



DIACAP REQUIREMENTS

27 October 2009

**Fabiola Navarro
AUSGAR Technologies
619.822.2968 x 109
fnavarro@ausgar.com**

UNCLASSIFIED

DIACAP

Congressional & DoD Requirements

DoDI 8510.01 – DoD Information Assurance Certification and Accreditation Process (DIACAP), 28 Nov 2007

- Federal Information Security Management Act (FISMA) of 2002, 17 Dec 2002
- DoDD 8100.1 – Global Information Grid (GiG) Overarching Policy, 19 Sep 2002
- DoDD 8500.01E – Information Assurance (IA) Implementation, 24 Oct 2002
- DoDI 8500.2 – IA Implementation, 6 Feb 2002

DIACAP Objectives

Protects and defends the Global Information Grid (GiG) by:

- Provide a standard DoD Certification and Accreditation (C&A) approach
- Manage and disseminating enterprise standards and guidelines for IA:
 - Design
 - Implementation
 - Configuration
 - Validation
 - Operational sustainment
 - Reporting
- Apply to all DoD-controlled Information Systems (ISs)
- Facilitate a dynamic environment
- Manage an IA posture across the DoD Information Systems life cycle

DIACAP Introduction

DODI 8510.01 (DIACAP)

- Network-centric versus System-focused C&A solution
 - Net-centric, information belongs to the enterprise, shared risks
- Authority and responsibility for certification are vested in the Senior IA Officer (SIAO)
- Supersedes DoD Information Technology Security Certification & Accreditation Process (DITSCAP), DoD Instruction (DoDI) 5200.40
 - Platform-centric, information belongs to system owner, system specific risks
 - Designated Accrediting Authority (DAA) appointed Certification Authority (CA)

DIACAP Introduction (cont)

Focus on overall security posture via IA controls compliance

- Baseline IA Controls address enterprise-wide threats and vulnerabilities
- Mission Assurance Category (MAC) & Confidentiality levels determine IA Controls

Applicability examples include:

- IS under contract to DoD
- Prototypes
- Joint Concept Technology Demos (JCTD)
- Stand-Alone IS
- Mobile Computing devices, wired or wireless

IA Controls - Integrity, Availability, Confidentiality

IA Controls (IACs) Characteristics

- Testable
- Measurable
- Assignable
- Accountable
- Repeatable

Inheritance

- Child system inherits IACs from Parent system/site
- Allows sharing of IA controls:
 - Validation & Compliance Status
- Eliminates duplication of testing and documentation

Severity and Impact codes

- Determine risk level associated with the security weakness
- Urgency which corrective actions must take place

DIACAP Service Level Team

Designated Accrediting Authority (DAA)

- Accredits Information Systems

Certification Authority (CA)

- Certifies Information System

Certification Authority Representative (CA Rep)

- Appointed and acting on behalf of the CA

Chief Information Office (CIO)

- Ensures IACs are implemented and C&A status is visible

Component SIAO

- Enforces component C&A process and tracks C&A status

DIACAP Program Level Team

Program Manager (PM) or System Manager (SM)

- Responsible for implementing the DIACAP for assigned DoD IS

Validator / Certification Agent

- Entity responsible for conducting validation procedure

Information Assurance Manager (IAM)

- Responsible for IA program and supports DIACAP implementation

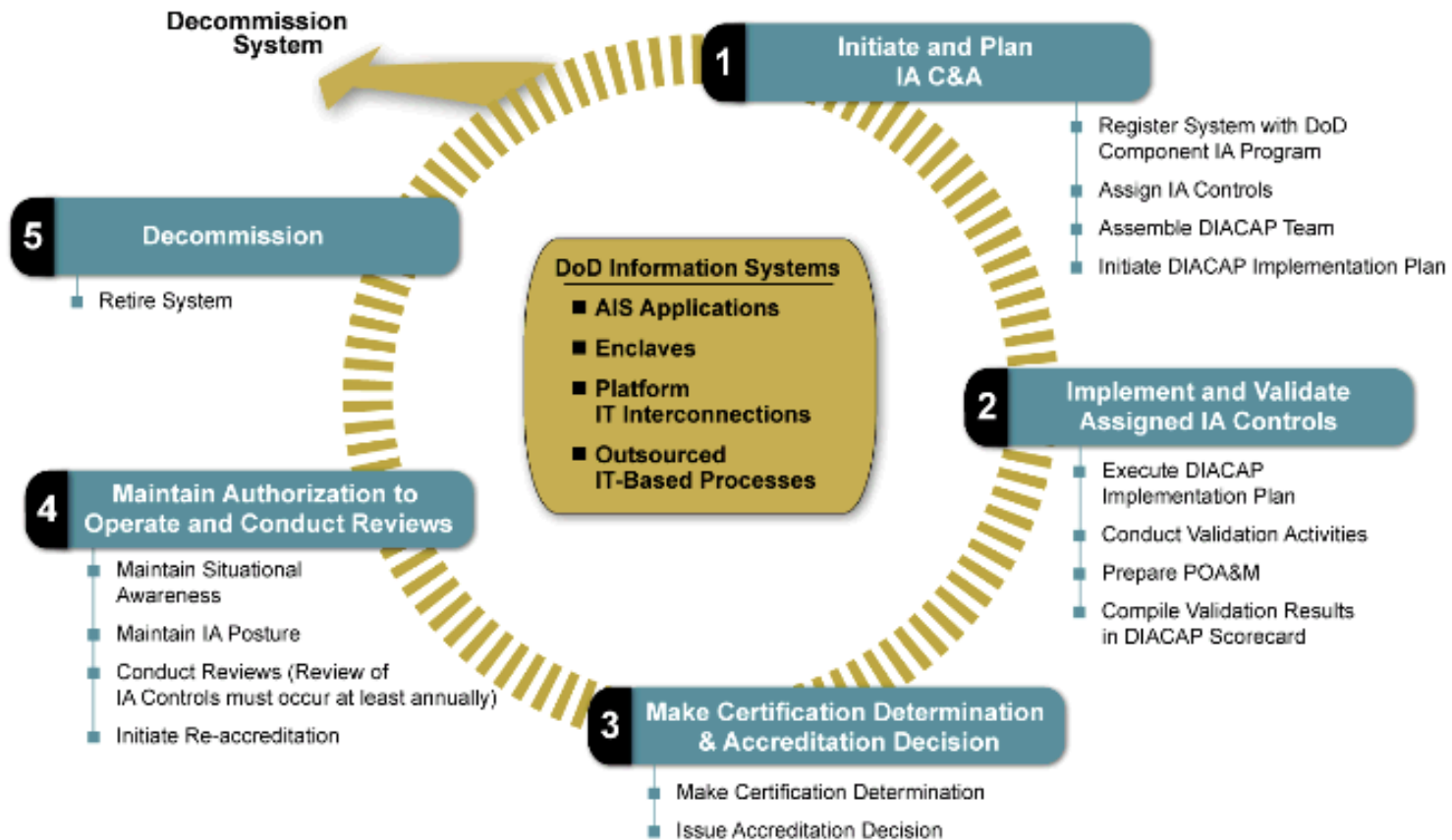
Information Assurance Officer (IAO)

