DIACAP Presentation

Presented by: Dennis Bailey

Date: July, 2007

Government C&A Models

- NIST SP 800-37 - Guide for the Security Certification and Accreditation of Federal Information Systems

- NIACAP - National Information Assurance Certification and Accreditation Process
  - Based on a process published by the Committee on National Security Systems (CNSS) documented in the National Security Telecommunications and Information System Security Instructions,1 otherwise known as NSTISSI No. 1000

  - Used for C&A of national security systems which are systems determined to be either “Top Secret,” “Secret,” or “Confidential” under Executive order 12958

Government C&A Models (continued)

- DCID 6/3 - Director of Central Intelligence Directive
  - 6/3 refers to the process described in section 6, part 3 of the Director of Central Intelligence Directives
  - For systems that require that anyone working on them to have a Top Secret, Sensitive Compartmentalized Information (SCI) clearance
- DITSCAP - DoD Information Technology Security Certification and Accreditation Process
  - Introduced in 1997 with 5200.40 directive for DoD systems
- DIACAP - DoD Information Assurance Certification and Accreditation Process (DIACAP)
  - Introduced on July 6, 2006 to replace DITSCAP

Introduction to DITSCAP

Phases of DITSCAP (DoD Information Technology Security Certification and Accreditation Process)

- Phase 1 - Definition
  - SSAA – System Security Authorization Agreement
- Phase 2 - Verification
  - 1. System architecture analysis.
  - 2. Software design analysis.
  - 3. Network connection rule compliance analysis.
  - 4. Integrity analysis of integrated products.
  - 5. Life-cycle management analysis.
    - 1. Computer Resource Management Plan (CRMP).
    - 2. Computer Resources Life-Cycle Management Plan (CRLCMP).
    - 3. Configuration identification procedures.
    - 4. Configuration control procedures.
    - 5. Configuration status accounting procedures.
    - 6. Configuration audit procedures and reports.
    - 7. Software engineering (development approach and engineering environment) procedures.
    - 8. Trusted distribution plans.
    - 9. Contingency, continuity of operations, and back-up plans.
  - 6. Vulnerability assessment.

Introduction to DITSCAP (Continued)

- Validation
  - 1. Security Test and Evaluation.
  - 2. Penetration testing.
  - 3. TEMPEST and Red-Black verification.
  - 4. Validation of COMSEC compliance.
  - 5. System management analysis.
  - 6. Site accreditation survey.
  - 7. Contingency plan evaluation.
  - 8. Risk-based management review.

- Post-Accreditation

Introduction to DIACAP

- DIACAP is the Department of Defense Information Assurance Certification and Accreditation Process.
- It was introduced by a Defense Department directive on July 6, 2006.
- Interim guidance was issued and the official 8510.bb document is waiting to be signed.
- Replaces DITSCAP, the C&A process since 1997.
- Regulatory policy is based on the 8500 series documents and FISMA.
- Transition requirements – 180 days to prepare a plan and accreditation before 3 year expiration of DITSCAP C&A.

Background on DIACAP

- DoD wanted to modernize their IA programs with the following goals in mind:
  - Streamline C&A processes
  - Compatibility with DoD's vision of net-centric operations and the Global Information Grid (GIG)
  - Compliance with the Federal Information Security Management Act of 2002 (FISMA)
  - Utilization of a C&A solution that considers shared risks

Net-Centric

- Data are visible, accessible and understandable when and where needed to accelerate decision making
- Tagging of all data with meta data to enable discovery by users
- All data is posted to shared spaces for users to access except when limited by security, policy or regulations.
- Emphasis on many-to-many sharing between COIs (Communities of Interest)
- A philosophy of enabling information sharing across the GIG (Global Information Grid)

Global Information Grid (GIG)

- Seamless and secure end-to-end IA architecture utilizing shared services
- Less focus on individual systems and more on enclaves
- Empowers the user with ability to access all relevant info and recognizes user as an information source
- Supports formation of dynamic communities of interest (COIs)
- Shift in approach from need to know to need to share

C&A on the GIG

- DIACAP supports the GIG through:
  - Focused on assurance for shared systems and not stove-piped systems.
  - Inheritance – the sharing of security controls, validation results and C&A status across systems and networks.
  - Putting C&A information for every system online and using that information as a part of accreditation decisions.
  - Takes accreditation decisions to the component and mission level.

