10th International Command and Control Research and Technology Symposium
The Future of C2

Defense Information Assurance Certification and Accreditation Process (DIACAP) and the Global Information Grid (GIG) Information Assurance (IA) Architecture

Information Assurance Track

CYGNACOM SOLUTIONS

Jenifer M. Wierum
CygnaCom Solutions, Inc.
7925 Jones Branch Drive, Suite 5200
McLean, VA 22102-3321
(O) 703-848-0883
(C) 210-396-0254
(F) 703-848-0985
jwierum@cygnacom.com
C&A@cygnacom.com

Defense Information Assurance Certification and Accreditation Process (DIACAP) and the Global Information Grid (GIG) Information Assurance (IA) Architecture

Jenifer M. Wierum
CygnaCom Solutions, Inc.
McLean, VA
(O) 703-848-0883
(C) 210-396-0254
jwierum@cygnacom.com

ABSTRACT

In the past, the Department of Defense (DoD) Certification and Accreditation (C&A) process has been both arduous and lengthy. It was perceived as intimidating and required vast amounts of documentation. The scope and complexity of the Global Information Grid (GIG) coupled with a plethora of overlapping and sometimes conflicting requirements necessitated a change to the C&A process. The GIG will require advances in Information Assurance (IA) technologies which will introduce new risks. The C&A process needed to be streamlined in order to ensure that it could properly support the GIG IA Architecture.

Therefore, the DoD Information Technology Security Certification and Accreditation Process (DITSCAP) is being replaced by the Defense Information Assurance Certification and Accreditation Process (DIACAP). The DIACAP is not just an upgraded DITSCAP, rather it's an entirely new process designed to fulfill the needs of the entities comprising the GIG. In support of the DIACAP, an automated tool has been created that will act as an Integrated System for Select Core IA Program Management Processes. This tool, known as the Enterprise Mission Assurance Support System (eMASS), is designed to Support the DoD 8500-series Policy Framework. Future iterations of eMASS will support DCID 6/3 (Intelligence Community) and NIST SP 800-37/53 (Civil) in addition to the DIACAP. This paper will outline the C&A approach and activities and show how it will subsume multiple existing requirements to better support the GIG IA Architecture.

Table of Contents

1.0 The History of Certification and Accreditation (C&A)

During the 1950's, the U.S. Government was concerned that emanations could be captured from an electric encryption device and then reconstructed. To counter this threat, the Government created a classified set of standards for limiting electric or electromagnetic radiation emanations from electronic equipment, known as TEMPEST.

The 1980's introduced computers into the daily operations of the U.S. Government. The Government quickly realized that a process for ensuring proper security and protection of the data needed to be developed. Based on this realization, the Government initiated Information Security programs. By the 1990's, the Government created Information Assurance (IA) programs oversee the safe and secure transmission and processing of information. The IA programs identified problems with the security measures utilized to safeguard information.

Through the years, the U.S. Government has issued several guidelines and standards relating to computer security and the proper handling of computer information. In addition to these documents the Government also created a method, known as Certification and Accreditation (C&A), of ensuring that a system met all of its security requirements prior to becoming operational.

The following provide brief introductions to many of the Information Security and IA documents that the Government has produced over the years and an idea of how the evolved over time.

1.1 Federal Information Processing Standard (FIPS) 102

In 1983, the National Bureau of Standards, now known as the National Institution of Standards and Technology (NIST), implemented Federal Information Processing Standard (FIPS) 102, the *Guideline for Computer Certification and Accreditation*. This process was designed to certify an application through a technical evaluation in order to determine if it met security requirements. The accreditation of the system was the official authorization that allowed the application to operate in the computing environment.

FIPS 102 defined Certification and Accreditation as follows:

- **Certification** - The technical evaluation, made as part of and in support of the accreditation process, that establishes the extent to which a particular computer system or network design and implementation meet a pre-specified set of security requirements [FIPS 102].

- **Accreditation** - The authorization and approval granted to an ADP system or network to process data in an operational environment, and made on the basis of a certification by designated technical personnel of the extent to which design and implementation of the system meet pre-specified requirements for achieving adequate security [FIPS 102].

1.2 Trusted Computer System Evaluation Criteria (TCSEC)

The Department of Defense (DoD) issued the Trusted Computer System Evaluation Criteria (TCSEC), DoD 5200.28-STD in December 1985 [DoD 5200.28-STD]. The TCSEC, commonly referred to as the Orange Book, provided computer security guidance for Automated Information Systems (AISs). This was followed by the Trusted Network Evaluation Criteria, affectionately referred to as The White Book in 1985 [NCSC, 1987]. The concepts put forward in these volumes later evolved into the Common Criteria [ISO, 15408].

1.3 Office of Management and Budget Circular A-130

In 1985, the Government also issued the Office of Management and Budget Circular A-130 (OMB A-130), *Management of Federal Information Resources* [OMB A130, 1996]. This circular provided uniform government-wide information resources management policies of Federal information resources as required by the Paperwork Reduction Act of 1980 [40 USC 3502].

1.4 Computer Security Act of 1987

Following OMB A-130, The Computer Security Act of 1987 developed standards and guidelines to assure [40 USC 0759]:

- Cost-effective security
- Privacy of sensitive information
- Standards and guidelines are followed
- Security plans are developed
- Mandatory periodic training is conducted

The Computer Security Act also provided a provision to allow agencies to waive mandatory FIPS. This waiver provision, in effect, significantly dampened the effectiveness of FIPS.

1.5 DoD Information Technology Security Certification and Accreditation Process (DITSCAP)

Implementation of the Orange Book was not enough. The DoD realized that an AIS must undergo a technical analysis and management approval before it would be allowed to operate. At this point, several DoD organizations had already created their own processes.

In 1992, the Office of the Assistant Secretary of Defense for Command, Control, Computers and Intelligence (ASD(NII)) realized the necessity of formalizing these multiple individual processes into one over-arching, DoD wide procedure. A working group was formed consisting of DoD Service and Agency representatives. Several existing processes were evaluated by the working group; however none were deemed appropriate for the entire department. After a few years the culmination of the working group’s efforts finally came to an end in 1997 with the introduction of the DoD Information Technology Security Certification and Accreditation Process (DITSCAP) [DoD 5200.40].

The DITSCAP was described as the process that would not only ensure all security issues had been met, but it would also reduce the overall cost of the accreditation process. It was to be applied to strategic and tactical systems, as well as stand-alone information systems and networks. The DITSCAP focused on risks at the system level and the infrastructure level. At the time, the DITSCAP was considered a "network-centric" process because it evaluated the impact of systems and networks against the overall infrastructure.

