

## **DIACAP and the GIG IA Architecture**

**10<sup>th</sup> ICCRTS**

**June 16, 2005**

**Jenifer M. Wierum**

**(O) 210-9252417**

**(C) 210-396-0254**

**[jwierum@cygnacom.com](mailto:jwierum@cygnacom.com)**

## OMB Circular A-130 (1996)

- OMB A-130 required systems and applications provide "adequate security"
  - Security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information.
  - Includes assuring that systems and applications used by the agency operate effectively and provide appropriate **confidentiality, integrity, and availability**, through the use of cost-effective management, personnel, operational, and technical controls.

## E-Government Act 2002 (FISMA)

- Federal Information Security Management Act (FISMA) was part of the E-Government Act 2002
- FISMA required government agencies and components to improve security
  - Set forth fundamental Security Objectives for information and information systems
    - Confidentiality
    - Integrity
    - Availability
- FISMA superceded the Computer Security Act of 1987
- FISMA removed the FIPS waiver provision provided in the Computer Security Act

[FISMA, 2002]

## DoD IA Implementation

- DoDD 8500.1 (2002)
  - Establishes policy and assigns responsibilities to achieve DoD IA through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network centric warfare. [DoDD 8500.1]
- DoDI 8500.2 (2003)
  - Defined the Security Controls required to ensure that the confidentiality, integrity, and availability of an information system were being met, monitored, and managed.
  - Security Controls outlined in the DoDI 8500.2 are mandatory. [DoDI 8500.2]

# DoD Information Systems

- AIS Application
  - AIS Application is the product or deliverable of an acquisition program
- Enclave
  - Collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security
- Outsourced IT-Based Processes
  - General term used to refer to outsourced business processes supported by private sector information systems, outsourced information technologies, or outsourced information services
- Platform IT Interconnection
  - Refers to network access to platform IT

[DoDI 8500.2]

# Security Objectives

- Integrity
  - Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity [44 USC 3542]
  - A loss of *integrity* is the unauthorized modification or destruction of information. [FIPS 199]
- Availability
  - Ensuring timely and reliable access to and use of information [44 USC 3542]
  - A loss of *availability* is the disruption of access to or use of information or an information system. [FIPS 199]
- Confidentiality
  - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information [44 USC 3542]
  - A loss of *confidentiality* is the unauthorized disclosure of information. [FIPS 199]

## Global Information Grid (GIG)

- 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.
- 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.
- 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.

[GiG IA, 2004]

## Global Information Grid (GIG)

- Requires greatly enhanced IA solutions to support the paradigm shift from “need to know” to “need to share.”
  - Information sharing will require user access that crosses traditional system and classification boundaries.
- Permit provisional access to data for users not normally possessing access privileges, but who may need access in certain mission-critical situations.
  - Will require that users, and perhaps even automated processes, the ability to override data owner and originator security settings in support of operational need.

[GiG IA,2004]

## DIACAP

- New C&A Process; not an updated DITSCAP
- Implements 8500.1 & 8500.2
- Intended to support the GIG
- Establishes a DoD-wide CM process
  - Considers the GIG architecture
  - Risk assessments conducted at the Department and the DoD-Component level according to FISMA
- Shifting from an individual system to Enterprise perspective
- Review annually
- More closely related to the updated DoD Acquisition Process

## Roles and Responsibilities

- Designated Approval Authority (DAA)
  - Authority and ability to evaluate the mission, business case, and budgetary needs for the system in view of the security risks.
  - Determines the acceptable level of residual risk and makes the authorization decision.
- Information Assurance Manager (IAM)/Certification Authority (CA)
  - Manages the certification process
  - Performs a comprehensive evaluation of the technical and non-technical of the certification effort
  - Reports the status of certification and makes the authorization recommendation to the DAA

## Roles and Responsibilities

- Program Manager/System Manager (PM/SM)
  - Represents the interests of the system throughout its life cycle
- User Representative (UR)
  - Concerned with system availability, integrity, and confidentiality as they relate to the system mission
- Validation Tester
  - Tests the system against the IA Controls to ensure the system is compliant

## Mission Assurance Category (MAC)

- Reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the warfighters' combat mission.
- Mission assurance categories are primarily used to determine the requirements for availability and integrity.