Components

- The DIACAP program is composed of three parts:
  - DIACAP Knowledge Service (KS)
  - Enterprise Mission Assurance Support Service (eMass)
  - C&A Processes

DIACAP Knowledge Service (KS)

- Tools such as current C&A guidelines, diagrams, process maps and documents
- Community forum to interact with users
- Implementation guidance and assessment procedures for each control

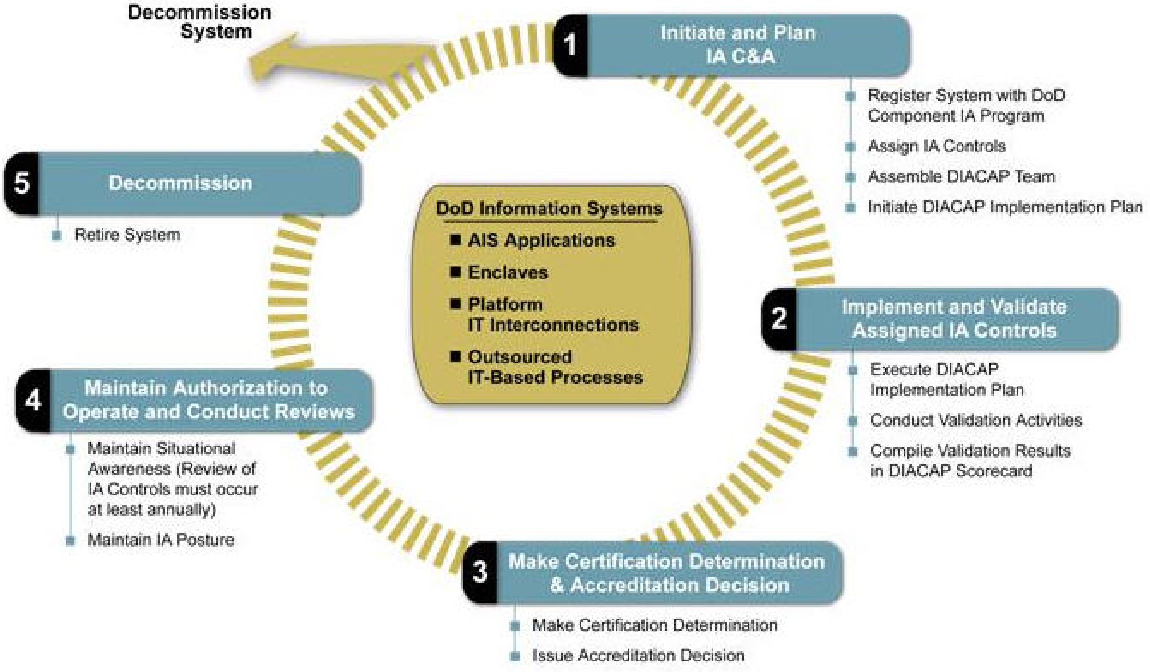
Enterprise Mission Assurance Support Services (eMass)

- Systems are registered using a System Identification Profile (SIP)
- Creates a C&A package for the management of each registered system
- Includes workflow and scheduling of activities
- Assignment and tracking of controls
- PKI used to audit transactions
- Scalable to any enterprise
- Developed by BAH

C&A Process

- The DIACAP process is composed of five phases:

THE 5 DIACAP ACTIVITIES



Decommission System

1 Initiate and Plan IA C&A

- Register System with DoD Component IA Program
- Assign IA Controls
- Assemble DIACAP Team
- Initiate DIACAP Implementation Plan

2 Implement and Validate Assigned IA Controls

- Execute DIACAP Implementation Plan
- Conduct Validation Activities
- Compile Validation Results in DIACAP Scorecard

3 Make Certification Determination & Accreditation Decision

- Make Certification Determination
- Issue Accreditation Decision

4 Maintain Authorization to Operate and Conduct Reviews

- Maintain Situational Awareness (Review of IA Controls must occur at least annually)
- Maintain IA Posture

5 Decommission

- Retire System

DoD Information Systems

- ■ AIS Applications
- ■ Enclaves
- ■ Platform IT Interconnections
- ■ Outsourced IT-Based Processes

© Electrosoft, 2007

Roles & Responsibilities

- Designated Accrediting Authority (DAA)
- Program or System Manager (PM or SM)
- Information Assurance Managers (IAM)
- Certifying Authority (CA)
- Principal Accrediting Authority (PAA)
- Senior Information Assurance Officer (SIAO)
- User Representative (UR)

System Identification Profile (SIP)

