AU/ACSC/2016

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

AIR FORCE IT SYSTEM SECURITY COMPLIANCE WITH LAW AND POLICY

by

Randy J. Michael, DAF, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor(s): Dr. Richard Smith and Dr. Patricia Williams Lessane

Maxwell Air Force Base, Alabama

April 2016

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Table of Contents

DISCLAIMER II

TABLE OF CONTENTS III

PREFACE IV

ABSTRACT V

INTRODUCTION 1

LAW AND POLICY 6

METHODOLOGIES 9

POSSIBLE SOLUTIONS 15
- Option 1: Air Force Policy Changes 15
- Option 2: DoD and AF Methodology Changes 16
- Option 3: DoD and Air Force policy and Methodology Changes 16
- Option 4: Cloud Computing to Eliminate Policy and Methodology Requirements 17
- Option 4: Application Rationalization 18

CONCLUSION 19

RECOMMENDATION 20

BIBLIOGRAPHY 27

PREFACE

The idea for this paper comes from my 24 plus years working in the information assurance field; as both a military member and as a civil servant for the Air Force. In those many years the one true standard has been that the policy's and methodology's utilized to further the requirements of public law and policy would not always align with commander's direction, mission requirements, allotted resources, or even with each other. All history aside, I have always agreed in principal with the overarching reasons behind the laws and policy's associated with securing our governments Information technology and the data contained within. This belief has always driven me to believe that there is a way to balance security with mission requirements in a way that minimizes overhead and excessive burocracy.

I would like to thank all the instructors throughout who have done so much to guide me through this program. I would also like to thank all of my peers who took the time to provide me with exceptional feedback and support each week at the cost of time with their family, friends, and time spent on their own assignments. I also would like to thank the people I work with who provided constant support to me throughout this program. I especially would like to thank my wife and children,, without whose support I never would have completed this effort. They provided constant support and understanding on long days working on this effort without ever complaining. My need to complete this course became their need for me to complete this course, they made it a priority for not just me, but for them as well.

ABSTRACT

As the warfighters need for Information Technology (IT) and the data contained within increases, so does the need for Information Assurance (IA) (data integrity) to support mission assurance. To ensure IA and to support the mission, changes need to be made to Air Force IT policies and methodologies to facilitate compliance with public laws, DoD guidance, and ensure IT security to support the warfighter. To support those needs there are public laws in place mandating IT security, as well as a plethora of DoD and AF policy's, instructions, and methodologies to further the goal of accomplishing those requirements. The issue at hand is the complexity of having layered implementation of a requirement so vital to the warfighter, and the seemingly inherent burocracy those layers of policy and methodology impose of the IA practitioner working to secure and comply with the requirements of public law. Currently the AF and DoD are working on multiple fronts to instill IA in IT, focus resources, and support the warfighter. The AF and DoD need to focus on the warfighter and consolidate the DoD IT footprint to the greatest extent practicable. This will remove excess layers of policy and burocracy; enabling the implementation of IA by streamlining down to those requirements which both secure data and support the warfighter.

INTRODUCTION

Information Technology (IT) systems and the data they contain are required to be secure. The application and implementation of security standards is a requirement of public law; and are implemented through federal regulations, Department of Defense (DoD), and Air Force (AF) policy. The importance of IA and its necessity to be implemented across the AF is not an isolated requirement; "…cyber threats to military and commercial sectors are growing, and that criminals have exploited 75 percent of our nation's computers"[1] should be of grave concern to all. Current policy does not always resemble the requirements of the framework codified in public law. Current AF processes do not adequately support the documentation of the security status of existing and developing IT systems in the AF inventory, as required by law. Existing and new IT systems security posture is not being documented quickly enough to support the new and existing systems. Current and developing airframes each require unique IT/cyber systems for support and operation. Today's system certification and compliancy tracking methods are very costly, time intensive, unrealistic, and often lag behind operational and test requirements. However, with changes to policy and implementation requirements, the IT system certification processes may be modified to enable the certification of IT systems and the security of Air Force data.

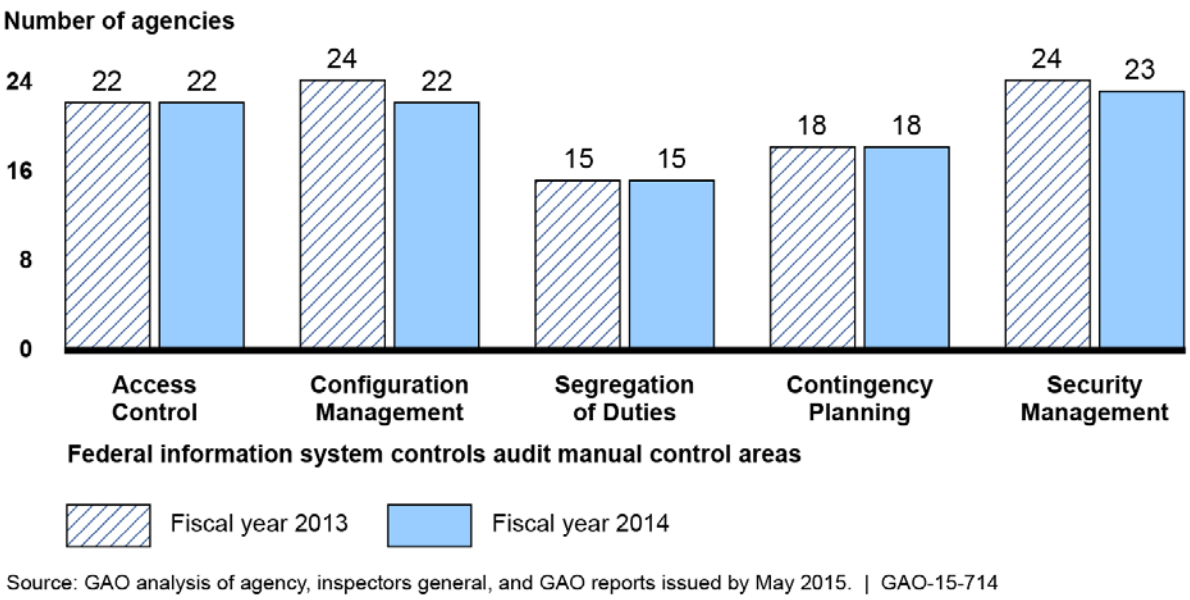
This research will utilize the problem/solution framework, and it will attempt to outline the requirements to keep Air Force IT systems and the data they contain secure and compliant with the requirements for IT system security. The research will work to find a more optimal[2] and

feasible solution to the question posed. By analyzing the current Air Force IT processes and those of other federal agencies, the research will define the problem and associated issues. Additionally, the research shall provide quantitative analysis of the data and sources utilized. Review of primary, secondary, and tertiary sources will provide the material needed to propose solutions based on the current requirements for the security of government systems and data. Comparative analysis of the proposed solutions will suggest a final solution recommendation, and provide implementation guidance.