## Required Levels of Integrity and Availability

MAC	Level of Integrity Required	Level of Availability Required
MAC I	High	High
MAC II	High	Medium
MAC III	Basic	Basic

## Confidentiality Level (CL)

- Independent of the MAC
- The CL is used to determine acceptable assess factors:
  - Requirements for individual security clearances or background investigations, access approvals and need-to-know determinations
  - Interconnection controls and approvals
  - Acceptable methods by which users may access the system

## 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

## Information Assurance (IA) Controls

- Each DoD information system assigned to a MAC
- Each DoD information system assigned a CL
- The MAC and CL determine the applicable IA Controls
- IA Controls are the baseline requirements for IA C&A
  - IA Controls ensure that the integrity, availability, or confidentiality of an information system meets its requirements
- The MAC IA Controls focus on integrity and availability
- The CL IA Controls focus on confidentiality and integrity

## IA Control Subject Areas

Abbreviation	Subject Area Name	Number of Controls in Subject Area
DC	Security Design & Configuration	31
IA	Identification and Authentication	9
EC	Enclave and Computing Environment	48
EB	Enclave Boundary Defense	8
PE	Physical and Environmental	27
PR	Personnel	7
CO	Continuity	24
VI	Vulnerability and Incident Management	3

## Examples of Integrity IA Controls

- Identification and Authentication
  - IAKM-2 Key Management
    - Symmetric Keys are produced, controlled and distributed using NSA-approved key management technology and processes. Asymmetric Keys are produced, controlled, and distributed using DoD PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user's private key.
- Identification and Authentication
  - IATS-2 Token and Certificate Standards
    - Identification and authentication is accomplished using the DoD PKI Class 3 or 4 certificate and hardware security token (when available) or an NSA-certified product.

