Research Paper Comparison of NIST SP 800-37 to ICD 503 (DCID 6/3)

For: Raymond J. Curts, PhD

George Mason University

Federal IT Security Policy
ISA 650 001, Spring 2013

April 25, 2013

Authors:
Dabir, Shashi
Kim, Myong Suk
Li, Ruoxi
Shah, Usman
Singh, Harmeet
Stayrook, David

Table of Contents

Abstract iii

Introduction 4

Documents Overview 5

Comparison and Analysis 9

DCID 6/3 Vs ICD 503 Vs NIST 800-37 9

Administration 14

Conclusions 17

Recommendation 19

Example 21

Appendix A 22

Bibliography 24

Abstract

Federal government agencies have published many guidelines and policies for information security in the past several years. This report selects two documents, National Institute of Standards and Technology (NIST) SP 800-37 and ICD 503 (DCID 6/3), for comparison and analysis. The goal is to determine whether one of the documents is better than the other. This has been done by examining three documents in detail, such as identifying their origins and the approaches they employ. The report concludes that the two documents are not directly comparable. Moreover, the authors propose a new scheme for the federal government, which may help them achieve better information assurance result.

Introduction

This document is based on a comparison of NIST SP 800-37 and ICD 503, which are Certification and Accreditation (C&A) related documents prepared for, and by, the U. S. Federal government. This document argues that NIST SP 800-37, published in Feb. 2010, is absolutely the more detailed and comprehensive document in relation to ICD 503, published in Sept. 2008. However, SP 800-37 is a guideline and ICD 503 is a higher level policy document. The authors will show that these documents are not directly relatable. It will demonstrated that NIST SP 800-37 is rooted in nearly all previous Federal C&A documentation with little reference to ICD 503 but does have some direct comparison with ICD 503's predecessor the DCID 6/3 manual.

NIST SP 800-37 is the current culmination of risk management security guidelines -- something that the U. S. Government has never had. Our document intimates that it is in the nature of the U. S. Government to work continually to provide new mandates and new authority to improve upon and permit change. It surmises how NIST SP 800-37 being a direct result of the Joint Task Force Transformation Initiative Working Group is the unification of the best elements of all previous C&A approaches. It will be shown that SP 800-37 will become the common baseline for Executive Branch agencies, including National Security Systems (NSS). It will show that NCSC-TG-031 Version 1, DoD Information Technology Security Certification and Accreditation Process (DITSCAP) (July 1996), DCID 6/3 (May 2000), and DoD Information Assurance Certification and Accreditation Process (DIACAP) (Nov. 2007) are clearly NIST SP 800-37 building blocks. Our document will show that Federal IT C&A has been slowly incorporating and

building on the common theme of system lifecycle strategies. In addition this document will conclude with a recommendation that is a new, innovative approach to achieving Information Assurance (IA).

Documents Overview

There is significant overlap in the purpose and content of C&A documentation between agencies of the U.S. Federal Government. IT security governance is a relatively new field, only two to three decades old, continually evolving over that time period and in short supply of skilled practitioners all the while. It is not impossible to imagine that a significant number of systems and software developers have obtained security credentials throughout the intervening years and contributed to the body of IA knowledge. It is possible that their most significant contribution has been the life-cycle view of C&A. Federal IT C&A has been slowly incorporating and building on the lifecycle strategies of systems and software development. One can see lifecycle concepts entering into the Department of Defense (DoD) C&A literature as early as July 1996 when the National Security Agency's (NSA) National Computer Security Center (NCSC), part of DoD, produced NCSC-TG-031 Version 1 "Certification and Accreditation Process Handbook for Certifiers." While they never arrived at the circular diagrammatic representation present in DIACAP and NIST SP 800-37, there are 48 life-cycle references in the document. NCSC-TG-031 Version 1 is an eight phase approach that isn't directly relatable to the life-cycle steps of SP 800-37 however there are some similarities. For example, in a broad sense Post Accreditation Activity 8 of NCSC-TG-031 Version 1 Maintain Accreditation is relatable to SP 800-37 Step 6 Monitor Security Controls. In