The DITSCAP employed a four phased approach:

- **Phase 1, Definition**. The Definition Phase includes activities to verify the system mission, environment and architecture, identify the threat, define the levels of effort, identify the Designated Approving Authority (DAA) and Certification Authority (Certifier), and document the C&A security requirements [DoD 5200.40].

- **Phase 2, Verification**. The Verification Phase includes activities to document compliance of the system with previously agreed on security requirements [DoD 5200.40].

- **Phase 3, Validation**. The Validation Phase includes activities to assure the fully integrated system in its specific operating environment and configuration provides an acceptable level of residual risk [DoD 5200.40].

- **Phase 4, Post Accreditation**. The Post Accreditation Phase includes activities to monitor system management, configuration, and changes to the operational and threat environment to ensure an acceptable level of residual risk is preserved [DoD 5200.40].

Within each of these phases, the DITSCAP outlined roles and responsibilities. These roles included:

- DAA
- Certifier and Certification Team
- User Representative
- Information System Security Officer (ISSO)
- Program Manager and Support Staff
- Developer, Integrator, or Maintainer
- Configuration Control and Configuration Management
- System Administration

The DITSCAP also dictated the creation of a System Security Authorization Agreement (SSAA). The SSAA is a living document that defines all of the system's specifications. It also describes the applicable set of planning and certification actions, resources, and documentation required to support the certification and accreditation.

1.6 British Standard 7799 (ISO/IEC 17799)

In parallel with the DoD development of the DITSCAP, the British Standards Institute developed a standard for Information Security, the British Standard [BS7799], released in 1995. The standard was more of a management standard focusing on the non-technical issues relating to IT systems. This standard was not widely known until it became the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 17799, the *Code of Practice for Information Security Management*, in 2000. ISO/IEC 17799 defined Information Security as the preservation of confidentiality, integrity, and availability. The standard was organized into ten main sections:

- Security Policy
- Security Organization
- Asset Classification and Control
- Personnel Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- Systems Development and Maintenance
- Business Continuity Management
- Compliance

Each section contains a set of information security control objectives with a range of controls outlined as the “best practice” for meeting the objectives. ISO/IEC 17799 is currently being revised and is expected to be re-released this year.

1.7 Common Criteria (ISO/IEC 15408)

Existing US, Canadian, and European criteria programs came together in 1993 and started the Common Criteria Project. The purpose was to devise one standard for Common Criteria evaluations. The initial version of the Common Criteria, Version 1.0, was completed in January 1996. Based on a number of trial evaluations and an extensive public review, Version 1.0 was extensively revised and Version 2.0 was produced in April of 1998. Concepts for the Common Criteria were taken from numerous sources including the Orange Book, TCSEC, BS 7799, as well as Canadian and European publications. In 1999, the Common Criteria was revised in order to align it with ISO/IEC 154508, *Evaluation Criteria for IT Security*. Whereas ISO/IEC 17799 was the management standard, the Common Criteria [ISO/IEC 15408] was the technical standard intended to support the specification and technical evaluation of IT security features in products.

1.8 National Information Assurance Certification and Accreditation Process (NIACAP)

In 2000, the U.S. Federal Government came out with their version of the DITSCAP called the National Information Assurance Certification and Accreditation Process (NIACAP), National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 1000

[NSTISSI 1000]. Due to the different nature of the information being protected, the NIACAP takes a slightly different approach to the C&A of a system than the DITSCAP. Both the DITSCAP and NIACAP used the four phased approach of: Definition, Verification, Validation, and Post Accreditation. However, unlike the DITSCAP the NIACAP did not require the role of an ISSO. The NIACAP also directed the creation of a System Security Plan (SSP) rather than the DITSCAP SSAA. Otherwise, the NIACAP is virtually identical to the DITSCAP and established the minimum standards required for certifying and accrediting national security systems.

1.9 The Defense Authorization Act of 2001

The Defense Authorization Act of 2001 contained the Government Information Security Reform Act (GISRA) [GISRA]. The GISRA required agencies to implement efforts to secure electronic information and systems; to thoroughly assess their security management practices; and to report on their security programs, processes, technology and personnel to the Office of Management and Budget (OMB).

1.10 The E-Government Act of 2002

New emerging threats to the U.S. Government dictated the need for new security measures. In response to these emerging threats, the E-Government Act became law in 2002. This legislation also contained the Federal Information Security Management Act (FISMA) [FISMA, 2002] which replaced the GISRA. FISMA required government agencies and components to improve security by setting forth fundamental Security Objectives for information and information systems. These objectives were the same objectives stated in ISO/IEC 17799 from 2000:

- Confidentiality
- Integrity
- Availability

FISMA superceded the Computer Security Act of 1987. FISMA removed the waiver provision provided in the Computer Security Act which allowed agencies to waive mandatory FIPS. However, as stated in FISMA, FIPS do not apply to national security systems.

1.11 Information Assurance Implementation (DoDI 8500.2)

FISMA started a chain reaction that required both the DoD and other Federal Government Departments and Agencies to update their current guidelines and standards regarding Information Assurance. To support FISMA, the DoD issued the *Information Assurance Implementation* [DoDI 8500.2] in 2003. DoDI 8500.2 defined the Security Controls required to ensure that the confidentiality, integrity, and availability of an information system were being met, monitored, and managed. A primary difference between DoDI 8500.2 and ISO/IEC 17799 is the fact that Security Controls outlined in the DoDI 8500.2 are mandatory, whereas the specific controls in ISO were not. The ISO standard expected that each organization would undertake a structured information security risk assessment process to determine its requirements before selecting controls that were appropriate to its particular circumstances

1.12 Federal Information Processing Standard (FIPS) 199

Based on the requirements set forth in FISMA, NIST also began developing a new guideline for C&A in 2003. The result was FIPS 199, the *Standards for Security Categorization of Federal Information and Information Systems* [FIPS 199]. This document replaced the 1983 FIPS 102. The new FIPS 199 developed the standards for categorizing information and information systems.

Based on the FISMA Security Objectives, FIPS Publication 199 defined three levels of potential impact on organizations or individuals due to a security breach:

- Low – Causing a limited adverse effect
- Medium – Causing a serious adverse effect
- High – Causing a severe or catastrophic adverse effect

In support of FIPS 199 and FISMA, NIST developed a suite of documents for conducting C&A. This documentation suite included the following:

- NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*

- NIST Special Publication 800-53, *Security Controls for Federal Information Systems* (interim guidance)

- NIST Special Publication 800-53A, *Techniques and Procedures for Verifying the Effectiveness of Security Controls in Federal Information Systems*

- NIST Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System*

- NIST Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Objectives and Risk Levels*

NIST is currently working on FIPS 200, *Minimum Security Controls for Federal Information Systems* [FIPS 200]. It is expected to be release later this year. Upon its release FIPS 200 will replace the interim guidance of NIST SP 800-53. This set of documentation is intended to provide a structured, yet flexible framework for selecting, specifying, employing, and evaluating the security controls in Federal information systems

1.13 Specific to Classified Systems

Through the years there has been special guidance provided for the handling of classified information and systems. The following provides brief descriptions of some of these guidelines.