There should be no argument that there is a valid need to ensure that information systems (IS) operated by the Air Force should be secure from outside intrusion (hacking), and that the data contained within those systems such as Personally Identifiable Information (PII), mission data, and flight test data on new and existing airframes should be secured and have a high level of assured integrity. It is the methodology to include the required process which should be currently and regularly challenged to ensure they are appropriate (to include cost and effort level required) and effective. DoD policy lacks the necessary clarity to adequately maintain the requirements of public law, even if initially an IT system is accredited as "…the process for reaccreditation of subsequent releases is vague and confusing."[3] The DoD Information Assurance Certification and Accreditation Process (DIACAP) is the DoD process for securing information systems to ensure compliance with the Federal Information Security Management Act of 2002 (FISMA). DIACAP compliance ensures information security; however, there is a cost to attain and maintain that compliance. The requirement and subsequent cost to certify and accredit information systems is should, included in the lifecycle of information systems. A lack of early and long-term planning in the system's lifecycle can increase the monetary burden on

system owners as there is "…a significant cost benefit to building in IA during the development phase"[4] of a system.

Current compliance costs are driven by both the size of the information system and its complexity. The larger and more complex a system is the greater amount of time is required to perform the required amount of security control tests and to document the systems test results and architecture. Any solution to issues raised would ideally include adding any C&A requirements in the system lifecycle planning process, which should allow people involved in the Planning, Programing, Budgeting, and Execution (PPBE) to have insight into the total cost of ownership of IT systems, and by doing this, encourage process optimization. Saving time and cost to the units and wings involved should be a top priority to those faced with budget and resource (Airmen) reductions. Systems not identified in the Enterprise Information Technology Database Repository (EITDR) IT systems cannot provide assurance that they or the data which they contain are secure. Insecure systems are a vulnerability not only to Air Force IT systems, but to the air frames and weapons systems they often support. A lack of proper registration and tracking can lead to an unknown number of unsecured systems. Overall there is not an adequate level of compliance within the federal government to ensure IT systems are secure and in compliance with FISMA. A 2015 Government Accountability Office (GAO) report identified deficiencies in how the federal government was ensuring IT security and compliance with FISMA; it found "…weaknesses in the processes used to implement FISMA requirements"[5] throughout the federal government (Figure 1).



Source: GAO analysis of agency, inspectors general, and GAO reports issued by May 2015. | GAO-15-714

Figure 1 Information Security Weaknesses at 24 Federal Agencies in Fiscal Years 2013 and 2014 [6]

There are multiple IT systems the government utilizes to track compliance and each of these systems tracks different requirements. There is however some overlap in compliance tracking, one example is that the EITDR and the DoD's Enterprise Mission Assurance Support Service (eMASS), both track the Certification and Accreditation (C&A) status of the IT systems entered into them. The AF and DoD both utilize eMASS to track Information Assurance (IA) "…system information, track the progress of IA activities of systems, and track current C&A status of systems."[7] Additionally the AF also utilizes EITDR to track C&A compliance along with many other compliance requirements.

The current methodology to ensure the security of information systems operating in the Air Force and DoD is extremely confusing, chaotic, conflicting, and costly. It necessitates great expenditures in both time and data security efforts. Currently, Air Force (AF) Information Technology (IT) systems are required to be Certified and Accredited (C&A) prior to being

operational. “C&A policies came about because of policy’s…including OMB Circular A-130”[8] which establishes necessary standards with respect to the management of federal information resources. These policys are meant to ensure that the IT systems are constructed within certain limits and minimum security standards. Once a system is constructed which meets or exceeds the minimum standards set forth in both law and policy, there is an additional Operation and Maintenance (O&M) requirement to ensure the IT system maintains its integrity and security throughout its lifecycle. There is a valid need to ensure that information systems operated by the Air Force should be secure from outside intrusion (hacking), and that the data contained within those systems such as business data, Personally Identifiable Information (PII), mission data, and flight test data on new and existing airframes should be secured and have a high level of assured integrity.

IT system security is a method, a method to ensure data integrity and security. Data security is the reason for IT security. The AF (entire government) needs to ensure that the data contained in its IT systems, data about things such as the F35, the Long Range Strike Bomber, stealth technology, and Personally Identifiable Information (PII), etc. The importance of the data is one aspect of what makes IT system security necessary. Stephany Bellomo and Carol Woody of the Software Engineering Institute have written about the effects of the “…lack of clarity”[9] concerning accrediting IT systems and the need to introduce security requirements early in the system acquisition lifecycle. Further pointing out that “…adding the security features late usually results in devastating changes to the architecture causing schedule delays and cost overruns.”[10]

LAW AND POLICY

There are many laws and policy's associated with IT system security, starting from FISMA at the congressional level to AFI33-210, which among other things "…establishes the AF Cybersecurity program and risk management framework (RMF) as an essential element to accomplishing the AF mission."[11]

Public Law 107-347[12], is known as the E-Government act and it requires the Office of Management and Budget (OMB) to report to congress on an annual basis the status of federal efforts to comply with Title III of the E Government Act of 2002. Title III section 301 of this act is more commonly known in the federal government as FISMA. This public law is the document from which all DoD and AF policy on the security of information systems is based. It recognizes "…the highly networked nature of the current Federal computing environment"[13] and states the requirement for implementing security controls for information systems to manage security risks. In the AF FISMA compliance is tracked in EITDR by AF level Subject Matter Experts (SMEs), Major Commands (MAJCOMs), IT system owners and Program Managers (PM).