- Formal System Registration
- Describes Mission and System
- Specifies DIACAP Team
- Determination of Mission Assurance Categories and Confidentiality Level

Mission Assurance Categories (MACs)

- Reflects the importance of information relative to the achievement of DoD goals and objectives, especially concerning combat missions.
  - MAC I: Information that is determined to be vital to the operation readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness
  - MAC II: Information that is important to the support of deployed and contingency forces.
  - MAC III: Information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short term

Mission Assurance Categories (MACs)

- Each MAC level has required levels of integrity and availability
  - MAC I - High Integrity, High Availability
  - MAC II - High Integrity, Medium Availability
  - MAC III - Basic Integrity, Basic Availability

Confidentiality Level (CL)

- The Confidentiality Level (CL) measures a system's confidentiality requirements based on whether the system processes classified, sensitive or public information.
  - Classified
  - Sensitive
  - Public

Baseline Assurance Levels

- The nine combinations of MAC and CL establish nine baseline IA levels within the GIG

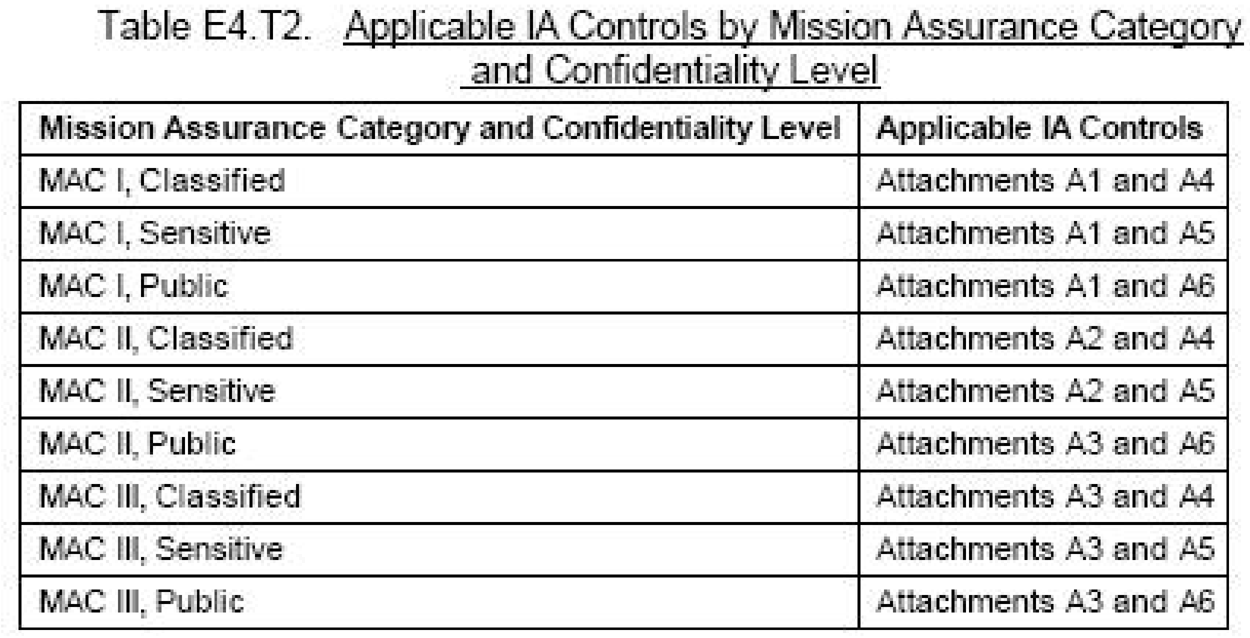


Table E4.T2. Applicable IA Controls by Mission Assurance Category and Confidentiality Level