1.13.1 Executive Order 12356

In 1982, Executive Order 12356 was issued in order to provide a uniform method for classifying, declassifying, and safeguarding national security information.

1.13.2 Executive Order 12829

A new Executive Order was introduced at the beginning of 1993. Executive Order 12829 established a National Industrial Security Program to safeguard Federal Government classified information that is released to contractors, licensees, and grantees of the United States Government.

1.13.3 National Industrial Security Program Operating Manual (NISPOM)

The classified community decided they also needed some form of standardized guidance. In of 1995, the U.S. Department of Defense published the National Industrial Security Program Operating Manual (NISPOM), DoD 5220.22. The NISPOM replaced the DoD Industrial Security Manual for Safeguarding Classified Information [DoD 5220.22-M]. It required each AIS to undergo an independent C&A process prior to operating with classified information. The NISPOM defined Levels of Concern based on the sensitivity of the information and the consequences of a loss to any of the following:

- Confidentiality
- Integrity
- Availability

These are the same objectives as described in BS 7799, which later became ISO/IEC 17799.

1.13.4 Director of Central Intelligence Directive (DCID) 6/3

In 1999, the DoD established new guidance for Information Systems with the Director of Central Intelligence Directive (DCID) 6/3 [DCID 6/3]. DCID 6/3 specified requirements for ensuring adequate protection of certain categories of intelligence information that is stored or processed on an Information System. The DCID 6/3 focused on the same core objectives stated in NISPOM and BS 7799: protecting the confidentiality of information, protecting data integrity, and protecting data availability.

1.13.5 National Security Agency/Center Security Service (NSA/CSS) Information System Certification and Accreditation Process (NISCAP)

In 2001, NSA/CSS developed the NISCAP in support of DCID 6/3 [NISCAP]. The NISCAP defines a standard C&A process for systems designed to process information under the purview of the Director, National Security Agency (DIRNSA). Additionally, NISCAP describes the security documentation required to support the process.

1.14 More Standards

This has been an overview but far from being a complete list. There are still more standards, legislation and guidance regarding Information Systems Security and C&A. Some of these include:

- Joint Department of Defense Intelligence Information Systems (DoDIIS) / Cryptologic Secure Compartmented Information (SCI) Information Systems Security Standards (JDCSISSS)
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11
- DoD 5200.1-R, *Information Security Program Regulation*
- DoD 5200.22-M, *National Industrial Security Program Operating Manual*
- DoD 7950.1-M, *Defense Automation Resources Management Manual*
- DoDD 8000.1, *Defense Information Management (IM) Program*
- DoD 8910.1, *Management and Control of Information Requirements*

An entire paper could be devoted to this subject alone. However, this history has been provided as an aid to understanding how Information Systems Security has evolved through the years. The main topic remains where are we now with C&A and where do we need to go.

2.0 The Current State of C&A

The C&A process was designed to manage information systems and ensure they met applicable security requirements prior to becoming operational. However to most people, the C&A process is like “The Plague,” it won’t go away yet people constantly try to avoid it. Instead of being viewed as helpful, C&A is considered a hindrance. It is neither timely nor cost-efficient in an era when technology advances are coming faster than ever. Typically, when you mention C&A people cringe and try to turn the other way. Most find the idea of

C&A too complex and confusing. In order to expedite the deployment of new systems, organizations have attempted to circumvent the C&A process, which inevitably lead to more issues and problems. In other words, the current C&A process has a bad reputation and will not meet the future demands of the Global Information Grid (GIG) IA Architecture.

As history shows, there are far too many different, and occasionally conflicting, guidelines and standards. A single standard appropriate for both the DoD and Federal Government, which can be applied to unclassified and classified environments is desperately needed.

2.1 C&A and the GIG

The Joint Chiefs of Staff published the Joint Vision 2020 (JV 2020) in June 2000 (based upon the Joint Vision 2010 of July 1996). The JV 2020 requires information and decision superiority in order to achieve full spectrum dominance. JV 2020 also highlights the importance of a Network-Centric Warfare (NCW) environment. The concept of the GIG was derived by the requirements set forth in the Joint Vision. The GIG will enable interoperability and end-to end integration of AISs. Global information sharing and streamlined management capabilities are expected as a part of the GIG.

However, as with any technology venture, the innovation involved in the realization of the GIG comprises a new set of security issues and challenges that must be faced. That Draft GIG IA Strategy, published in June 2004 [GiG IA, 2004], described several challenges with regard to C&A:

- The GIG will comprise a seamless and secure end-to-end IA Architecture requiring shared enterprise services with streamlined management capabilities. The concept of individual systems will no longer exist [GiG IA, 2004].

- The GIG will encompass DoD, the Intelligence Community (IC), Federal, industry, and international partnership communities. Access privileges will be required in order to ensure information is available to those who need it and protected from those without the appropriate privileges [GiG IA, 2004].

- The GIG enables the formation of dynamic communities of interest (COIs). In some circumstances, these COIs will be formed on short notice and may exist for a relatively short timeframe. Therefore, it will not be conceivable to pre-identify all COIs that will require access to the GIG [GiG IA, 2004].

- The GIG requires greatly enhanced IA solutions to support the paradigm shift from “need to know” to “need to share.” This sharing of information will require user access that crosses traditional system and classification boundaries [GiG IA, 2004].

- The GIG will permit provisional access to data for users not normally possessing access privileges, but who may need access in certain mission-critical situations. Such scenarios will require that users, and perhaps even automated processes, will be able to override data owner and originator security settings in support of operational need [GiG IA, 2004].

All of these issues present interesting challenges for C&A. Information Assurance needs to be the first thought, not an after-thought. Considering the current attitude toward C&A, ensuring the successful implementation of the GIG IA Architecture will also require a successful process and attitude changes regarding C&A.

2.2 Defense Information Assurance Certification and Accreditation Process (DIACAP)

The U.S. DoD has developed a new C&A process. The Defense Information Assurance Certification and Accreditation Process (DIACAP) [DoDI 8510.bb] will be replacing the DITSCAP. The DIACAP is not an upgraded DITSCAP, rather it is an entirely new process designed to fulfill the needs of the entities comprising the GIG. It also establishes a DoD-wide configuration management process that considers the GIG architecture and risk assessments that are conducted at the Department and the DoD-Component level according to FISMA.

