything*, should we not be making the best decisions possible about what we *are* going to do?

In closing, despite three decades and huge sums of money expended on certifying and accrediting its systems and networks, the DoD still experiences daily penetrations of its systems and significant losses of data. If the DoD continues to use a formal certification and accreditation (or “assessment and authorization”) process, as it appears it will, it should move away from focusing accreditations on discrete systems and networks and instead focus on the organizations that develop, manage and operate those systems and networks. The RMF and NIST controls are easily adaptable to this approach. This would result in significant cost savings as well as saving significant amounts of time in the system development and fielding process. The DoD should continue its move to a Joint Information Environment and leverage FedRAMP approved cloud based services as much as possible. It should continue to improve upon and expand automated continuous monitoring capabilities and use continuous monitoring to augment, but not replace, the accreditation process. It should formally adopt the SANS Top 20 Critical Controls/Consensus Audit Guidelines as an approved methodology for resource limited organizations to focus on the greatest risks.

Endnotes

[1] U.S. Department of Defense, *Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP)*, Department of Defense Instruction 5200.40 (Washington, DC: U.S. Department of Defense, December 30, 1997), 4.

[2] Peter Williams and Tiffani Steward, “DoD’s Information Assurance Certification & Accreditation Process,” *Defense Acquisition Technology and Logistics* 36, no. 5, (September-October 2007): 12-13.

[3] Rebecca Onuskanich, “Out with the DIACAP, In with the DIARMF” white paper, December 12, 2011, http://www.xlr8-technologies.com/CMS/admin/Assets/lunarline/assets/pdfs/%20whitepapers/out%20with%20diacap%20in%20with%20diarmf%20-%20lunarline%20white%20paper_dec%2011.pdf (accessed November 12, 2012).

[4] The author made queries to the offices of the Chief Information Officers (CIO) of the Departments of Defense, Army, Navy and Air Force. The DoD CIO representative contacted related that this type of data was not tracked or held at the DoD level and would only be available from the individual services. The Army and the Navy CIO representatives contacted related this type of data was not collected and so was not available. The Air Force CIO representative did not respond as of the writing of this paper.

[5] Eric Landree, Daniel Gonzales, Chad Ohlandt and Carolyn Wong, *Implications of Aggregated DoD Information Systems for Information Assurance Certification and Accreditation* (Santa Monica, CA: Rand National Defense Research Institute, 2010), 3.

[6] Ibid., 2.

[7] U.S. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*, (Washington, DC: U.S. Department of Defense, July 2011) 11.

[8] *National Institute of Standards and Technology* web site, Federal Information security Management Act (FISMA) overview page, http://csrc.nist.gov/groups/SMA/fisma/overview.html (accessed December 12, 2012).

[9] William Jackson, “FISMA Effectiveness Questioned,” March 18, 2007, http://gcn.com/articles/2007/03/18/fismas-effectiveness-questioned.aspx (accessed November 12, 2012).

[10] U.S. House of Representatives Bill H.R. 4257: Federal Information Security Amendments Act of 2012 full text, http://www.govtrack.us/congress/bills/112/hr4257/text (accessed December 15, 2012).

[11] Ibid.

[12] William Jackson, “New FISMA Looks a lot Like Old FISMA, Survey Finds,” September 13, 2012, http://gcn.com/articles/2012/09/13/datapoint-federal-it-security-survey.aspx (accessed December 13, 2012)

[13] *U.S. Department of Health and Human Services Health Information Privacy Home Page*, http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html (accessed February 3, 2013).

[14] Steve Lipner, Partner Director of Program Management, Trustworthy Computing Security, Microsoft Corporation, telephone interview by author, January 22, 2013; and email message to author, January 23, 2013.

[15] *ISO 27000.org Home Page*, http://www.27000.org/index.htm (accessed February 3, 2013).

[16] Onuskanich, "Out with the DIACAP, In with the DIARMF," 3.

[17] Len Marzigliano, "Goodbye DIACAP, Hello DIARMF," November 17 2011, http://resources.infosecinstitute.com/goodbye-diacap-hello-diarmf/ (accessed 12 November, 2012).

[18] SANS 20 Critical Security Controls Home Page, http://www.sans.org/critical-security-controls/ (accessed February 8, 2013).

[19] Statement of Mr. John Streufert, Deputy Chief Information Officer for Information Security, U.S. Department of State; before the U.S. Congress, House or Representatives, Committee on Oversight and Government Reform Hearing: *Federal Information Security – Current Challenges and Future Policy Considerations*, 111th Congress, 2nd sess., March 24, 2010, 30.

[20] U.S. Department of Commerce, National Institute of Standards and Technology (NIST), *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, NIST Special Publication (SP) 800-137, (Washington, DC: U.S. Department of Commerce, September 2010), 1.

[21] *National Institute of Standards and Technology* web site, Continuous Monitoring FAQs, http://csrc.nist.gov/groups/SMA/fisma/documents/faq-continuous-monitoring.pdf (accessed December 13, 2012).

[22] National Institute of Standards and Technology, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, 2.

[23] Ibid, D-16.

[24] John Modrich and Tom Stuckey, *Whitepaper: Continuous Monitoring (CM) – Re-Certification and Authorization of Systems using Automatable CM Data to Evaluate Risk on a Continual Basis*, (MITRE Corporation, March, 2012), 2.

[25] Federal Chief Information Officer Steven VanRoekel, "Security Authorization of Information Systems in Cloud Computing Environments," memorandum for Chief Information Officers, Washington, DC, December 8, 2011.

[26] Matthew Weigalt, "FedRAMP Certifies a Major Player," February 1, 2013, http://fcw.com/articles/2013/02/01/cgi-fedramp.aspx (accessed February 3, 2013).

[27] Claudette Roulo, “Official Describes Joint Information Environment,” October 3, 2012, American Forces Press Service, http://www.defense.gov/news/newsarticle.aspx?id=118092 (accessed February 2, 2013).

[28] Statement of LTG Keith Alexander, Director NSA and Commander USCYBERCOM, to the U.S. Congress, Senate, Armed Services Committee Hearing: *U.S. Strategic Command and U.S. Cyber Command in review of the Defense Authorization request for FY2013 and the Future Years Defense Program*, March 27, 2012, http://search.proquest.com.ezproxy.usawcpubs.org/docview/963523011# (accessed December 16, 2012).

[29] U.S. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*, (Washington, DC: U.S. Department of Defense, July 2011) 3.

[30] Bradley Graham, “Hackers Attack Via Chinese Web Sites,” Washington Post, August 25, 2005, http://www.washingtonpost.com/wp-dyn/content/article/2005/08/24/AR2005082402318.html (accessed December 16, 2012)

[31] U.S. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*, (Washington, DC: U.S. Department of Defense, July 2011), 1.

[32] U.S. Army Information Systems Engineering Command, *Assurance in Depth*, Concept Paper (Fort Huachuca, AZ: U.S. Army Information Systems Engineering Command, May, 2001), 4.

[33] National Institute of Standards and Technology, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, 1.