- Ensures appropriate IA posture is maintained

User Representative (UR)

- An individual or organization that represents the user community for a particular system for DIACAP purposes

DIACAP Activities



Information Assurance Roadmap

DIACAP Activities:



JCIDS



Pre-Concept Refinement

Concept Refinement

Technology Development

System Development & Demonstration

Production & Deployment

Operations & Support

Shutdown & Phase Out



Conceptual Design & Advanced Planning

Preliminary System Design

Detailed Design & Development

Production and/or construction

Operational Use & System Support



DIACAP Package

Generated through DIACAP activity implementation

- System Identification Profile (SIP)
- DIACAP Implementation Plan (DIP)
- IT Security POA&M
- Supporting Certification Documentation
 - Validation results
 - Artifacts
- DIACAP Scorecard
 - Certification determination
 - Accreditation decision

DIACAP DoD Service Components

Navy C&A

- OPNAVINST 5239.1B, Navy Information Assurance (IA) Program
- DoN IA Pub 5239 Series
- DoN DITSCAP to DIACAP Transition Handbook, 9 June, 2008 ver 1.1
- The DAA is centralized, NETWARCOM
- Certification Authority (CA) is centralized
- Navy CA vets a list of DIACAP validators (**qualified certification agents**) and CA reviewers perform CA Liaison role

ARMY C&A

- AR 25-2, Information Assurance, 23 March 2009
- C&A Best Business Practices
- The DAA is decentralized, and is appointed by the CIO/G-6 at the General Officer, SES level upon nomination (i.e. 200+ DAAs)
- Certification Authority (CA) is centralized in the Army Senior Information Assurance Officer (SIAO) organization
- Army CA vets a list of qualified government organizations and labs as trusted Agents of the CA to perform the functions as the 3rd party independent validator

Marine Corps C&A

- USMC Enterprise IA Directive, Sep 08
- USMC follows DoN DITSCAP Handbook and the DoN DITSCAP to DIACAP transition guide
- Three (3) DAAs
 - Operational DAA, Marine Corps Enterprise Network (MCEN) DAA
 - Developmental DDAs
 - Marine Corps Systems Command (MARCORSYSCOM)
 - Marine Corps Tactical Systems Support Activity (MCTSSA)
- Centralized CA
 - SYSCOM Certifier, assigned by Marine Corps SIAO

Air Force C&A

- AF Policy Directive (AFPD) 33-2, IA Programs
- Three (3) Accrediting Authorities:
 - The Air Force DAA (AF-DAA) for the AF-GIG (including approval of all connections to the AF-GIG), and all AF ISs
 - The SAP/SAR DAA is the lead DAA for all AF SAP/SAR systems
 - Lead DAA for all AF Space Systems
- Centralized CA
- Agent of the Certifying Authority (ACA)
 - Require licensing approval from AF SIAO

C&A Reciprocity

- DoD Information System C&A Reciprocity Memo, 23 July 2009

Reciprocity defined as “mutual agreement among participating enterprises to accept each other’s security assessments in order to reuse IS resources and/or accept each other’s assessed security posture in order to share information.”

1. Establishes the security terms and conditions for fostering reciprocity when a DoD IS is deployed as an enterprise solution or Enterprise IS
2. DoD Components deploying Non-Enterprise ISs

- Defense Information System Network/ Global Information Grid (DISN/ GIG) Flag Panel responsibilities to assess DoD Information Enterprise risk, authorize information exchanges and DoD Information Enterprise connections for ISs IAW DoD Instruction 8510.01

Impact if not compliant

- Cost
- Schedule
- Performance
- Denial to connect (e.g. DATO)



Contact Information

Senior Information Assurance Engineers

- Suzana Meszaros (smeszaros@ausgar.com)
- Caterina Brott (cbrott@ausgar.com)
- Cale Dansbee (cdansbee@ausgar.com)

Corporate Office (619) 822-2968