The DIACAP states that it will be applied to the following:

> "The acquisition, operation and sustainment of all DoD-owned or controlled information systems that receive, process, store, display or transmit DoD information, regardless of classification or sensitivity of the information or information system. This includes Enclaves, AIS Applications (e.g., Core Enterprise Services), Outsourced Information Technology (IT)-Based Processes, and Platform IT Interconnections." [DoDI 8510.bb]

The DIACAP implements DoDI 8500.2. This instruction specifies four Information System categories:

- Enclave
- AIS Application /Service
- Outsourced IT-Based Process
- Platform IT Interconnection

Per the DIACAP instruction, DoD Information Systems are responsible for implementing the baseline DoD IA Controls. These controls will be tested by means of the DIACAP. DoD IA Controls compliance is required in order to achieve accreditation.

The DIACAP relies on the IA Controls defined in DoDI 8500.2. The DoDI 8500.2 defines an IA Control as follows:

> "An objective IA condition of integrity, availability, or confidentiality achieved through the application of specific safeguards or through the

> regulation of specific activities that is expressed in a specified format (i.e., a control number, a control name, control text, and a control class). Specific management, personnel, operational, and technical controls are applied to each DoD information system to achieve an appropriate level of integrity, availability, and confidentiality in accordance with OMB Circular A-130." [DoDI 8500.2]

The DIACAP adds that an IA Control must achieve the appropriate levels of integrity, availability, and confidentiality according to the system's Mission Assurance Category (MAC) level. There are three MAC levels defined in DoDI 8500.2. Table 2.2-1 describes these MAC levels in terms of Loss of Integrity, Loss of Availability, and the Level of Protection Measures required.

Table 2.2-1 – Mission Assurance Category (MAC) Levels

MAC	Loss of Integrity	Loss of Availability	Protection Measures
MAC I	Unacceptable	Unacceptable	Stringent
MAC II	Unacceptable	Difficult	Additional Safeguards
MAC III	Tolerated	Tolerated	Protective; Commensurate with Best Practices

In addition to MAC levels, DIACAP implements the concept of Confidentiality Levels (CLs) as described in DoDI 8500.2. The CL is used to determine acceptable assess factors. DoDI 8500.2 indicates some of these factors may include: requirements for individual security clearances or background investigations, access approvals, and need-to-know determinations; interconnection controls and approvals; and acceptable methods by which users may access the system. Table 2.2-2 describes the three CLs.

Table 2.2-2 – Confidentiality Levels (CLs)

CL	Definition
Classified	High level required for Systems Processing Classified Information
Sensitive	Medium level required for Systems Processing Sensitive Information
Public	Basic level required for Systems Processing Public Information

The DIACAP and DoDI 8500.2 also define three levels of operating system robustness. Robustness is described as a characterization of the strength of a security function, mechanism, service, or solution, and the assurance that it is implemented and functioning correctly. The three levels of robustness are as follows:

- High - Security services and mechanisms that provide the most stringent protection and rigorous security countermeasures

- Medium - Security services and mechanisms that provide for layering of additional safeguards above good commercial practices

- Basic - Security services and mechanisms that equate to best commercial practices

With regard to operating system robustness, there are two important measurements taken into consideration, internal and external system exposure. DoDI 8500.2 defines internal and external system exposure as follows:

- Internal system exposure is a measure of the difference between the established security criteria for individual access and the actual access privileges of authorized users [DoDI 8500.2].

- External system exposure is a measure of the degree of isolation from other information systems, either through physical or cryptographic means [DoDI 8500.2]. .

Based on the internal and external measurements a level of system robustness can be derived.

Table 2.2-3 – Levels of Robustness

CL	Level of Internal System Exposure	Level of External System Exposure	Level of Total System Exposure	Level of Operating Environment Robustness
Classified	Low	Low	Low	High
Sensitive	Low	Medium	Medium	Medium
Public	Low	N/A	Low	Basic

Since the DIACAP implements the IA Controls identified in DoDI 8500.2, there are sets of mandatory controls based on the systems MAC and CL. The MAC and CL are independent of one another, so there are a total of 9 possible combinations. Each MAC and CL have a specific set of mandatory IA Controls defined in DoDI 8500.2. The MAC IA Controls address Integrity and Availability, while the CL IA Controls primarily address Confidentiality. The following table depicts the total number of IA Controls (equaling a Required Baseline Score) depending on a given system's MAC and CL.

Table 2.2-4 – Required Baseline Scores

MAC	CL	MAC IA Controls Actual		Confidentiality IA Controls	Required Baseline Score
		Integrity	Availability		
MAC I	Classified	32	38	45	115
MAC I	Sensitive	32	38	37	107
MAC I	Public	32	38	11	81
MAC II	Classified	32	38	45	115
MAC II	Sensitive	32	38	37	107
MAC II	Public	32	38	11	81
MAC III	Classified	27	37	45	109
MAC III	Sensitive	27	37	37	101
MAC III	Public	27	37	11	75

So, how will the DIACAP be able to address some of the current issues regarding C&A. First, the DIACAP will ease the burden of documentation requirements. SSAAs will no longer be necessary. A typical DIACAP package will contain a minimal set of documentation which will most likely include:

- System Identification Profile
- DIACAP Strategy
- IA Implementation Plan
- DIACAP Scorecard
- Certification Determination
- DIACAP Plan of Actions and Milestones (POA&M), as required
- Accreditation Decision
- Artifacts and Evidence of Compliance

The DIACAP Scorecard is the "report card" of how the system faired against applicable mandatory IA Controls. The DIACAP states that the Scorecard:

> "Shows the MAC and Confidentiality levels and associated IA Controls implementation score, as well as the difference between full compliance with all assigned IA Controls and actual compliance. The Scorecard will also address Component Augmented IA Controls that either supplement the baseline IA Controls articulated in DoDI 8500.2 or which meet or mitigate IA Controls with which the DoD Component is not in compliance." [DoDI 8510.bb]

The DIACAP further states that regarding the Scorecard:

> "At a minimum, a favorable accreditation decision is a requirement for interconnection of enclaves, to include enclave connection to a DoD enterprise information environment such as the NIPRNet or SIPRNet; for the hosting of AIS applications and services within enclaves; for DoD user access to outsourced IT-based processes through DoD enclaves; and for the interconnection of platform IT to DoD enclaves. The DIACAP Scorecard serves as the basis for reaching an interconnection agreement." [DoDI 8510.bb]

Table 2.2-5 depicts a notional DIACAP Scorecard [DoDI 8510.bb].