OMB Circular A-130, "…revises procedures formerly contained in Appendix III to OMB Circular No. A-130"[14] also known as FISMA. It is important to understand that the original public law (FISMA) tasked OMB to report to congress on an annual basis. Therefore, it is logical that OMB would provide more detailed direction and structure down to the federal agencies in the form of this circular. Also this provides framework for those federal agencies to manage the security requirements and then feed the status to OMB on an annual basis. This Circular requires certain processes to occur and re-occur on a regular basis, including the scrutiny of IA controls.[15]

There is also the requirement to analyze and assess the risk associated with each security control at least every three years.[16] Among other things it "…encourages the use of automation to provide senior leaders the necessary information to make cost-effective, risk-based decisions with regard to the organizational information systems supporting their core missions and business functions."[17] As encompassing and authoritative as this appendix is for all federal IT systems, this circular appendix does not apply to certain National Security Systems (NSS). For those systems covered under other guidance, this appendix directs that they follow guidance specifically published for those systems containing NSS data.

DoD Instruction 8500.1, establishes a "…DoD cybersecurity program to protect and defend DoD information and information technology (IT)."[18] It is applicable to all DoD IT and all DoD information stored electronically, wherever that data or system may be. It further directs the implementation of a risk management framework all the way from the DoD down to the individual IS level. It directs that risk must be managed from early in the systems development lifecycle, throughout its use, and into sustainment. To achieve compliance with these requirements the AF is still utilizing DIACAP. There have been several delays in the implementation of RMF; however, the AF is moving towards implementing RMF at some un-announced point in the future.

DoD Instruction (DoDI) 8510.01 establishes the requirement for utilizing RMF for all IT within the DoD, [19] replacing DIACAP as the required process. This instruction replaces DIACAP with RMF. It is the direction given by the department of defense to ensure all agencies within the DoD are implementing security measures and controls utilizing RMF. It is applicable to all IT and electronically stored information in the DoD. It also mandates that resources for

implementing RMF must be budgeted for. This mandates that system designers and owners must budget for IT security.

Air Force Policy Directive (AFPD) 33-2, implements the AF IA program as it relates to FISMA, multiple DoD policy's, and other AF instructions. It is the AF implementation of DoDI 8500.01 which is the DoD IA instruction. This directive sets a framework for the creation of other AFIs to support IA in the AF. Specifically, it directs supporting instructions to follow the 33-2XX format when being written and implemented; with all 200 series publications such as AFI 33-210 to be specifically in support of the AF requirement to implement IA for the AF portion of DoD information systems. Among other things, according to AFPD 33-2, it "…addresses the Head of DoD Components responsibilities identified in DoD Directives in relation to Information Assurance."[20] It is the directive required to support the creation of all subsequent AFIs written to provide guidance on AF IA.

The AF fulfills the requirements of FISMA, DODI 8510.01, OMB circular A130, AFPD33-2, and others through its implementation of its own IT security strategy and process in AFI33-210. This instruction sets forth AF processes to certify and accredit AF systems while following DoDs guidance to utilize RMF. AFI 33-210[21] specifies the roles and responsibilities within the Air Force Certification and Accreditation Program (AFCAP) utilizing the Risk Management Framework (RMF) mandated by federal requirements. This AFI is applicable to all AF information systems with the exception of those NSS and systems containing Special Compartmental Information (SCI) under the purview of the Deputy Chief of Staff, Intelligence, Surveillance and Reconnaissance (AF/A2).

METHODOLOGIES

The DoD CIO has published many strategies/ methodologies to further the FISMA requirement of integrating IA into the IT system development process, as well as the need to be more fiscally responsible when developing, operating, and maintaining IT applications and systems. The DoD CIO's strategy for implementing the Joint Information Environment (JIE), implements the DoD's solution to the issues associated with the data acquisition shortfalls presenting themselves in the current operational environment where there are many separate operational environments providing less than optimal support to the warfighter.[22] The implementation of this strategy by the DoD validates that the needs of the warfighter should be the focus for IT application and system development, as well as establishing a method for consolidating those systems supporting the warfighter to a common architected environment.

Implementation of the JIE implements a Single Security Architecture (SSA) which means that IA can be integrated operated singularly versus across hundreds or thousands of separate architectures. This SSA can be manifested through standard architecture in DoD data centers as well as through DoD provided cloud solutions.[23]

Application rationalization (consolidation) is another part of the DoD's JIE and cloud computing strategies. It is a logical extension of FDCCI and its mandate to reduce the hardware and software footprint across the federal government. Application rationalization induces efficiencies through virtualization and strong rules of engagement for application development and sustainment. The DoD is moving to consolidate and eliminate duplicative applications so as

to focus both IA effort and monetary resources on remaining applications, promoting optimization.[24]

Considering the remaining applications being developed and maintained, the current methodology to ensure the security of information systems operating in the Air Force (AF) is the AFCAP outlined in AFI33-210. Currently, AF IT systems are required to Certified and Accredited (C&A) prior to being operational utilizing the DIACAP process and the new risk management framework. Although the AF is currently not fully implemented RMF in accordance with DoD policy, it is moving to integrate its methodology as soon as the necessary infrastructure and processes are in place. Unlike the DIACAP where IT systems are required to go through a lengthy re-certification process every 3 years, the RMF process will include real time monitoring of IT systems and thus not require re-certification unless the system owner implements changes which so drastically change the IA security status of an IT system that recertification becomes a necessity.

The DIACAP certification process enables system owners to integrate IA during system development, prior to system deployment. There is "…a significant cost benefit to building in IA during the development phase, as opposed to bolting on IA capabilities after an information system is operational."[25] There are inherent issues when using DIACAP, especially if the IT system owners are attempting to field the system quickly. Specifically, the delays in receiving accreditation using the DIACAP process are such that, according to Stephany Bellomo and Carol Woody of the Software Engineering Institute, "…the DIACAP process almost negates the benefits gained through rapid development methods."[26] As almost all government acquisition programs require at least one IT system to support it, it would only seem logical that the true cost of developmental information would be clearly defined early in the process, but often the total

cost of ownership in the system development lifecycle does not always adequately focus on the supporting existing IT systems. Bellomo and Woody also state that there is "…a lack of funding for projects already in the software maintenance phase to start emphasizing security"[27] needed to maintain or re-accredit SW and systems. DIACAP is the DoD enterprise wide approach to instilling information assurance in IT systems more efficiently and was meant to be less burdensome and laborious than previous methodologies .[28] The AF must utilize the DoD's DIACAP process to certify systems to operate (figure 3).