## Examples of Availability IA Controls

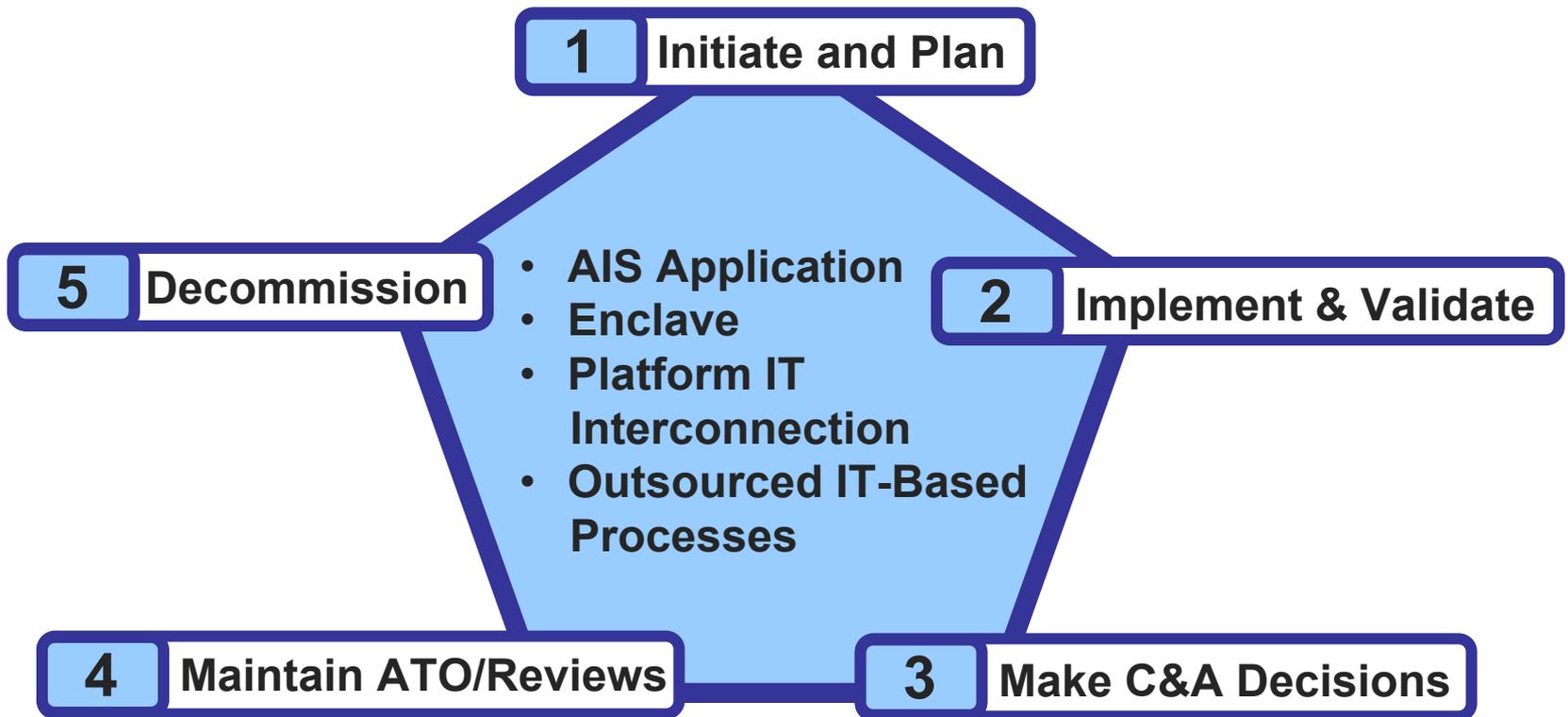
- Security Design and Configuration
  - DCAR-1 Procedural Review
    - An annual IA review is conducted that comprehensively evaluates existing policies and processes to ensure procedural consistency and to ensure that they fully support the goal of uninterrupted operations.
- Security Design and Configuration
  - DCSD-1 IA Documentation
    - All appointments to required IA roles are established in writing, to include assigned duties and appointment criteria such as training, security clearance, and IT-designation. A System Security Plan is established that describes the technical, administrative, and procedural IA program and policies that govern the DoD information system, and identifies all IA personnel and specific IA requirements and objectives.

[DoDI 8500.2]

## Examples of Confidentiality IA Controls

- Identification and Authentication
  - IAGA-1 Group Identification and Authentication
    - Group authenticators for application or network access may be used only in conjunction with an individual authenticator. Any use of group authenticators not based on the DoD PKI has been explicitly approved by the DAA.
- Security Design and Configuration
  - DCAS-1 Acquisition Standards
    - The acquisition of all IA- and IA-enabled GOTS IT products is limited to products that have been evaluated by the NSA or in accordance with NSA-approved processes. The acquisition of all IA- and IA-enabled COTS IT products is limited to products that have been evaluated or validated through one of the following sources – the International Common Criteria (CC), the NIAP Evaluation and Validation Program, or the FIPS validation program. Robustness requirements, the mission, and customer needs will enable an experienced information systems security engineer to recommend a Protection Profile, a particular evaluated product or a security target with the appropriate assurance requirements for a product to be submitted for evaluation.