Table 2.2-5 – Notional DIACAP Scorecard

MAC	CL	Required Baseline Score	Actual Baseline Score	DoD Component Augmented	Accreditation Decision
MAC I	Classified	115			
MAC I	Sensitive	107			
MAC I	Public	81			
MAC II	Classified	115			
MAC II	Sensitive	107			
MAC II	Public	81			
MAC III	Classified	109			
MAC III	Sensitive	101			
MAC III	Public	75			

Now that the majority of the DIACAP and DoDI 8500.2 definitions have been presented, the overall DIACAP process can be shown. Figure 2.2-1 depicts the DIACAP process as shown in one of the latest briefings to the DoD Public Key Infrastructure (PKI) C&A Working Group [eMASS].

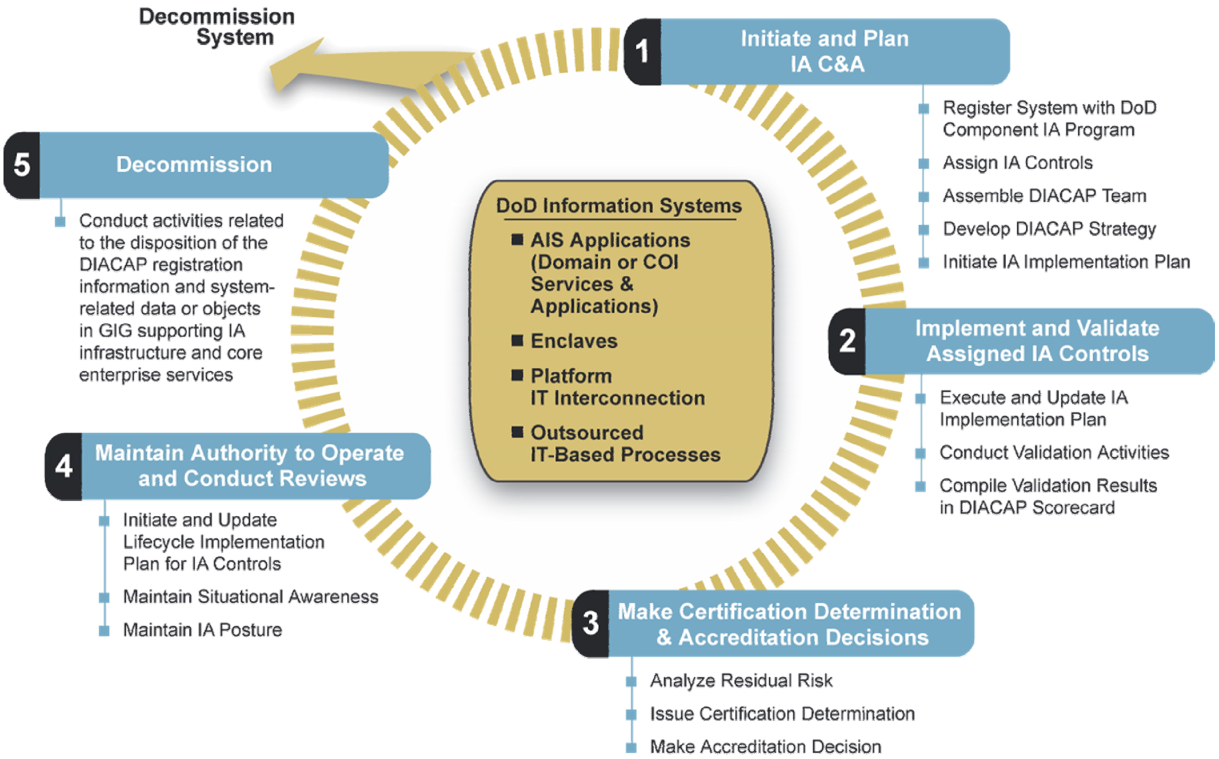

Decommission System
1
Initiate and Plan IA C&A
Register System with DoD Component IA Program
Assign IA Controls
Assemble DIACAP Team
Develop DIACAP Strategy
Initiate IA Implementation Plan
2
Implement and Validate Assigned IA Controls
Execute and Update IA Implementation Plan
Conduct Validation Activities
Compile Validation Results in DIACAP Scorecard
3
Make Certification Determination & Accreditation Decisions
Analyze Residual Risk
Issue Certification Determination
Make Accreditation Decision
4
Maintain Authority to Operate and Conduct Reviews
Initiate and Update Lifecycle Implementation Plan for IA Controls
Maintain Situational Awareness
Maintain IA Posture
5
Decommission
Conduct activities related to the disposition of the DIACAP registration information and system-related data or objects in GIG supporting IA infrastructure and core enterprise services
DoD Information Systems
AIS Applications (Domain or COI Services & Applications)
Enclaves
Platform IT Interconnection
Outsourced IT-Based Processes

Figure 2.2-1 – The DIACAP Process

The key participants in the DIACAP process are:

- DAA
- Information Assurance Manager
- Program Manager
- User Representative
- Certification Authority

The DIACAP is a fairly straight-forward process that can easily be completed. The largest factor in successfully accomplishing the DIACAP will require a change in attitude toward C&A.

2.3 Enterprise Mission Assurance Support System (eMASS)

In support of the DIACAP, an automated tool has been created that will act as an Integrated System for Select Core IA Program Management Processes. This tool, the Enterprise Mission Assurance Support System (eMASS), is designed to support the DoD 8500-series Policy Framework. So, not only is the documentation burden being lightened, but there will also be an automated tool available to support C&A efforts. This will cut down on the time expended to generate the required C&A documentation, as well as the time it takes to conduct the new activities as outlined in the DIACAP. Additionally, since the timeframe should be reduced, the overall cost of the C&A effort should be reduced as well.