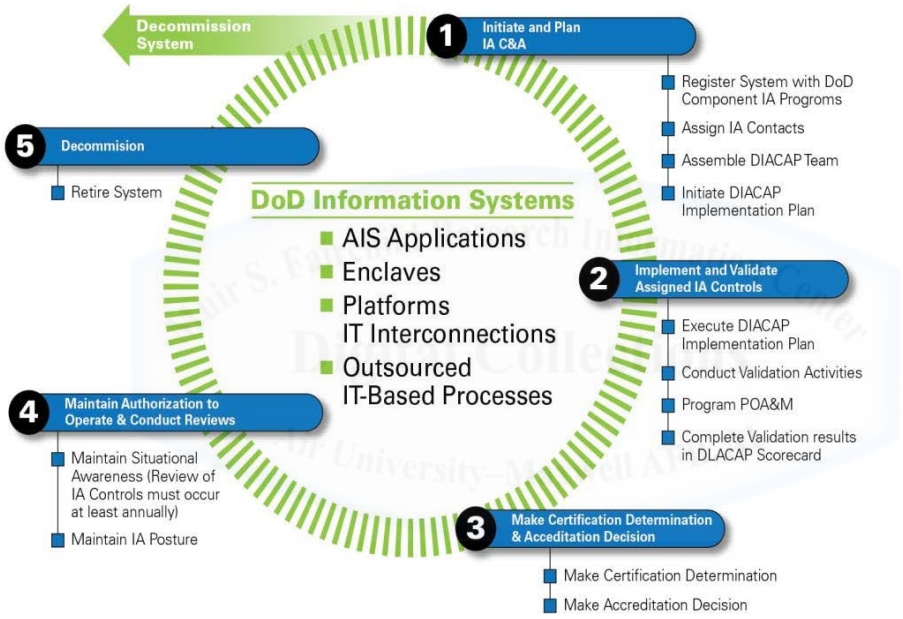


Figure 2 Department of Defense (DoD) DIACAP Process[29]

For the AF, this means using tools when appropriate to complete the DICAP to obtain a certification to operate a system in the most agile and timely manner possible. At the AF level, the tools used to track the state of IT system compliance and security are EITDR and eMASS. EITDR is the IT portfolio management system used by the AF to track IT systems and their compliance.[30] It is not however the tool used to actually complete the DIACAP process. The

eMASS tool is the method used to complete all IT system certification process. This process will soon migrate to the RMF process utilizing real time monitoring to maintain system security and certification to operate.

The RMF process (figure 3) begins with categorizing the system as either an IS or as Platform IT (PIT). You must describe they system and register it with the appropriate component. In this case in would be with the AF and it would need to be registered in EITDR. Step 2 would be to identify the security controls that would be applicable to this particular IS or PIT. This is done by (in the case of the AF) the AF CIO and would occur during the process to make the determination that it is an IS or PIT. The component CIO has pre-identified a set of security controls (questions) which are applicable to the type of IS. Then the security controls are documented in the system security plan. Next is step 3 where we implement the security controls outlined in the security plan on the IS and answer those controls in the security plan. This can consist of many things to include altering system design (if early enough in development) to making system configuration changes in the system software. There are many types of controls from physical security controls (locks on doors) to software security design (using encryption). Step 4 is to develop a review methodology and to review the answers to the required security controls. Step 5 is authorizing the system which begins with building a Plan of Action and Milestones (POA&M) identifying any and all vulnerabilities identified when answering the security controls or during the validation step of the process. You also need to identify the steps needed to either remediate or mitigate all the known vulnerabilities listed on the POA&M. The system PM then assembles the package to be submitted to the Action Officer (AO) for adjudication and eventual approval of the IS to operate.

The AO can determine the system is granted an Authority to Operate (ATO), Grant it an Interim Authority To Test (IATT), or if the AO feels the risks to security in the POA&M are to great issue a Denial of Authority To Operate (DATO). Step 6 is the most valuable new step in the AFCAP and it is the monitor step. In this step the Information System Security Manager (ISSM) in concert with others must determine which security controls would cause the greatest security impact if not followed or if their operational state were to be modified. They must also continually monitor subsets of the controls to ensure continuous compliance. This is the real time monitoring part of the requirement. The ISSM is responsible to report any changes in security status to the AO and to make recommendations when necessary to rescind the ATO of any system not in compliance with its approval to operate.

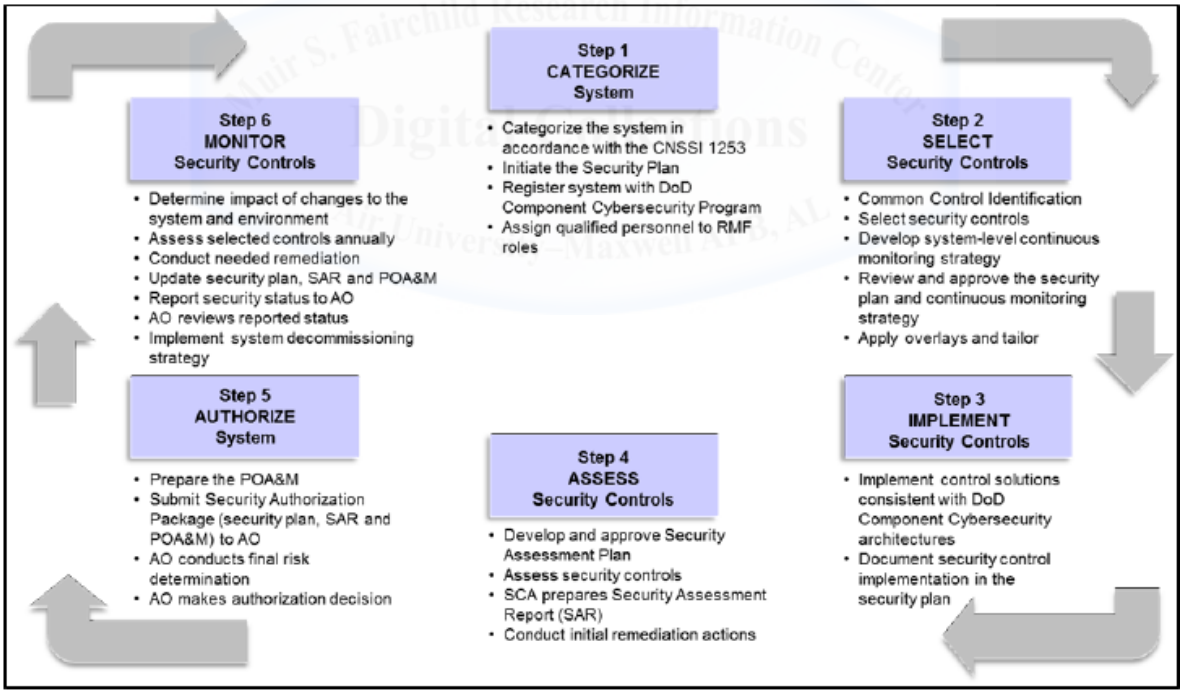


Figure 3 RMF Process[31]