Activity 8 it states, “Accreditation maintenance involves ensuring that the system continues to operate within the stated parameters of the accreditation.” (National Security Agency xxxii) This is precisely the intent of SP 800-37 Step 6-6 where it states “Review the reported security status of the information system (including the effectiveness of security controls employed within and inherited by the system) on an ongoing basis in accordance with the monitoring strategy to determine whether the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation remains acceptable.” (National Institutes of Standards and Technology 41)

In DITSCAP there are 14 references to “life cycle.” It is also a phased approach, like NCSC-TG-031 Version 1, with no life cycle diagram. DITSCAP has four phases. Again the last phase in its life cycle, Phase IV Post Accreditation is slightly relatable to SP 800-37, Step 6-6 again (see above). “Phase IV contains activities necessary to operate and manage the system so that it will maintain an acceptable level of residual risk. Post-accreditation activities include; ongoing maintenance of the SSAA, system operations, change management, and compliance validation.”

However, neither NCSC-TG-031 Version 1 nor DITSCAP took the next step to connect the beginning and end of system life diagrammatically to suggest that when equipment or systems are end-of-life that there can be a replacement device or system for which some of the original controls will be applicable and new controls must be established.

DIACAP references the term life cycle 14 times in its text. It takes the next step and presents a life-cycle diagram (Department of Defense 13) where Activity 5, Decommission, and Activity 1, Initiate and Plan are connected and suggests that systems

are continually re-evaluated and re-assessed so that a new system is born from an old system, or a new device replaces an old device, and the controls in place can be assessed towards their re-use and new controls put in place as the new system moves forward in the life cycle.

NIST SP 800-37 bills itself as a “Security Life Cycle Approach”. (National Institutes of Standards and Technology Title Page) There are 65 references to the term life cycle in the text of SP 800-37 not counting the numerous times it shows up in title and header sections on each page. NIST has numerous other documents that relate to and/or complement SP 800-37. For example, the selection of security controls. Step 2 in SP 800-37 is titled Security Control Allocation. This section of SP 800-37 references NIST SP 800-53 “Recommended Security Controls for Federal Information Systems and Organizations.” Others that relate to or can be seen as complementary of SP 800-37 are NIST SP 800-30 “Guide for Conducting Risk Assessment” and SP 800-39 “Managing Information Security Risk: Organization, Mission, and Information System View.” These are the most relatable documents to the C&A process in the NIST library of security documentation, however, 800 series special publications are currently the most prolific and detailed of all the security documents produced by the U. S. Federal Government. These NIST documents are likely to be the source documents adapted to all other new and relevant agency specific C&A documentation; paraphrased, directly referenced, and most likely studied by every agency C&A document writer and C&A leadership to be competent in their respective roles.

The efforts of the Joint Task Force Transformation Initiative Working Group, chaired by NIST, are becoming apparent. While “federal agencies are required to follow certain specific NIST Special Publications in accordance with OMB policy, there is flexibility in how agencies apply the guidance.” (National Institutes of Standards and Technology IV) Similarly, the Committee on National Security Systems (CNSS) policy document CNSSP 22 “Information Assurance Risk Management for National Security Systems” refers often to NIST SP 800-37 and 800-39. “The CNSS intends to adopt National Institute of Standards and Technology (NIST) issuances where applicable. Additional CNSS issuances will occur only when the needs of NSS are not sufficiently addressed in a NIST document.” (Takai, Teresa M. "Foreward") And now there is a smattering of information being produced regarding DIARMF, the Defense Information Assurance Risk Management Framework, for which early information suggests SP 800-37’s six-step life-cycle is at its core while DoD exercises its legal rights to build upon NIST’s work. (Marzigliano) This will likely happen across the board as every agency both utilizes, and adapts, the NIST framework.

It can be argued that the end result of each agency adapting the NIST special publications as their core documentation will be a more controlled government wide C&A development arena. Whereby under the auspices of NIST and FISMA extreme measures should get reigned back in as appropriate but this should also leave the door open for improvements and enhancements in the NIST body of work. Hopefully, a program that reviews the successes and failures of their special publications as a government wide baseline for C&A practice will be put in place: A follow-on Joint Task Force, where on a more frequent basis respective changes can be made to the NIST baseline documents. At

a much higher level, this constitutes a system, or "framework," of establishing and maintaining best practices: A life-cycle of C&A Risk Management Framework renewal that does not assume that one government agency has all the answers regarding C&A best practice.