# DIACAP Process



## DIACAP Phase 1 - Initiate and Plan

- Register System
- Assign IA Controls
- Assemble DIACAP Team
- Develop DIACAP Strategy
- Initiate IA Implementation Plan

# Enterprise Mission Assurance Support System (eMASS)

Welcome:

\*\*\*\*\* UNCLASSIFIED \*\*\*\*\*

**eMASS** Enterprise Mission Assurance Support System

Home Reports Workload Help Edit Profile Logout

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](#)

# Register the IA Program

McAnulty,John.P.5161530000

\*\*\*\*\* UNCLASSIFIED \*\*\*\*\*

e**MASS** Enterprise Mission Assurance Support System

Home Reports Workload Help Edit Profile Logout

## Certification & Accreditation

System Listing | New System Registration | **Resume Registration**

### Register System

1. Enter System Information	<b>2. Select Guidance Authority</b>	3. Select Additional Control Sets	4. Provide Additional Control Set Selection Criteria	5. Add Additional Control and/or Upgrade Assigned Controls	6. Set Inheritability	7. Assign Personnel	8. Review and Register
-----------------------------	-------------------------------------	-----------------------------------	--	--	-----------------------	---------------------	------------------------

### Guidance Authority

DoDI 8500.2

DoDI 8500.2

MAC

DoD Confidentiality

### Other Mandated Control Sets:

Security Notice | Privacy Statement | Accessibility Statement

Version 0.4.16

\*\*\*\*\* UNCLASSIFIED \*\*\*\*\*

# eMASS System Page

eMASS Enterprise Mission Assurance Support System

Home Reports Workload Help Edit Profile Logout

## Certification & Accreditation

System Listing New System Registration Resume Registration

### System Main Page

**CLOPS** Consolidated Logistics Operations Planning System **Organization:**  
**System Status:** Unaccredited/Pending  
**Revalidation Date:** 3/4/2006 **Type:** AIS Application  
**Package Classification:** Unclassified **System Classification:** Secret  
**Category:** Distribution  
**My Roles:**

Main Personnel Architecture System Info System Artifacts Package Review/History

- [-] CLOPS
  - [-] COAS-2
  - [-] COBR-1
  - [-] CODB-2
  - [-] CODP-2
  - [-] COEB-1
  - [-] COED-1
  - [-] COEF-2
  - [-] COMS-2
  - [-] COPS-2
  - [-] COSP-1
  - [-] COSW-1

IAM - Package → PM/SM → User Rep → CA → DAA

**Control Icon Key** Mandated M Upgraded U Added A

Acronym	Name	Subject Area	Control Set	Status
<span style="background-color: #cccccc; border: 1px solid black; padding: 0 2px;">M</span> <a href="#">COAS-2</a>	Alternate Site Designation	Continuity	DoDI 8500.2	Non-Compliant
<span style="background-color: #cccccc; border: 1px solid black; padding: 0 2px;">M</span> <a href="#">COBR-1</a>	Protection of Backup and Restoration Assets	Continuity	DoDI 8500.2	Non-Compliant
<span style="background-color: #cccccc; border: 1px solid black; padding: 0 2px;">M</span> <a href="#">CODB-2</a>	Data Backup Procedures	Continuity	DoDI 8500.2	Non-Compliant
<span style="background-color: #cccccc; border: 1px solid black; padding: 0 2px;">M</span> <a href="#">CODP-2</a>	Disaster and Recovery Planning	Continuity	DoDI 8500.2	Non-Compliant
<span style="background-color: #cccccc; border: 1px solid black; padding: 0 2px;">M</span> <a href="#">COEB-1</a>	Enclave Boundary Defense	Continuity	DoDI 8500.2	Non-Compliant

## DIACAP Phase 2 – Implement and Validate

- Execute and Update IA Implementation Plan
- Conduct Validation Activities
- Compile Validation Results
  - DIACAP Scorecard

# Validating IA Controls (IAKM-2 Key Management)

- **Production, Control, and Distribution of Asymmetric Keys**
  - **Validation Test:**
    - Review system documentation.
    - Ensure that asymmetric keys, if utilized, are produced, controlled, and distributed using appropriate DoD PKI assurance level certificates and hardware security tokens that protect the user's private key (i.e. CAC).
    - Record the results.
  - **Test Preparation:**
    - Obtain system documentation addressing the production, control, and distribution of asymmetric keys.
  - **Expected Results:**
    - Asymmetric keys utilize appropriate DoD PKI assurance level certificates and hardware security tokens.