Another methodology being pursued by the federal government is cloud computing. As of 2011, it was estimated that the federal government could migrate as much as 25% of IT spending to cloud computing.[32] (Figure 4) This methodology would allow the federal government to increase efficiency of both cyber operations and the implementation of IA for government data. Whether the clouding strategy is to the cloud in DoD or commercial facilities, the IA would be approved at the federal level, leaving little to no work for local IA practitioners as there would be no IT systems to C&A. Only the software being developed would need to be created with IA compliance in mind.

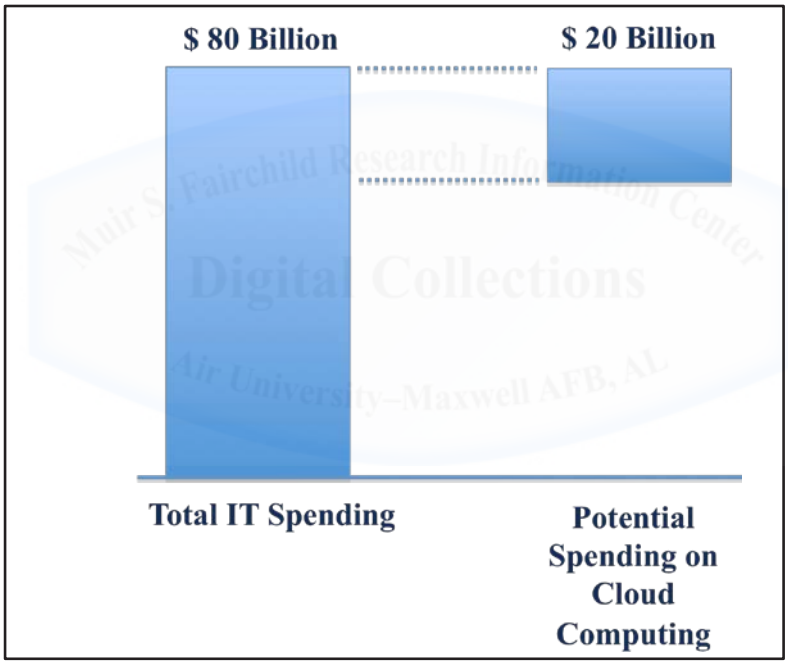


Figure 4 Estimated Portion of Federal IT Spending Able to Move to The Cloud[33]

Cloud computing provides a robust environment without the infrastructure costs currently associated with data storage and IT security. The costs of hardware, training, maintenance, etc. can be virtually eliminated through the adoption of a viable cloud computing strategy.

POSSIBLE SOLUTIONS

When evaluating possible solutions, it is important to consider all relevant options. Comparative analysis of all options is essential. A valid comparison must include all options, their effectiveness towards meeting stated goals, and any possible ramifications to each option's implementation. The high number of possible configurations, the complexities required, as well as the inter-relational dynamics of the IT systems and the supported systems being developed and operated necessitates that any recommendations be as dynamic as possible.

Option 1: Air Force Policy Changes

One possible course of action (COA) would be to write more specifics into the AFIs related to IA in information systems. This would have the benefit of providing detailed instructions and a level of clarity to the IA practitioner who is charged with completing the certification process to document the IA state of the IT system. It would also induce a greater amount of instructions, which would introduce a greater level of complexity. A higher level of complexity may induce confusion and a greater lack of clarity to the IA process. More specific guidance in AF instructions could induce rigidity to the process. A more ridged process could slow the acquisition process for information systems. A slower acquisition process of IT systems could have negative effects of the AF weapons systems they support. AF weapons system acquisition is a dynamic process inclusive of development and test. This process requires IT systems to support each phase of acquisition. A larger layer of more restrictive or specific AFIs could impede the current flexibility in the acquisition process.

Option 2: DoD and AF Methodology Changes

AF methodology takes most of its direction from public law and DoD instructions. The AFCAP outlined is AFI33-210 merely implements the requirements of FISMA and the various DoDI's, such as DoDI 8510.01. The AF is already in the process of implementing a methodology change; they are in the planning stages of moving from DIACAP to RMF. Another recent methodology change was for the AF to begin documenting its IA C&A process in the eMASS (DoD). Previously, the AF was documenting the process in EITDR (AF), which then routinely was used to update the DoD. The more the AF utilizes existing DoD systems and processes, the more clear the requirements are to IA practitioners working to instill IA in IT.

Any addition of AF methodology's may provide additional clarity for the requirements of RMF, but may also induce greater complexity to what is already a process which lacks efficiency according to many, such as Bellomo and Woody[34] in their analysis of the current DoD processes. Additional AF processes may provide support for IT systems supporting AF mission objectives but also at a cost in time, effort, and clarity.

Option 3: DoD and Air Force policy and Methodology Changes

A combination of what is reasonable and applicable from both options could itself prove to be a viable and effective option. If the DoD provided more streamlined and detailed guidance with supporting examples for IA practitioners to follow; and if the AF minimized its policy's, then the result may be a clearer and coherent single set of guidelines. This less confusing option would allow the AF IA practitioners to follow DoD guidance to meet the DoD requirements outlined in their instructions which is a more logical workflow since the IT system owners and

practitioners must also now document that compliance in EMASS, which is a DoD system. Since the AF no longer maintains its own C&A tracking system (formerly EITDR), minimizing AFIs to the greatest extent practicable would foster simplicity of processes.

The DoD could also add to the solution by further clarifying requirements for AF-specific systems in their DoD guidance, where needed. As the AF migrates to the joint environment and to the DoD cloud, AF level guidance will become less necessary to IT practitioners. The existing AF and DoD efforts to migrate IT systems to the cloud[35] is a good reason to begin migrating IA policy and possibly methodologies away from the Services and to the DoD. All this would be dependent on the DoD increasing the breadth of its policy to include mission-specific requirements of the individual Services not currently covered by existing DoD policy. Additionally, it would require the DoD to be more specific in its RMF methodology to be more instructive to the individual services.