Comparison and Analysis

DCID 6/3 Vs ICD 503 Vs NIST 800-37

DCID 6/3 provides uniform policy guidance and requirements for ensuring adequate protection of certain categories of intelligence information, Sensitive Compartmented Information and special access programs for intelligence under the purview of the DCI (Intelligence, Director Central). DCID 6/3's treatment of "information assurance" is more aggressive than the other C&A documents referenced in this report.

DCID 6/3's way to accredit an Information System (IS) is to use Levels-of-Concern, Protection Levels, Interconnected System Requirements and Administrative Requirements such as training, document marking, physical security, personnel security. It also identifies Technical Security and Assurance Requirements (determine what controls apply) and determines required Documentation and Testing Activities [this is a function of the required controls}

It also provides guidance to write the System Security Plan, Validate Security in Place, Test against Security Requirements, Prepare Certification Package, and Forward

Certfication Package to the DAA and Accreditation decision by DAA, DCID 6/3 is cast in the mold of SDLC phase.

ICD 503 establishes a policy for conducting certification and accreditation in the Intelligence Community (IC). This document is more of a "holistic and strategic" process "through the use of common standards and reciprocally accepted certification and accreditation decisions". This document provides a high level overview of how C&A is to be conducted, and does not provide details of how C&A is to be conducted on the same lines as NIST 800-37.

The ICD 503 addresses only the IC elements and is solely meant for IC elements And counterintelligence concerns whereas NIST 800-37 does not address any counterintelligence concerns. ICD 503 uses the terms "management, operational, and technical security controls" which are adapted from NIST 800-37, whereas DCID 6/3 has its own set of security controls, based on Protection Levels and Levels of Concern.

ICD 503 accepts "Accreditations granted by the Commonwealth/5-Eyes Partners (Australia, Canada, New Zealand, United Kingdom) for their respective sovereign information technology systems or items of information technology that store, process, and or communicate national intelligence information provided by the U.S. Government", whereas NIST 800-37 does not address international accreditations.

The NIST 800-37 framework consists of security categorization, security control

selection and implementation, security control assessment, information system authorization and security control monitoring. IA implementation and authorization activities are integrated into a System Development Life Cycle and enables performance of a continuous monitoring process on operational systems. It continuously tracks changes to the information system that effect security controls and reassess control effectiveness. NIST 800-37 is solely to manage the Risk Management Framework of Federal Civilian Agencies, whereas DCID 6/3/ICD503 is for IC elements.

NIST in partnership with the DoD, the Office of the Director of National Intelligence (ODNI), and the Committee on National Security Systems (CNSS), has developed a common information security framework for the federal government and its contractors. NIST 800-37 categorizes a three-tiered approach to risk management that addresses risk-related concerns at: (i) the *organization* level; (ii) the *mission and business process* level; and (iii) the *information system* level, whereas DCID 6/3/ICD 503 does not have a tiered approach. NIST document addresses in particular, net-centric architectures (e.g., service-oriented architectures [SOAs], cloud computing) and introduces two important concepts: (i) *dynamic subsystems*; and (ii) *external subsystems*, whereas DCID 6/3/ICD 503 do not mention as such.

	DCID 6/3	ICD503	NIST 800-37
Process	11 steps	Steps, Process, Phases unclear	4 phases with 10 tasks and 31 subtasks
Systems Classification	5 “Protection Levels”	No protection level or categories	12 categories from FIPS 199
Measurement Standard	80 “security features and assurances,” organized into 36 areas	None	Controls from NIST 800-53
Other Characteristics	Static Procedural Activity SCI/SAP programs, Aggressive Information Assurance	Holistic and strategic process, common standards, reciprocally accepted certification and accreditation decisions	Dynamic, near real-time risk management Unclassified environment
Security Controls	Security Controls based on Protection Levels and Levels of Concern	Management, Operational and Technical Controls	Management, Operational and Technical Controls