There are a number of benefits to eMASS. A recent briefing to the DoD PKI C&A Working Group outlined the following benefits [eMASS]:

- **Automation**
  - Creates a C&A "package" for management of each registered system
  - Eliminates need for users to manually track down controls or related documentation
  - Notification, workflow, and workload status features enable users to track detailed, current status of each registered system

- **Accountability**
  - DoD PKI and auditing features enable tracking of each transaction
  - Roles-based access control enhances system security
  - Tracks all registered enterprise systems and provides current, detailed status of each

- **Extensibility**
  - Scalable to any enterprise, regardless of size and mission

- **Flexibility**
  - Designed to support multiple IA requirements types
  - Roles and Permissions can be customized to fit each enterprise's structure
  - Provides option to allow child or peer systems to "inherit" controls from other systems as a means of enhancing enterprise-level system security

This same reference [eMASS] identified the core features of eMASS which include:

- **Certification and Accreditation**
  - C&A package creation tool
  - System Registration
  - IA control set selection (baseline and supplemental)
  - Validation Test implementation
  - Set and manage recurring events
  - Create and manage artifacts
  - Track and manage validation/revalidation

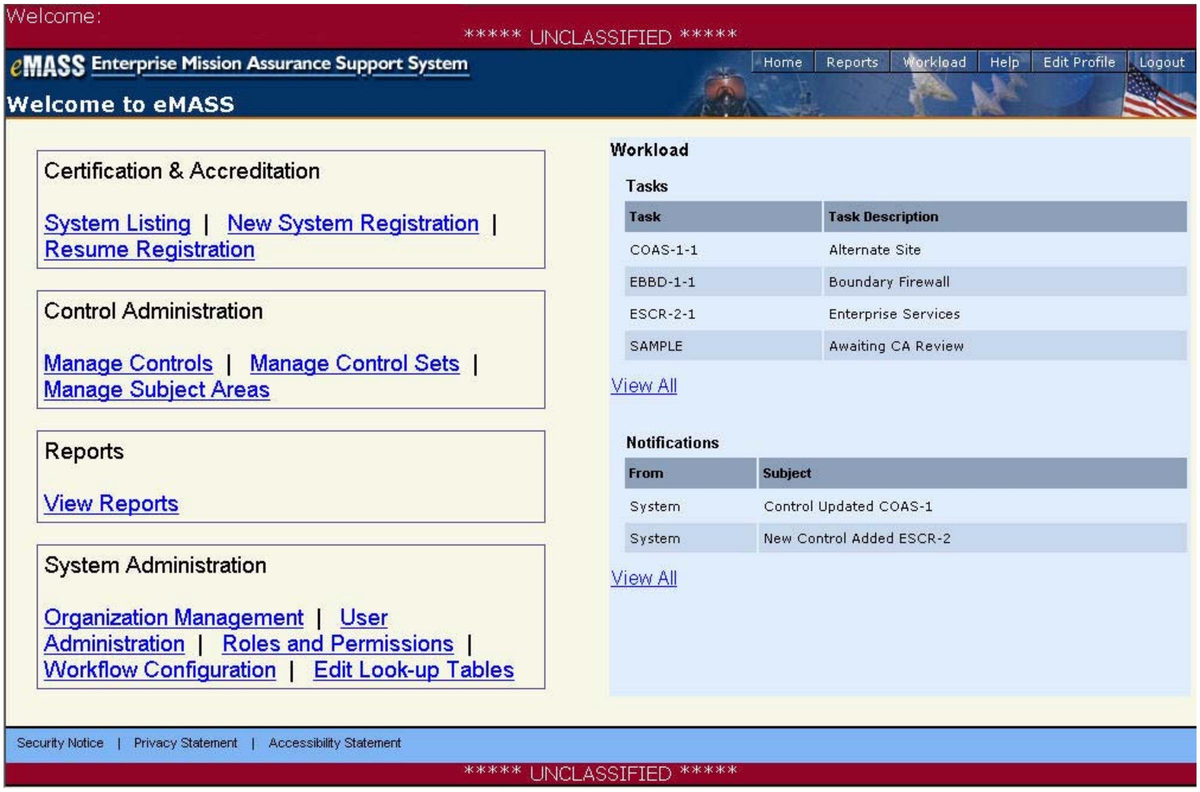
- **Controls Administration Module (CAM)**
  - View, add, delete, or modify control sets, subject areas, and controls
  - Write validation procedures and attach implementation guidance

- **Reports**
  - Generate reports on C&A process, controls, users, and system status
  - Flexibility allows users to generate reports on specific information types
  - Eliminates need for large volumes of hardcopy documents (e.g., DITSCAP SSAA)

- **System Administration**
  - eMASS System management/maintenance console for users with Administrator privileges

Since eMASS is a C&A management tool it can electronically capture system information, create C&A workflows, track C&A progress, monitor current C&A status, and provide visibility into current IA system security status across the enterprise

The eMASS site is not currently available for use. It is expected to be available shortly after the DIACAP is signed. To get an idea of what the eMASS site will offer, Figure 2.3-1 depicts the eMASS homepage. [eMASS]



Welcome:

***** UNCLASSIFIED *****

eMASS Enterprise Mission Assurance Support System

Welcome to eMASS

Certification & Accreditation

System Listing | New System Registration | Resume Registration

Control Administration

Manage Controls | Manage Control Sets | Manage Subject Areas

Reports

View Reports

System Administration

Organization Management | User Administration | Roles and Permissions | Workflow Configuration | Edit Look-up Tables

Workload

Tasks

Task	Task Description
COAS-1-1	Alternate Site
EBBD-1-1	Boundary Firewall
ESCR-2-1	Enterprise Services
SAMPLE	Awaiting CA Review