Option 4: Cloud Computing to Eliminate Policy and Methodology Requirements

The DoD is making cloud computing an ever increasing priority when planning for the future. The DoD Chief Information Officer (CIO) Teresa M. Takai has made it clear in her 2012 strategy document, that the DoD was going to increasingly move towards cloud as a first option for computing and storage requirements for the DoD[36]. The AF and DoD are already in the process of approving cloud vendors to maintain government data. While some services may migrate more data faster than the AF, the process is already underway and the AF is signaling through cloud policy that it is moving in the direction of cloud for as much data as possible. This option seems to provide good promise as it eliminates the requirement to instill IA in IT systems at the local level and levy's them at the cloud data center level; no matter if the data center is

contractor or DoD owned. In the case of the contractor, all requirements can be articulated in the contract and DoD compliance requirements become the contractual obligation of the contractor. In the case of the DoD owned data center, the requirements become those of the DoD operator and not of the Air Force.

While there are many good reasons to consider more widespread use of cloud computing, the main reason lies in the many federal mandates such as the Federal Data Center Consolidation Initiative (FDCCI) which requires among other things (including the consolidation of data centers), the use of cloud computing.[37] Another mandate that bolsters the need for the FDCCI is the DoD's drive towards the Joint Information Environment (JIE). The JIE is the DoD's response to the needs of the warfighter. The DoD's JIE strategy acknowledges capability gaps in warfighter support and puts forth the process to consolidate and optimize data services with the specific intent of improving support to the warfighter.[38]

Option 4: Application Rationalization

Like the IT system consolidation involved in cloud computing, the DoD is also pursuing an application rationalization or consolidation strategy. This is a DoD strategy to implement efficiencies and cost reductions through the elimination of redundant IT applications.[39] This strategy involves the requirement to stop IT system or application development until the owner has completed multiple levels of analysis to include evaluating all possible options through an Analysis of Alternatives (AoA), business case analysis, architectural (IA) analysis, etc. This process is linked to FDCCI and is often an integral part of implementing FDCCI in the DoD and the AF. The DoD considers the consolidation of applications an integral part of its cloud computing strategy.[40]

CONCLUSION

A combination of the listed options is the most optimal path to the best IA possible in government IT. The best tool to ensure the successful implementation and maintenance of IA in government owned IT systems is clarity. As the joint and cloud environment is expanding its control of all things cyber, perhaps it is time for the DoD to take a more authoritative stance on the control of the IA of all DoD cyber systems. Within its own pages, AFI33-210, the AFCAP, points out that one of its main purposes is to standardize the way the AF meets DoD requirements; and those requirements are the requirements of DODI 8500.01, 8510.01, and others. So, why not just direct AF IT system owners to DODI 8500.01 and 8510.01 to meet those requirements. The extra layer of instruction provides some benefit to the IT system owner wishing to secure their system, but not enough to warrant the added layer of burocracy to a specific process almost wholly managed by the DoD. A policy memo, or at the most, a much more specific AFI outlining areas of responsibility within the AF would be more productive and less confusing to the IT owners who must complete the DOD RMF process.

Consolidation of IT systems through data center consolidation along with application rationalization would reduce the scope of the IT systems requiring governance and oversight. Along with implementing FDCCI, additional application rationalization can further reduce the scope of the IA and management burden. Policy and process modification would be a next step, followed by the AF and DoD migrating more and more IT systems to cloud environments managed by DoD. Long-term Cloud environments managed by DoD would be the most optimal solution as it would also allow the AF to put more effort into mission and weapon system

requirements and maintain a much smaller IA workforce than it currently is forced to maintain due to the public law requirements of FISMA. Adding to that a minimization of AF policy in favor of more comprehensive DoD policy to cover those IT systems not able to be migrated to the cloud provides a more complete solution to IA of AF IT.

RECOMMENDATION

Making a recommendation for action for such a complex set of issues as IT system compliance with laws and policy's, especially those concerning the implementation of IA requirements is difficult. It is not as simple as recommending that a single policy or law be modified or eliminated. In this case the best answer is to implement a balanced approach which spreads changes across the spectrum of policy's, laws, standards, and practices utilized to guide and implement IA in IT systems throughout the AF. My recommendations are:

The DoD should continually evaluate the implementation of its JIE strategy to see if it can be accelerated or in some other way optimized. The core of the JIE is the adaptation of a single architecture and single network for the joint environment to support the warfighter. The warfighter should be the focus of all DoD efforts with regard to IT system development and maintenance. The focus on a single network aids the DoD and AF in simplifying the processes and policy's required to ensure IT system security.

The AF should continue to pursue the cloud computing strategy put forth by the DoD to reduce to the greatest extent possible, the number of AF IT systems. This is not only a viable IA strategy, but should induce better IA compliance through process simplicity and IT efficiency.

The AF should also accelerate its application consolidation through its pursuit of data center consolidation as mandated by the FDCCI. As is the case with cloud computing, data center consolidation eliminates redundant data centers and applications the AF is currently required to maintain. These reductions eliminates IT systems and applications requiring the implementation of IA to secure those systems and the government data which they contain. The reduction in AF data centers will reduce the number of trained professionals required to develop, deploy, and maintain AF IT systems and applications, as well as the number and complexity of AF and DoD instructions required to maintain the process.

The DoD and the services should produce joint or overarching policies to cover IA implementation in IT systems. The AF should reduce to the greatest extent possible its policy footprint as the DoD revises its policy to be more inclusive of the services unique requirements (including those of the AF).

The DoD and AF should share methodologies for the implantation of IA. To the greatest extent practicable the DoD should implement more detailed guidance (where required) in order to satisfy the guidance requirements of the services. This would allow the AF (as well as the other services) to rescind their service specific methodology guidance such as AFI 33-210, the AF Certification and Accreditation Program (AFCAP) in favor of DoD guidance such as that instituting RMF.

Policy and guidance from a higher level, utilized by all the services, would eliminate redundant publications; making the whole process simpler, more efficient to operate, and simpler to maintain. In addition, the services could benefit from the implementation of a more common operating environment through the sharing of resources such as IA practitioners working to accredit systems, IA practitioner training, approving authorities, etc.