	DCID 6/3	ICD503	NIST 800-37
RMF	None	None	Tiered Risk Mgt Framework(Org, Mission and Business Process Level, Information Systems Level
Net-Centric Architecture	No mention of net-centric architectures(SOA, Cloud computing)	No mention of net-centric architectures	Addresses net-centric architectures[39] (e.g., service-oriented architectures [SOAs], cloud computing) and introduces two concepts: (i) *dynamic subsystems*; and (ii) *external subsystems*
Counterintelligence Concerns	No counterintelligence concerns	Addresses counterintelligence concerns	No counterintelligence concerns

Administration

SP 800-37 is the more comprehensive document in relation to ICD 503. The immediate conclusion is that ICD 503, being briefer and less detailed, would be the easier document to implement but that is likely to be an incorrect conclusion. As mentioned earlier, SP 800-37 is a guidelines document and ICD 503 is a policy document. ICD 503 is a policy document without its associated guideline document, or manual, as in the case of its predecessor DCID 6/3. ICD 503 rescinded the DCID 6/3 manual, possibly in anticipation of producing its own manual, but none of that can be ascertained from available documentation.

If a proper security organization has policies, procedures, standards, and guidelines, then NIST is heavy in the standards and guidelines area. SP 800-37, a guideline, allows for a system, potentially different in every case, to define the security controls that will be applied. ICD 503, a policy document, talks at length about the responsibilities of the Authorizing Official, or the Delegated Authorizing Official but provides little, if any, guidance relative to the how-to of C&A.

By comparison, ICD 503 is the much briefer document. However, if ICD 503 intends for the IC security practitioner to utilize rescinded document DCID 6/3 until a new manual/guideline is available it never makes that statement. DCID 6/3 states in at least three different sections of the document that “Information technology risk management standards published, issued, and promulgated for the IC by the IC CIO may include standards, policies, and guidelines approved by either or both NIST or CNSS.” (Intelligence 2, 6) Within ICD 503 there is no other section directing the reader to what specific standards, policies, and guidelines are to be used or where they may be found. Maybe this is intentional by the IC.

To further differentiate the two documents administratively, in Section 2 of SP 800-37, 15 pages are devoted to educating the reader in the "The Fundamentals of Managing Information System-Related Security Risks, i.e., the RMF (Risk Management Framework) and the Development Life Cycle. This is excellent background information and reviews the prevailing security concepts of our time. Also, Chapter 3 of SP 800-37, the six step lifecycle process, is a very effective, well written process with no rivals in Federal C&A literature. It is both general and specific, pulling in other NIST special publications to support the six step lifecycle. All questions are answered: Why does it exist, what are its references, etc. The tasks defined within each step are individual goals to be satisfied in the C&A process. Each of the six steps builds into the next and culminates in the long term monitoring and re-assessment of the system.

Where there could be commonality between the documents, ICD 503 comes up short. In SP 800-37, NIST devotes an entire appendix, approximately 1 and 1/4 pages to the listing of 1) Legislation, 2) Policies, Directives, Instructions, 3) Standards, and 4) Guidelines whereby the IC, in ICD 503, only makes the repeated statement discussed above regarding "standards published, issued, and promulgated for the IC by the IC CIO" and only provides a brief paragraph in Section A regarding the Authority for creating the document. Also, SP 800-37's other appendix's are very detailed. There is an appendix describing thirteen different roles and responsibilities in the Risk Management Framework (RMF) and Development Life Cycle hierarchy whereby everything regarding personnel and systems in ICD 503 is referred to as the IC element above which the Authorizing Official or Delegated Authorizing Official conduct the certification and accreditation.

From an administrative perspective, the IC's previous C&A document, the DCID 6/3 Manual, is more comparable to NIST SP 800-37. However, it is the author's opinion that SP 800-37 is the

better structured document and easier to read relative to the DCID 6/3 Manual. The DCID 6/3 Manual does not contain a single appendix. It's difficult to imagine that so much information could be covered in the text alone without any explanatory sections at the end to help bring it all together. Overall, SP 800-37's structure, readability, information flow, and relevance to current security practices lend support to the idea of it being the easier document to administer.