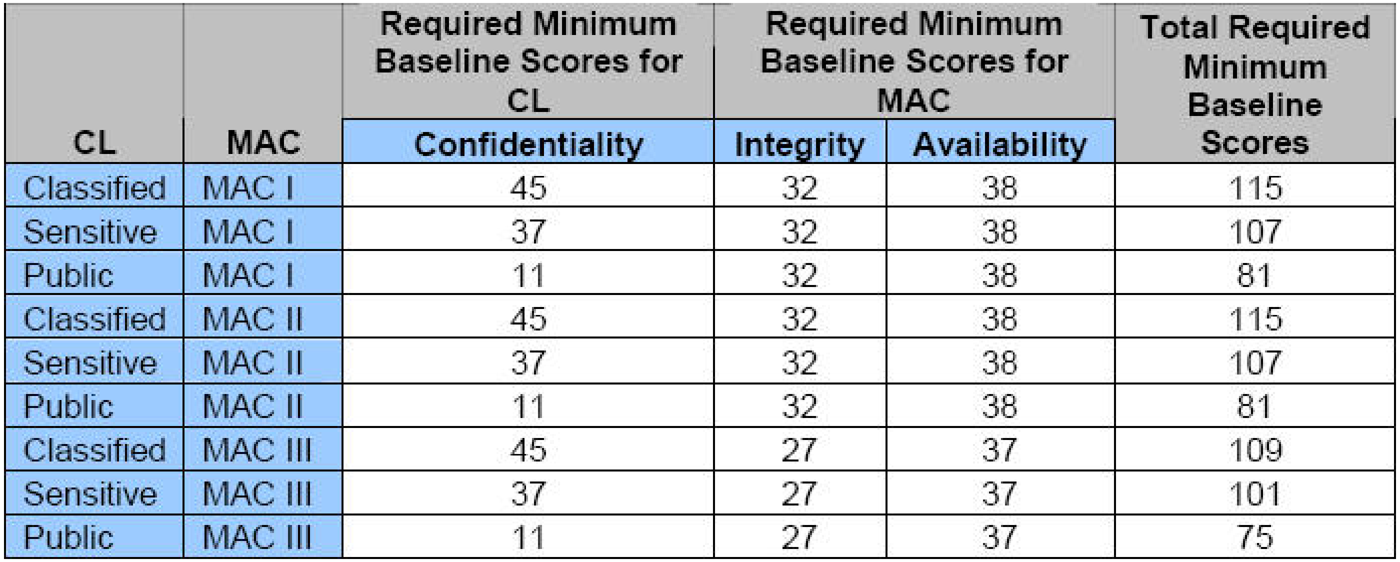
Mission Assurance Category and Confidentiality Level	Applicable IA Controls
MAC I, Classified	Attachments A1 and A4
MAC I, Sensitive	Attachments A1 and A5
MAC I, Public	Attachments A1 and A6
MAC II, Classified	Attachments A2 and A4
MAC II, Sensitive	Attachments A2 and A5
MAC II, Public	Attachments A3 and A6
MAC III, Classified	Attachments A3 and A4
MAC III, Sensitive	Attachments A3 and A5
MAC III, Public	Attachments A3 and A6

IA Control Subject Areas

- DoD 8500.2 (Information Assurance Implementation) Enclosure 4
  - DC - Security Design & Configuration
  - IA - Identification and Authentication
  - EC - Enclave & Computing Environment
  - EB - Enclave Boundary Defense
  - PE - Physical & Environmental
  - PR - Personal
  - CO - Continuity
  - VI - Vulnerability & Incident Management

Minimum Score

- Each system has to get a required minimum number of points in the IA categories of Confidentiality, Availability and Integrity



		Required Minimum Baseline Scores for CL	Required Minimum Baseline Scores for MAC		Total Required Minimum Baseline Scores
CL	MAC	Confidentiality	Integrity	Availability	
Classified	MAC I	45	32	38	115
Sensitive	MAC I	37	32	38	107
Public	MAC I	11	32	38	81
Classified	MAC II	45	32	38	115
Sensitive	MAC II	37	32	38	107
Public	MAC II	11	32	38	81
Classified	MAC III	45	27	37	109
Sensitive	MAC III	37	27	37	101
Public	MAC III	11	27	37	75

Scorecard

- The Scorecard shows the certification and accreditation status of a system in a concise format
  - Specific Controls Required
  - Number of Compliant/Non-compliant Areas
  - Assessed Risk Status of Each Non-compliant area
  - Accreditation decision

Accreditation Package

- System Identification Profile
  - Implementation Plan
  - IA Controls – Inherited and implemented
  - Implementation Status
  - Responsible entities
  - Resources
  - Estimated completion date for each IA Control
- Supporting Documentation for Certification
  - Actual Validation Results
  - Artifacts associated with implementation of IA Controls
- DIACAP Scorecard
  - • Certification determination
  - • Accreditation Determination
- POA&M (If required)

Accreditation Decisions

- Authorization to Operate (ATO) – 3 years with annual reviews.
- Interim Authorization to Operate (IATO) – 180 days, no more than 2 in a row.
- Interim Authorization to Test (IATT) – Special testing of operational system or with live data.
- Denial of Authorization to Operate (DATO) - POA&M required to address issues.