

**Introduction to DIACAP for  
Certification and Accreditation  
Practitioners**



**Transition from DITSCAP to DIACAP and  
New Roles for C&A Teams**

# Agenda

---

- **From DITSCAP to DIACAP**
- C&A and the Grid
- DIACAP Structure
- Completing the Process
- The Scorecard
- Determinations and Decisions



# Previously...

- FISMA (Title III of the eGovernment Act)
- Global Information Grid (GIG 8100.1)
- Net-centricity (DoD Directive 8320.2)
- 8500 Requirements for IA Programs



DIACAP will reinforce all of these

# C&A Direction...

---

- DITSCAP
  - 5200.40 – DITSCAP Direction (January 1997)
  - 8510.10-M Application Manual (July 2000)
- DITSCAP addressed system security in a vacuum, asking C&A personnel to evaluate risk for single systems.
- DIACAP is not a new version of DITSCAP

# FISMA

---

## Federal Information Security Management Act Public Law 107-347 (E-Government Act)

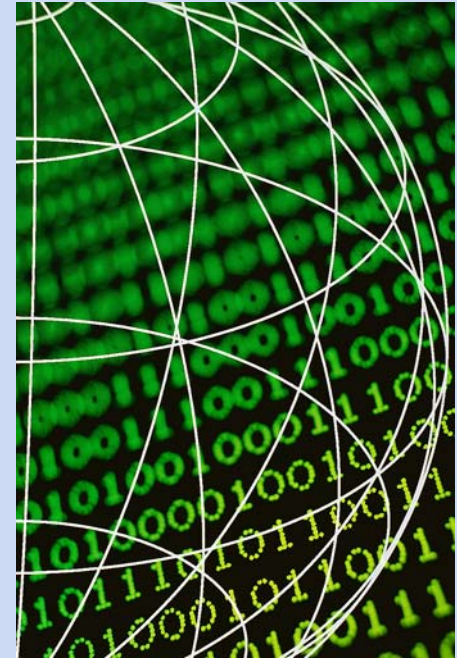


- Requirement to establish organization-wide security programs
- Annual assessments and reporting

# Agenda



- From DITSCAP to DIACAP
- **C&A and the Grid**
- DIACAP Structure
- Completing the Process
- The Scorecard
- Determinations and Decisions



# Need for New C&A System

---

- Inter-connected enterprise requires a C&A solution that considers shared risks
- Number of systems made DITSCAP SSAA packages an overwhelming burden
- C&A becoming an impediment to new technology and project roll-outs to support the GIG/net-centric world



# Net-centricity

---

- Focus on information *sharing*
  - The goal of Net Centric Enterprise Services is to make data available in a secure manner
  - Dependable network infrastructure is a key component
- Data must be *retrievable*
  - Tags/Metadata
  - Classification system must be universal



# The GIG

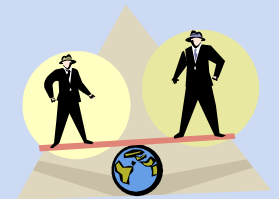


- Global Information Grid
  - Replaces the concept of individual systems with the “net-centric” system
  - No more standalone/stovepipe programs
- Service-based
  - Service Assurance a key component
  - System/Network Availability, Information Protection, & Information Delivery



# GIG Requirements for C&A

- Establish an IT “Enterprise” scheme for certifying and accrediting systems
  - DoD-wide database of certification plans
  - Accreditation status is available to community
- Component-wide standards
  - Shared Risk = Shared Risk Assessment Program
  - Training for each DAA, CA, Tester, etc.



# C&A's Importance in the GIG

---

- C&A is the process by which the assurance of security is verified
- The interconnection of all systems (GIG) makes C&A even more vital to the health of the DoD



# C&A's Responsibility



- Become part of the collaborative environment of the GIG
  - Contribute to and learn from the experiences of other programs
  - Provide true lifecycle support to projects
- Enforcing uniform, component-wide standards for IA

# Agenda

---

- From DITSCAP to DIACAP
- C&A and the Grid
- **DIACAP Structure**
- Completing the Process
- The Scorecard
- Determinations and Decisions



# DIACAP Governance



## Who's in charge?

- DISA
- DLA
- NSA
- OSD CIO
- OSD AT&L
- Components

Each group has a role to play in the GIG and has varying degrees of power over the future of DIACAP