DCID 6/3 seems to be a very effective, in depth, step-by-step C&A process. Relative to SP 800-37 it is a very differently structured document. However, it did employ a lifecycle approach and definitely contributed to the lifecycle concepts incorporated in SP 800-37. If SP 800-37 moves through steps 1 through 4 and then over the life time of the system goes back and forth between the monitoring of security controls and the C&A process, evaluating and re-evaluating security controls, assessing and re-assessing the security posture of the system, then DCID 6/3 insinuates the same process in Section 9, Part B, Step 1 whereby it states "Risk management is relevant to the entire life cycle of an IS. During IS development, security countermeasures are chosen. During IS implementation and operation, the effectiveness of in-place countermeasures is reconfirmed, and the effect of current threat conditions on system security is assessed to determine if additional countermeasures are needed to sustain the accredited IS's security. In scheduling risk management activities and designating resources, careful consideration should be given to Certification and Accreditation (C&A) goals and milestones. Associated risks can then be assessed and corrective action taken for unacceptable risks. Risk management requires the routine tracking and evaluation of the security state of an IS." (Director of Central Intelligence 9-1)

Conclusions

Agencies of the Federal Executive Branch have developed their own policy and guidance for information security and C&A in the last two decades. These documents have had common elements. The life-cycle theme has been a common thread that has gone through a number of iterations culminating in SP 800-37.

According to this research, NIST SP 800-37 and ICD 503 are two different types of documents and do not lend themselves to direct comparison with one another. However, it is not beyond the realm of possibilities that SP 800-37 could now become the guideline document. In addition, the IC has not produced guidance for ICD 503. The need for both documents is apparent if there are still to be both policy and guideline documents.

For example, ICD 503 applies to the National Reconnaissance Office (NRO) since it is a part of the IC. On the other hand, NRO as a part of DoD must comply with FISMA. NRO is a typical example of an organization that has to satisfy multiple compliances. NRO CIO Annual Report 2010 shows that NRO must produce documents to satisfy CNSS Policy 22, ICD 503 and NIST 800-37 (Singer). The likely future is that all elements of the IC will need to be compliant with both ICD 503 and NIST documentation.

NIST SP 800-37 and several other NIST SPs are the direct result of the Joint Task Force Transformation Initiative (JTFTI) Working Group which is the common link to all preceding documentation. This joint effort was staffed by senior leadership from defense, intelligence, and civilian agencies: DoD, ODNI, CNSS, and NIST (Grimes). These participating agencies established common guidance for information systems security for national security and non-national security systems pulling in elements of individual C&A efforts.

CNSS has authorized the use of SP 800-37 with possible modifications for application to national security systems. What is unclear is how SP 800-37 will be applicable to both national and non-national security systems. Differences remain between guidance for national security and non-national security systems in areas such as system categorization, selection of security controls, and program management controls (Government Accountability Office).

According to officials, implementing the harmonized guidance could take several years to complete due to both the large number and criticality of the systems that must be reauthorized under the new guidance (Welke). DoD and IC are developing agency-specific guidance and transition plans for implementing the harmonized guidance. Agencies made progress in harmonizing information security policies for national security and non-national security systems. However, much more work remains to ensure continued progress (Government Accountability Office).

Recommendation

Several C&A approaches were studied as part of this comparison analysis. This Point-based, system-oriented scheme is discovered as a new approach. It is innovative and well thought out approach but it is lacking details. In-depth discussion is included in this section.

The major issues in federal IT policies are incompatibility and overlapping. One possible solution is to develop a point-based, system-oriented scheme. It functions in the following way.