View All

Notifications

From	Subject
System	Control Updated COAS-1
System	New Control Added ESCR-2

View All

Security Notice | Privacy Statement | Accessibility Statement

***** UNCLASSIFIED *****

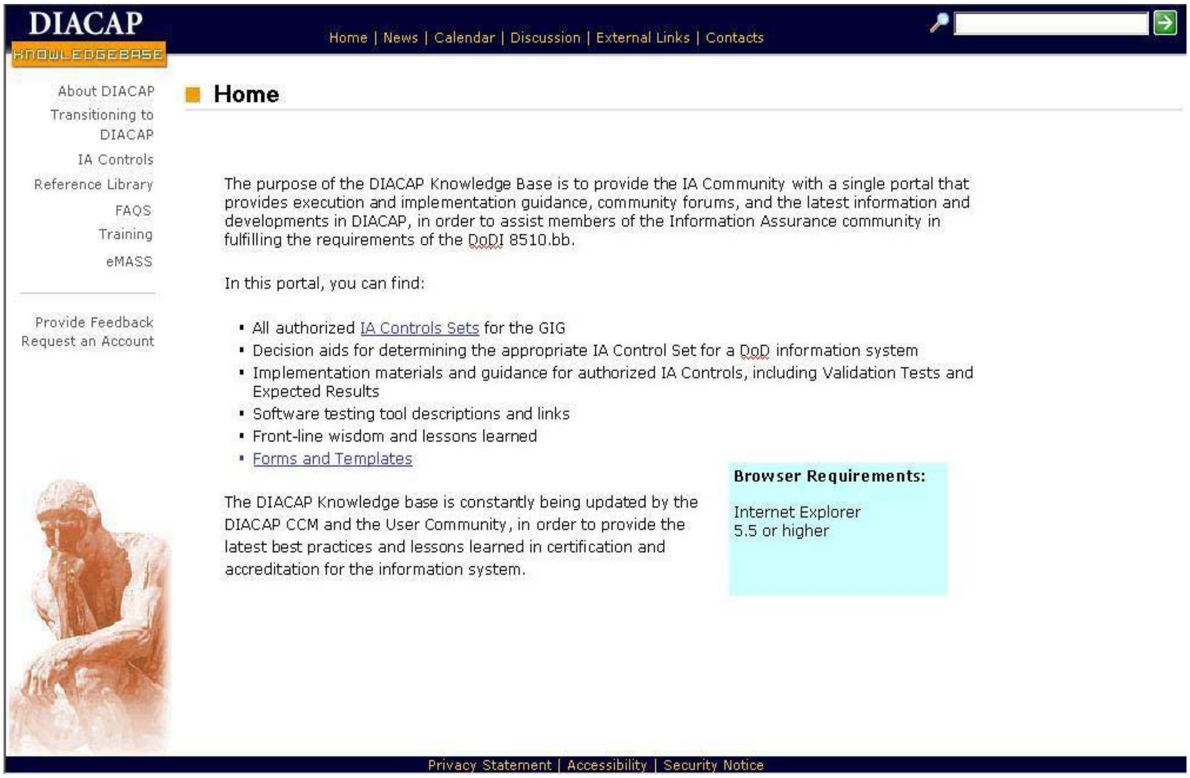
Figure 2.3-1 – eMASS Homepage

eMASS should prove to be an excellent and easy to use C&A management tool.

2.4 DIACAP Knowledge Base

In addition to eMASS, a DIACAP Knowledge Base is being created. This Knowledge Base will be an on-line resource that provides current GIG IA C&A Guidelines. It will contain a library of DIACAP tools, provide a collaboration area for the DIACAP user community, and provide news regarding IA and IA events.

The DIACAP Knowledge Base is not yet available for use. It should be available as soon as the DIACAP is signed. To gain an understanding of what the Knowledge Base will have to offer, Figure 2.4-1 depicts the DIACAP Knowledge Base homepage. [DIACAP KB]



Home

The purpose of the DIACAP Knowledge Base is to provide the IA Community with a single portal that provides execution and implementation guidance, community forums, and the latest information and developments in DIACAP, in order to assist members of the Information Assurance community in fulfilling the requirements of the DoDI 8510.bb.

In this portal, you can find:

- All authorized IA Controls Sets for the GIG
- Decision aids for determining the appropriate IA Control Set for a DoD information system
- Implementation materials and guidance for authorized IA Controls, including Validation Tests and Expected Results
- Software testing tool descriptions and links
- Front-line wisdom and lessons learned
- Forms and Templates

The DIACAP Knowledge base is constantly being updated by the DIACAP CCM and the User Community, in order to provide the latest best practices and lessons learned in certification and accreditation for the information system.

Browser Requirements:

Internet Explorer 5.5 or higher

Figure 2.4-1 – The DIACAP Knowledge Base

3.0 Evolution of a GIG C&A Process

The DoDI 8500.2, DIACAP, and eMASS are a good start. The next phase of the C&A process development will be to create one process that also incorporates the Federal and IC Information System requirements. eMASS already plans to include more tools, as well as include support for DCID 6/3 and NIST SP 800-37/53 future iterations. However, achieving and implementing one all-encompassing C&A process will not be easy. All organizations within the DoD, Federal, and IC communities must be open and receptive to the idea of one process. History has indicated that each community tends to create their own processes because they feel they have special requirements not addressed by another process.

In order to realize the goal of one C&A process, each community of interest must be able to have input into the process. They must feel that their specific needs and concerns are being heard and addressed by the process. Compromises must be reached in order to move forward. In reality, each community is trying to achieve the same objective: ensuring the security of information systems during the storage, processing, transmission, sharing and dissemination of information within the new GIG IA Architecture.

In order to succeed, this type of effort will take an extremely large amount of collaboration. As we move forward with the GIG, a new C&A process for all communities of interest must be a “Living Process.” It must be modified and updated as lessons are learned and new information technologies, with potential new risks, are introduced.

One of the biggest challenges facing the idea of one C&A process is attitude. The success of a new process is more than just creating documents and automated tools. Past attitudes regarding C&A must be overcome. A new C&A will need to gain a reputation as being easy, timely, and cost-effective. A shift in attitude will take an effort, and can only be achieved with communication, time, and patience.

Acronyms

AIS	Automated Information System
ASD	Assistant Secretary of Defense
BS	British Standard
C&A	Certification and Accreditation
CAM	Controls Administration Module
CL	Confidentiality Level
COIs	Communities of Interest
DAA	Designated Approving Authority
DCID	Director of Central Intelligence Directive
DIACAP	Defense Information Assurance Certification and Accreditation Process
DIRNSA	Director, National Security Agency
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DoD	Department of Defense
DoDIIS	DoD Intelligence Information Systems
eMASS	Enterprise Mission Assurance Support System
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
GIG	Global Information Grid
GISRA	Government Information Security Reform Act
HIPAA	Health Insurance Portability and Accountability Act
IA	Information Assurance
IC	Intelligence Community
IEC	International Electrotechnical Commission
IM	Information Manager
ISO	International Organization for Standardization
ISSO	Information System Security Officer
IT	Information Technology
JDCSISSS	Joint DoD Cryptologic SCI Information Systems Security Standards
MAC	Mission Assurance Category
NCW	Network-Centric Warfare
NIACAP	National Information Assurance Certification and Accreditation Process

NISCAP	NSA/CSS Information System Certification and Accreditation Process
NISPOM	National Industrial Security Program Operating Manual
NIST	National Institution of Standards and Technology
NSA/CSS	National Security Agency/Center Security Service
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
NSTISSP	National Security Telecommunications and Information Systems Security Policy
OMB	Office of Management and Budget
PKI	Public Key Infrastructure
POA&M	Plan of Actions and Milestones
SCI	Secure Compartmented Information
SSAA	System Security Authorization Agreement
SSP	System Security Plan
TCSEC	Trusted Computer System Evaluation Criteria