To more easily adapt a streamlined stance with regard to policy and guidance, the DoD and AF should accelerate to the greatest extent practical, the adoption of the JIE, cloud computing, and application rationalization. A reduction in the number of IT systems and applications, along with the implementation and enforcement of a single architecture will provide for an easier path to reduce the amount and complexity of current policy and guidance. The requirements of public law be best served by consolidating IT systems, data centers, and applications to reduce the burden on the remaining IA workforce. Streamlining the current policy footprint of the AF and DoD to eliminate unnecessary and redundant guidance will best serve the needs of the IT system owners and IA practitioners. Consolidation and simplification utilizing all methods available is the best solution to ensuring the security of AF IT systems, applications, and data in the most efficient way possible.

Notes

[1] Gen Keith B. Alexander, "Hearing on National Defense Authorization Act for Fiscal Year 2012," Committee on Armed Services, US House of Representatives, H.A.S.C. No. 112–26, March 16, 2011, p.4

[2] John T. Ackerman, Matthew C. Stafford, and Thomas Williams, "Six Research Frameworks" (2010); RE106, Instructional Narrative, August 2015, page 5

[3] Stephany Bellomo, Carol Woody, DoD Information Assurance and Agile: Challenges and Recommendations Gathered Through Interviews with Agile Program Managers and DoD Accreditation Reviewers, November 2012, Page 19: http://www.sei.cmu.edu/reports/12tn024.pdf

[4] Peter Williams, Tiffani Steward, DoD's Information Assurance Certification & Accreditation Process, Information Security, Defense AT&L, September-October 2007, page 13: http://www.dau.mil/pubscats/PubsCats/atl/2004_01_02/williams_so07.pdf

[5] GAO Highlights, Highlights of GAO-15-714, Federal Information Security, Agencies Need to Correct Weaknesses and Fully Implement Security Programs, September 2015: http://www.gao.gov/assets/680/672802.pdf

[6] Ibid

[7] Peter Williams, Tiffani Steward, DoD's Information Assurance Certification & Accreditation Process, Information Security, Defense AT&L, September-October 2007, page 13: http://www.dau.mil/pubscats/PubsCats/atl/2004_01_02/williams_so07.pdf

[8] Lt. Col Karen Burke, Defense Intelligence Agency, DoD Certification and Accreditation C&A Process, 9 September 1998, From CISR Video Library, security lectures: https://www.youtube.com/watch?v=6ch5oVzc-Jg

[9] Stephany Bellomo, Carol Woody, DoD Information Assurance and Agile: Challenges and Recommendations Gathered Through Interviews with Agile Program Managers and DoD Accreditation Reviewers, November 2012, Page 19: http://www.sei.cmu.edu/reports/12tn024.pdf

[10] Ibid, page 22

[11] Air Force Instruction 33-210, Air Force Certification and Accreditation (C&A) Program (AFCAP); 31 August 2015, page 2

[12] Public Law (PL) 107-347, the 107th Congress of the United States, 17 December 2002: https://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf

Notes

[13] Ibid

[14] OMB Circular A-130, Appendix III, Transmittal Memorandum No. 4, Security of Federal Information Resources, Requirements, 28 November 2000: https://www.whitehouse.gov/omb/circulars_a130_a130appendix_iii

[15] Ibid

[16] Ibid

[17] National Institute of Standards and Technology (NIST) Special Publication 800-37 Revision 1, "Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems," Chapter 1, page 1; February 2010

[18] DoDI 8500.01, Risk Management Framework (RMF) for DoD Information Technology (IT), DoD CIO, 12 March 2014, page 1: http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf

[19] DoDI 8510.01, Cybersecurity, DoD CIO, 12 March 2014, page 1: http://www.dtic.mil/whs/directives/corres/pdf/851001_2014.pdf

[20]AFPD33-2, Information Assurance (IA) Program, 3 August 2011: http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afpd33-2/afpd33-2.pdf

[21] AFI33-210, Air Force Certification and Accreditation Program (AFCAP), October 2014: http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi33-210/afi33-210.pdf

[22] The Department of Defense Strategy for Implementing the Joint Information Environment, 18 Sept 2013; page 1: http://dodcio.defense.gov/Portals/0/Documents/JIE/2013-09-13_DoD_Strategy_for_Implmenting_JIE_(NDAA_931)_Final_Document.pdf

[23] Ibid, page 7

[24] The Department of Defense Strategy for Implementing the Joint Information Environment, 18 Sept 2013; page 8: http://dodcio.defense.gov/Portals/0/Documents/JIE/2013-09-13_DoD_Strategy_for_Implmenting_JIE_(NDAA_931)_Final_Document.pdf

[25] Peter Williams, Tiffani Steward, DoD's Information Assurance Certification & Accreditation Process, Information Security, Defense AT&L, September-October 2007, page 13: http://www.dau.mil/pubscats/PubsCats/atl/2004_01_02/williams_so07.pdf

Notes

[26] Stephany Bellomo, Carol Woody, DoD Information Assurance and Agile: Challenges and Recommendations Gathered Through Interviews with Agile Program Managers and DoD Accreditation Reviewers, November 2012, Page 5: http://www.sei.cmu.edu/reports/12tn024.pdf

[27] Ibid, page 16

[28] Peter Williams, Tiffani Steward, DoD's Information Assurance Certification & Accreditation Process, Information Security, Defense AT&L, September-October 2007, page 13: http://www.dau.mil/pubscats/PubsCats/atl/2004_01_02/williams_so07.pdf

[29] Stephany Bellomo, Carol Woody, DoD Information Assurance and Agile: Challenges and Recommendations Gathered Through Interviews with Agile Program Managers and DoD Accreditation Reviewers, November 2012, Page 5: http://www.sei.cmu.edu/reports/12tn024.pdf

[30] AFI33-141, Air Force Information Technology Portfolio Management and IT Investment Review, 23 December 2008: http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi33-141/afi33-141.pdf

[31] DoDI 8510.01, Cybersecurity, DoD CIO, 12 March 2014, page 28: http://www.dtic.mil/whs/directives/corres/pdf/851001_2014.pdf

[32] Vivek Kundra, U.S. Chief Information Officer, Federal Cloud Computing Strategy, 8 February 2011: http://acmait.com/pdf/Federal-Cloud-Computing-Strategy.pdf

[33] Ibid

[34] Stephany Bellomo, Carol Woody, DoD Information Assurance and Agile: Challenges and Recommendations Gathered Through Interviews with Agile Program Managers and DoD Accreditation Reviewers, November 2012, Page 5: http://www.sei.cmu.edu/reports/12tn024.pdf