1. Categorize IT systems within the federal government according to their information security classification, namely top secret, secret, classified, unclassified and controlled unclassified information. The six basic system categories (i.e. top secret systems, secret systems and etc.) are abstract concepts requiring specific instances (DoD top secret system, DoE secret system, etc.)
2. Assign each category a base (minimum) score, for example, 2000 points for top secret systems, 1000 for secret, 800 for classified, 100 for unclassified and 200 for controlled unclassified information.
3. For each category, define a set of security controls and policies that must be satisfied by this system, and assign numerical values to each individual security control component and policy. The sum of those values must be greater or equal to the base point of this system.
4. A system is considered to be secure and compliant to laws/regulations/policies when its owner or user can prove their system is able to achieve a score that is greater than or equal to its base score

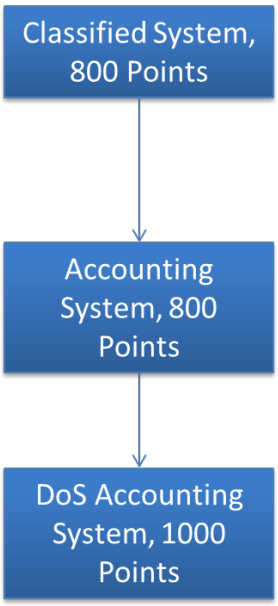
This scheme is able to solve compatibility and overlapping problems because to achieve the base score, a system only needs to comply with one set of policy, which means a system doesn't have to comply with incompatible policy and overlapping policy.

The benefit of such scheme is threefold: it utilizes existing policies, mechanisms, guidelines and best practices on information assurance; it provides maximum clarity, so that system owners/users always know exactly how they should secure their system, and what policies they must comply with. Lastly and most importantly, policies and security control components in this scheme are not fixed, they are allowed to be adjusted and updated; in the meantime, the scheme itself remains unchanged. In other words, this scheme is very flexible and stable; such a property also makes it future proof.

There are some unsettled questions with this scheme. For example, who sets the base score? Who approves which policies and security controls that a system must comply and implement? NIST is the obvious candidate; after all, it providing a significant amount of security and C&A documentation to be currently applied in the Federal space.

Example

System Hierarchy



Criteria

Policy, 400 Points	Federal Government IT Security Policy, 400 Points
Controls, 400 Points	Malware Defense, 200 Points
	Data Recovery Capability, 200 Points

Policy, 400 Points	PRA, 400 Points
Controls, 400 Points	Malware Defense, 200 Points
	Data Recovery Capability, 200 Points

Policy, 500 Points	PRA, 400 Points
	DoS IT Security Policy, 100 Points
Controls, 500 Points	Malware Defense, 200 Points
	Data Recovery Capability, 200 Points
	Data Loss Prevention, 100 Points

Appendix A

Feature / Element	Document A	Document B	Document C	Explanatory Notes
Document Number	NIST SP 800-37	ICD 503	DCID 6/3	Issuing agency number
Formal Title	Guide for Applying the Risk Management Framework to Federal Information Systems -- A Security Life Cycle Approach	Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation	Protecting Sensitive Compartmented Information within Information Systems (DCID 6/3) - Manual	Complete title
Author	NIST	IC	IC	Agency that authored the document
Author's Intent	Guideline - Risk Management Framework	Policy	Policy guidance, manual	Why did the agency generate the document?
Date	February, 2010	September, 2008	May, 2000	Date of most recent version
Status	Rev. 1	Rev. 1	Rev. 1	Current status
Applicability	Non-Intelligence, Federal Govt.	Intelligence Community	Intelligence Community	To whom does it apply?
Heritage / Ancestry	NCSC-TG-031, NAICAP, DITSCAP, DCID 6/3, DIACAP	DCID 6/3, 6/5	DCID 1/16 Supplement	Source document(s)
Supersedes	All guidance/manuals	DCID 6/3, 6/5	DCID 1/16 Supplement	Predecessor document(s)
Focus / Philosophy	Application of Enterprise Risk Management Framework including C&A	Enterprise C&A Policy	Manual, policy supplement	Primary central concept / basic approach
Scope	Extensive, well written, current, specific, flexible where needed	General, no depth beyond executive level authorities, still viable	Extensive, manualized, section, subsection, …, still viable	Level of analysis / applicability
Method	Monitoring and remediation of controls as needed	Reciprocity	Routine tracking and evaluation of security state	Method of application / enforcement
Core Issues	RMF	implements strategic goals agreed upon Jan. 2007 by the IC CIO	establishes the security requirements for all applicable systems	Core problem addressed