References

[40 USC 0759]	Computer Security Act of 1987. U.S. Code 759. Washington, DC: U.S. Congress, 1987.
[40 USC 3502]	Paperwork Reduction Act of 1995. U.S. Code 3502(2). Washington, DC: U.S. Congress, 22 May 1995.
[BS 7799]	The British Standard for Information Security. British Standard 7799. London, UK: British Standards Institute, 1995.
[DCID 6/3]	Protecting Sensitive Compartmented Information Within Information Systems. Director of Central Intelligence Directive (DCID) 6/3. Washington, DC: U.S. Central Intelligence Agency (CIA), 5 June 1999.
[DIACAP KB]	DIACAP Knowledge Base Overview. Briefing. Washington, DC: DoD PKI C&A Working Group, March 2005.
[DoD 5200.1-R]	Information Security Program Regulation. DoD 5200.1-R. Washington, DC: U.S. Department of Defense, 1997.
[DoD 5200.22-M]	National Industrial Security Program Operating Manual. DoD 5200.22-M. Washington, DC: U.S. Department of Defense, 1991.
[DoD 5200.28]	Department of Defense Trusted Computer Security Evaluation Criteria (TCSEC), (a.k.a. The Orange Book). Washington, DC: U.S. Department of Defense, December 1985.
[DoD 5220.22]	National Industrial Security Program Operating Manual (NISPOM). DoD 5220.22. Washington, DC: U.S. Department of Defense, 1995.
[DoD 5220.22-M]	DoD Industrial Security Manual for Safeguarding Classified Information. DoD 5220.22-M. Washington, DC: U.S. Department of Defense Assistant Secretary of Defense for Command, Control, Communications and Intelligence, 1989.
[DoD 5200.40]	DoD Information Technology Security Certification and Accreditation Process (DITSCAP). Washington, DC: U.S. Department of Defense (DoD), 30 December 1997.
[DoD 7950.1-M]	Defense Automation Resources Management Manual. DoD 7950.1-M. Washington, DC: U.S. Department of Defense, 1988.
[DoDD 8000.1]	Defense Information Management (IM) Program. DoD 8000.1. Washington, DC: U.S. Department of Defense, 1992.

[DoDD 8000.1]	Management of DoD Information Resources and Information Technology. DoD 8000.1. Washington, DC: U.S. Department of Defense, 2002.
[DoDI 8500.2]	Information Assurance Implementation. DoD Instruction 8500.2. Washington, DC: U.S. Department of Defense, 2003.
[DoDI 8510.bb]	Defense Information Assurance Certification and Accreditation Process (DIACAP). DoD Instruction 8510.bb. Washington, DC: U.S. Department of Defense, draft 2005.
[DoDD 8910.1]	Management and Control of Information Requirements. DoDD 8910.1. Washington, DC: U.S. Department of Defense, 1993.
[eMASS]	eMASS Overview. Briefing. Washington, DC: DoD PKI C&A Working Group, March 2005.
[EO 12356]	National Security Information. Executive Order 12356. Washington, DC: U.S. Office of the President, 6 April 1982.
[EO 12829]	National Industrial Security Program. Executive Order 12829. Washington, DC: U.S. Office of the President, 1993.
[FIPS 102]	Guidelines for Computer Security Certification and Accreditation. FIPS 102. Washington, DC: U.S. National Institute of Standards and Technology, 1983.
[FIPS 199]	Standards for Security Categorization of Federal Information and Information Systems. FIPS 199. Washington, DC: U.S. National Institute of Standards and Technology, 2003.
[FIPS 200]	Minimum Security Controls for Federal Information Systems. FIPS 200. Washington, DC: U.S. National Institute of Standards and Technology, expected December 2005.
[FISMA, 2002]	Federal Information Security Management Act (FISMA). Washington, DC: U.S. Congress, 2002.
[GiG IA, 2004]	GIG IA Strategy (Draft). Fort Meade, MD: National Security Agency (NSA) Information Assurance Directorate, June 2004.
[ISO/IEC 15408]	Common Criteria for Information Technology Security Version 2.1. ISO/IEC Standard 15408. International Organization for Standardization, 1999.

[ISO/IEC 17799]	Code of Practice for Information Security Management. ISO/IEC Standard 17799. International Organization for Standardization, 2000.
[JDCSISSS]	Joint Department of Defense Intelligence Information Systems (DoDIIS) / Cryptologic SCI Information Systems Security Standards (JDCSISSS). Washington, DC: U.S. Department of Defense, 2001.
[JV 2020]	Joint Vision 2020. Washington, DC: U.S. Joint Chiefs of Staff (JCS), June 2000.
[JV 2010]	Joint Vision 2010. Washington, DC: U.S. Joint Chiefs of Staff (JCS), 1996.
[NCSC, 1987]	Trusted Network Interpretation. Fort Meade, MD: National Computer Security Center, 31 July 1987.
[NISCAP]	National Security Agency/Center Security Service (NSA/CSS) Information System Certification and Accreditation Process (NISCAP). Washington, DC: U.S. National Security Agency/Center Security Service (NSA/CSS), 2001.
[NSTISSI 1000]	National Information Assurance Certification and Accreditation Process (NIACAP). NSTISSI 1000. Washington, DC: National Security Telecommunications and Information Systems Security Committee (NSTISSC), 2000.
[NSTISSP 11]	National Policy Regarding the Evaluation of Commercial Products. National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11. Washington, DC: Chairman of the National Security Telecommunications and Information Systems Security Committee (NSTISSC) Committee on National Security Systems (CNSS), 2000.
[OMB A130, 1996]	Management of Federal Information Resources. Washington, DC: U.S. Office of Management and Budget (OMB), 8 February 1996.
[PL 104-191]	Health Insurance Portability and Accountability Act of 1996 (HIPAA). Public Law 104-191. Washington, DC: 104th Congress, 1996.
[PL 106-398]	National Defense Authorization Act for Fiscal Year 2001; Government Information Security Reform Act (GISRA). PL 106-398. Washington, DC: U.S. Congress, 2001.
[SP 800-37]	Guide for the Security Certification and Accreditation of Federal Information Systems. NIST Special Publication 800-37. Washington, DC: U.S. National Institute of Standards and Technology, 2004.

[SP 800-53]	Security Controls for Federal Information Systems (interim guidance). NIST Special Publication 800-53. Washington, DC: U.S. National Institute of Standards and Technology, 2005
[SP 800-53A]	Techniques and Procedures for Verifying the Effectiveness of Security Controls in Federal Information Systems. NIST Special Publication 800-53A. Washington, DC: U.S. National Institute of Standards and Technology, draft 2004.
[SP 800-59]	Guideline for Identifying an Information System as a National Security System. NIST Special Publication 800-59. Washington, DC: U.S. National Institute of Standards and Technology, 2003.
[SP 800-60]	Guide for Mapping Types of Information and Information Systems to Security Objectives and Risk Levels. NIST Special Publication 800-60. Washington, DC: U.S. National Institute of Standards and Technology, 2004.