# Validating IA Controls (IAKM-2 Key Management)

- **Symmetric Keys**

- **Test Script:**

- Review system documentation. Ensure that symmetric keys, if utilized, are produced, controlled and distributed using NSA-approved key management technology and processes.
    - Record the results.

- **Test Preparation:**

- Obtain system documentation addressing the production, control, and distribution of symmetric keys.

- **Expected Results:**

- Symmetric keys are produced, controlled, and distributed using NSA-approved key management technology and processes.

## 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

# e-Mass Digital Scorecard

\*\*\*\*\* SENSITIVE \*\*\*\*\*

**eMASS Enterprise Mission Assurance Support System** Home View Workload Help Edit Profile Log Out

**Certification and Accreditation Module**

**Returned Digital Score Card** [Download PDF Version](#)

**DRRS** Defense Readiness Reporting System    Organization: OSD    System Status: ATO    Revalidation Date: 15 Jul 04  
System Type: Enclave    System Category: Infrastructure    System Classification: Confidential

**ATO Granted**    This DoD information system is authorized to conduct full operations at a specified MAC and confidentiality level.  
14 Sep 04: by DLA    There is no residual risk, or there is an acceptable risk without operational restrictions.

DoDI 8500.2 Subject Area	Control Acronym	DoDI 8500.2 Controls	Compliant/ Noncompliant	Comment	Severity Code (H,M,L)
Security Design and Configuration	DCAR-1	Procedural Review	Compliant		
	DCBP-1	Best Security Practices	Compliant		
	DCCB-2	Control Board	Compliant		
	DCCS-2	Configuration and Specifications	Compliant		
	DCCT-1	Compliance Testing	Compliant		
	DCDS-1	Dedicated IA Services	Compliant		
Identification and Authentication	IAKM-2	Key Management	Compliant		
	IATS-2	Token and Certificate Standards	Compliant		
Enclave and Computing Environment	ECAT-2	Audit Trail, Monitoring, Analysis and Reporting	Compliant		
	ECCD-2	Changes to Data	Compliant		

\*\*\*\*\* SENSITIVE \*\*\*\*\*

Privacy Statement | Accessibility | Security Notice

## DIACAP Phase 3 – Make C&A Decisions

- Analyze Residual Risk
- Issue Certification Determination
- Make Accreditation Decision

## Analyze Residual Risk

- Conducted by the IAM or CA
- Residual risk describes the risk remaining after risk mitigation has occurred (i.e., application of countermeasures, security controls, or the implementation of corrective actions).
- IAM assesses residual risk to the DoD Component information environment, to the information exposed to the DoD information system, and to the mission being supported by the DoD information system
- IAM/CA makes certification accreditation recommendations to the DAA

## Accreditation Decisions

- Approval to Operate (ATO)
  - Authorization of a DoD information system to process, store, or transmit information, granted by a DAA. Authorization is based on an acceptable IA design and implementation of assigned IA Controls.
- Interim Approval to Operate (IATO)
  - Temporary approval granted by a DAA to operate based on an assessment of the implementation status of the assigned IA Controls.
- Interim Approval to Test (IATT)
  - Temporary approval granted by a DAA to conduct system testing based on an assessment of the implementation status of the assigned IA Controls.
- Denial of Approval to Operate (DATO)
  - A DAA determination that a DoD information system cannot operate because of an inadequate IA design or failure to implement assigned IA Controls.