Feature / Element	Document A	Document B	Document C	Explanatory Notes
Documentation	Security Assessment Report	not specified	Prot. Lvl. 1 - System Security Plan; CONOPS - Security Concept of Ops; Prot. Lvl. 2 add guides or manuals for privileged users; Certification test plans, etc.	How / where are results documented?
Complements	Any policy, security controls documentation	DCID 6/3 manual	DCID 6/3 policy	Document(s) that it adds to
Duplicates / Overlaps	DCID 6/3	N/A	SP 800-37	Document(s) that cover the same issues & apply to the same general set of agencies
Conflicts With	N/A	N/A	N/A	Document(s) that it contradicts
Conflict Resolution	not addressed	Reciprocity, governance and dispute resolution	see ICD 503	How does it handle conflicts with other documents?
Major Strength	Effective, well written	Policy establishment	Effective, well written	What's good about it
Major Weakness	Does not address reciprocity	Rescinded manual and never provided a new one; no reference to relevant security documentation or where to find it	Straight process	What's not so good about it
What Should Change?	N/A	Provide reference documents section	No changes needed; process to be followed	How could it be better
Ease of Administration	Easier -- Excellent background information, flexibile documentation and system definition	Seems dated and not applicable, repetitive	very specific, step-by-step	Which is easier to administer and why?
Which Is Better?		X		Which is better from a policy perspective and why?
Which Ensures Better Security ?	X			Which does a better job of ensuring IT security? And, why?
Do We Need Both?	Now only need SP 800-37; should become the baseline guideline for all existing C&A policy documentation			Do we really need both? Why / Why Not?

Bibliography

Department of Defense. *DoD Information Assurance Certification and Accreditation Process (DIACAP).* Instruction. Washington, D.C.: Department of Defense, 2007. Electronic.

Director of Central Intelligence. "Protecting Sensitive Compartmented Information within Information Systems (DCID 6/3)." 24 May 2000.

Director of National Intelligence. "ICD 503, Intelligence Community INformation Technology Systems Security Risk Management, Certification and Accreditation." 15 Sept. 2008.

Government Accountability Office. *Information Security: Progress Made on Harmonizing Policies and Guidance for National Security and Non-National Security Systems*. Government Document. Washington D.C.: GAO, 2010. Electronic.

Grimes, John G. *CNSS Report: Progress Against 2008 Priorities.* Progress Report. Washington D.C.: CNSS, 2009.

Intelligence, Director Central. *Protecting Sensitive Compartmented Information within Information Systems (DCID 6/3) - Manual*. Manual. Washington, D.C.: Central Intelligence Agency, 2000.

Intelligence, Director of National. *Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation*. Directive. Washington, D.C.: Intelligence Community, 2008.

Marzigliano, Len. *http://resources.infosecinstitute.com/goodbye-diacap-hello-diarmf/*. 17 November 2011. Electronic. 22 April 2013.

National Institutes of Standards and Technology. *NIST SP 800-37: Guide for Applying the Risk Management Framework to Federal Information Systems*. Guideline. Gaithersburg, MD: National Institute of Standards and Technology, 2010. Electronic.

National Security Agency. *NCSC Certification and Accreditation Process Handbook for Certifiers (NCSC-TG-031).* Handbook . Washington, D.C.: National Computer Security Center, 1996. Electronic

Office of Management and Budget. "Circular A-119." 10 Feb. 1998.

Singer, Jill T. *NRO CIO Annual Report 2010.* 15 4 2011. 16 4 2013. <http://www.nro.gov/news/CIO-ar-01.pdf>.

Takai, Teresa M. *CNSSP No. 22, Policy on Information Assurance Risk Management for National Security Systems*. Policy. Washington, D.C.: Committee on National Security Systems (CNSS), 2012. Electronic.

—. *Policy on Information Assurance Risk Management for National Security Systems*. Federal secuity policy document. Washington, D.C.: Committee on National Security Systems Policy, January 2012.

Welke, Steve. "The NIST Information Assurance Risk Management Approach." White Paper. 2009.

The Evolving Story of Information Assurance at the DoD Philip L. Campbell Sandia Report January 2007