[35] Teresa M. Takai, Chief Information Officer, Department of Defense, Cloud Computing Strategy, July 2012, Page Memorandum: http://dodcio.defense.gov/Portals/0/Documents/Cloud/DoD%20Cloud%20Computing%20Strategy%20Final%20with%20Memo%20-%20July%205%202012.pdf

[36] Ibid

[37] Federal Data Center Consolidation Initiative, Department of Defense 2011 Data Center Consolidation Plan & Consolidation Report, 8 Nov 2011: http://dodcio.defense.gov/Portals/0/Documents/FDCCI-Final-2011.pdf

Notes

[38] The Department of Defense Strategy for Implementing the Joint Information Environment, 18 Sept 2013; page 3: http://dodcio.defense.gov/Portals/0/Documents/JIE/2013-09-13_DoD_Strategy_for_Implmenting_JIE_(NDAA_931)_Final_Document.pdf

[39] Ibid, page 8

[40] Teresa M. Takai, Chief Information Officer, Department of Defense, Cloud Computing Strategy, July 2012, Page E-3: http://dodcio.defense.gov/Portals/0/Documents/Cloud/DoD%20Cloud%20Computing%20Strategy%20Final%20with%20Memo%20-%20July%205%202012.pdf

BIBLIOGRAPHY

Alexander, Keith B. “Hearing on National Defense Authorization Act for Fiscal Year 2012,” Committee on Armed Services, US House of Representatives, H.A.S.C. No. 112–26, March 16, 2011Air Force Instruction 33-210, Air Force Certification and Accreditation (C&A) Program (AFCAP); 23 December 2008, change 1 incorporated 2 October 2014

Department of Defense Chief Information Officer, Federal Data Center Consolidation Initiative, Department of Defense 2011 Data Center Consolidation Plan & Consolidation Report, 8 Nov 2011: http://dodcio.defense.gov/Portals/0/Documents/FDCCI-Final-2011.pdf

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

DoD, The Department of Defense Strategy for Implementing the Joint Information Environment, 18 Sept 2013: http://dodcio.defense.gov/Portals/0/Documents/JIE/2013-09-13_DoD_Strategy_for_Implmenting_JIE_(NDAA_931)_Final_Document.pdf

GAO Highlights, Highlights of GAO-15-714, Federal Information Security, Agencies Need to Correct Weaknesses and Fully Implement Security Programs, September 2015: http://www.gao.gov/assets/680/672802.pdf

John T. Ackerman, Matthew C. Stafford, and Thomas Williams, “Six Research Frameworks” (2010); RE106, Instructional Narrative, August 2015

Kundra, Vivek, U.S. Chief Information Officer, Federal Cloud Computing Strategy, 8 February 2011: http://acmait.com/pdf/Federal-Cloud-Computing-Strategy.pdf

Lt. Col Karen Burke, Defense Intelligence Agency, DoD Certification and Accreditation C&A Process, 9 September 1998, From CISR Video Library, security lectures: https://www.youtube.com/watch?v=6ch5oVzc-Jg

National Institute of Standards and Technology (NIST) Special Publication 800-37 Revision 1, “Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems,” Chapter 1, page 1; February 2010

OMB Circular A-130, Appendix III, Transmittal Memorandum No. 4, Security of Federal Information Resources, Requirements, 28 November 2000

OMB Circular A-130, Appendix III, Transmittal Memorandum No. 4, Security of Federal Information Resources, Requirements, 28 November 2000: https://www.whitehouse.gov/omb/circulars_a130_a130appendix_iii

Peter Williams and Tiffany Stewart, Defense AT&L magazine, volume 36, number 5, “DoD’s Information Assurance Certification & Accreditation Process”; September-October 2007

Secretary of Defense, Department of Defense Instruction 8500.01, Risk Management Framework (RMF) for DoD Information Technology (IT), DoD CIO, 12 March 2014: http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf

Secretary of Defense, Department of Defense Instruction 8510.01, Cybersecurity, DoD CIO, 12 March 2014: http://www.dtic.mil/whs/directives/corres/pdf/851001_2014.pdf

Secretary of the Air Force, 33-210, Air Force Certification and Accreditation (C&A) Program (AFCAP); 31 August 2015

Secretary of the Air Force, Air Force Instruction 33-141, Air Force Information Technology Portfolio Management and IT Investment Review, 23 December 2008: http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi33-141/afi33-141.pdf

Secretary of the Air Force, Air Force Instruction 33-210, Air Force Certification and Accreditation Program (AFCAP), October 2014: http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi33-210/afi33-210.pdf

Secretary of the Air Force, Air Force Policy Directive 33-2, Information Assurance (IA) Program, 3 August 2011: http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afpd33-2/afpd33-2.pdf

Stephany Bellomo, Carol Woody, DoD Information Assurance and Agile: Challenges and Recommendations Gathered Through Interviews with Agile Program Managers and DoD Accreditation Reviewers, November 2012: http://www.sei.cmu.edu/reports/12tn024.pdf

Takai, Teresa M., Chief Information Officer, Department of Defense, Cloud Computing Strategy, July 2012: http://dodcio.defense.gov/Portals/0/Documents/Cloud/DoD%20Cloud%20Computing%20Strategy%20Final%20with%20Memo%20-%20July%205%202012.pdf

The Federal Information Security Management Act (FISMA), Chapter 35 of Title 44, United States Code (U.S.C.); 2002

Tucker, Patrick, "For Years, the Pentagon Hooked Everything To The Internet. Now It's a 'Big, Big Problem", Defense One, 29 September 2015: http://www.defenseone.com/technology/2015/09/years-pentagon-hooked-everything-internet-now-its-big-big-problem/122402/?oref=d-dontmiss

US Congress, Public Law (PL) 107-347, the 107th Congress of the United States, 17 December 2002: https://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf

Wilshusen, Gregory, "Federal Information Security: Agencies Need to Correct Weaknesses and Fully Implement Security Programs: GAO-15-714"; Highlights of GAO-15-714, a report to congressional committees, 29 Sept 2015 Air Force Instruction

Wilshusen, Gregory, "Information Security: Despite Reported Progress, Federal Agencies Need to Address Persistent Weaknesses: GAO-07-837"; Highlights of GAO-07-837, a report to congressional committees, 27 July 2007