## Example Contents of DIACAP Package

- 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

## DIACAP Phase 4 – Maintain ATO/Reviews

- Initiate and Update Lifecycle Implementation Plan for IA Controls
- Maintain Situational Awareness
- Maintain IA Posture

## Types of Phase 4 Activities

- Exercise configuration management of IA Controls Implementation Plan for operational system, which permits IT component swaps and minor software releases
- Incorporate newly assigned or modified IA Controls into IA Implementation Plan, or corrections of other identified security vulnerabilities
- Update DIACAP Package and IA Controls Scorecard
- Conduct IA monitoring as specified in the IA Implementation Plan
- Conduct assigned / scheduled vulnerability scans and penetration tests
- Re-verify identified IA Controls
- Validate continued IA Controls compliance and IA Controls Scorecard

## DIACAP Phase 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

## Summary

- DIACAP implements DoD 8500 Series
- DIACAP intended to support the GIG
- DIACAP not signed-off yet
  - Possibly the end of June
- e-Mass pilot not completed
  - Limited initial pilot participants
- e-Mass intends to incorporate DCID 6/3 and NIST SP 800-37/53 controls later this year
- Requires an attitude change toward C&A
- Requires a DAA paradigm shift in terms of access controls
- Need buy-in from other GIG organizations

s j d d  
j d j s  
d C & A  
: M #  
s i z x  
^ z s n  
: M A x  
\ d c A  
F I P S  
i % d k  
o ; o A  
n e f o  
W J E j  
% C l m  
o J d N  
g C C u  
A D < x  
\* j d j  
W J E j  
% C l m  
o D < N  
g J d u  
x P K I  
\* j d j  
o A S :  
Q P a f  
o o J \  
: o j i  
s A c n  
N I A P  
J E j D  
C l m L  
D < N o  
J d u ?  
f % # p  
j d j s  
d f % #  
# % # d

# References

## References

[44 USC 3542]	<u>Public Printing and Documents</u> , Chapter 35 “Coordination of Federal Information Policy”, Subchapter III “Information Security”. U.S. Code 44, Section 3502. Washington, DC: U.S. Congress, 2005.
[DIACAP KB]	<u>DIACAP Knowledge Base Overview</u> . Briefing. Washington, DC: DoD PKI C&A Working Group, March 2005.
[DoD 5220.22-M]	<u>National Industrial Security Program Operating Manual</u> (NISPOM). DoD 5220.22. Washington, DC: U.S. Department of Defense, 1995.
[DoDI 5000.2]	<u>Operation of the Defense Acquisition System</u> . DoDI 5000.2. Washington, DC: U.S. Department of Defense, 2003.
[DoDD 8500.1]	<u>Information Assurance</u> . DoD Directive 8500.1. Washington, DC: U.S. Department of Defense, 2002.
[DoDI 8500.2]	<u>Information Assurance Implementation</u> . DoD Instruction 8500.2. Washington, DC: U.S. Department of Defense, 2003.
[DoDI 8510.bb]	<u>Defense Information Assurance Certification and Accreditation Process</u> (DIACAP). DoD Instruction 8510.bb. Washington, DC: U.S. Department of Defense, draft 2005.

# References

[DoD 8510.b-M]	<u>Defense Information Assurance Certification and Accreditation Process (DIACAP) Manual Draft Annotated Outline</u> . DoD 8510.b-M. Washington, DC: U.S. Department of Defense, draft 2005.
[DoD Acquisition Guidebook]	<u>DoD Acquisition Guidebook</u> . Washington, DC: U.S. Department of Defense, 2004.
[eMASS]	<u>eMASS Overview</u> . Briefing. Washington, DC: DoD PKI C&A Working Group, March 2005.
[FIPS 199]	<u>Standards for Security Categorization of Federal Information and Information Systems</u> . FIPS 199. Washington, DC: U.S. National Institute of Standards and Technology, 2003.
[FISMA, 2002]	<u>Federal Information Security Management Act (FISMA)</u> . Washington, DC: U.S. Congress, 2002.
[GiG IA, 2004]	<u>GIG IA Strategy (Draft)</u> . Fort Meade, MD: National Security Agency (NSA) Information Assurance Directorate, June 2004.
[OMB A130, 1996]	<u>Management of Federal Information Resources</u> . Washington, DC: U.S. Office of Management and Budget (OMB), 8 February 1996.