# DIACAP Guidelines

---

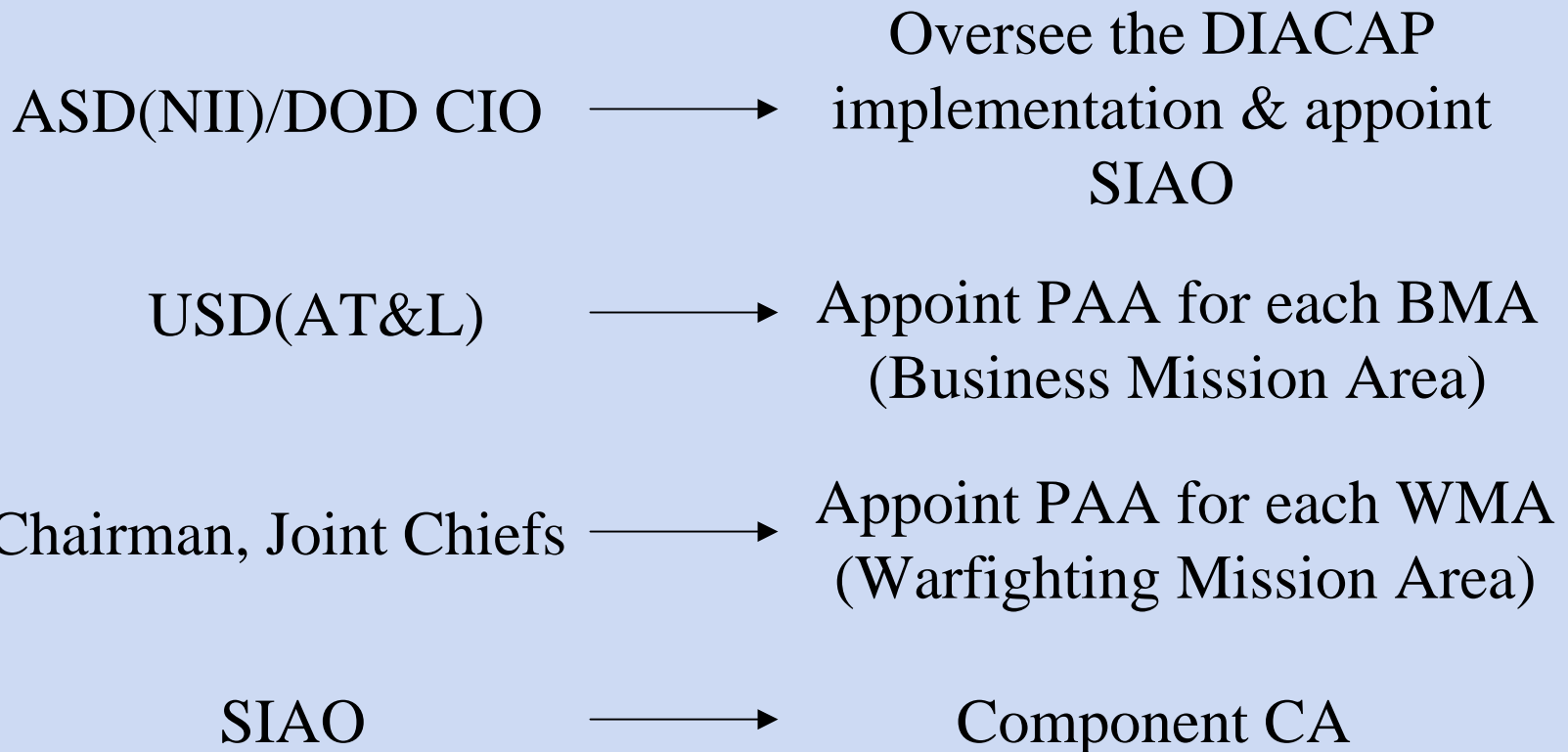
Director, DISA → Develop DIACAP training, awareness, guidance, etc.

Director, NSA → Develop GIG documentation for DIACAP

Component Directors → Establish component-wide standards for C&A

# DIACAP Responsibilities

---



# Accreditation Responsibilities

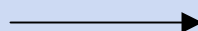


PAA



Component Accreditation  
Decisions

Component  
Heads



Appoint DAAs, take  
responsibility for all  
connected systems ATO  
status



DAA



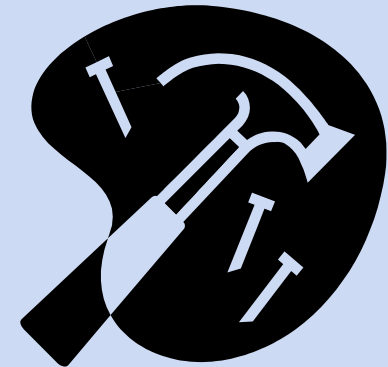
Accreditation Decisions  
for Component Subset



# Agenda

---

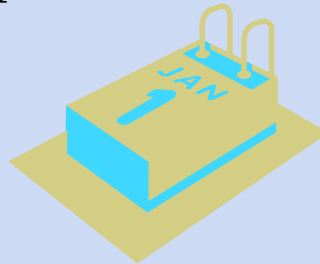
- From DITSCAP to DIACAP
- C&A and the Grid
- DIACAP Structure
- **Completing the Process**
- The Scorecard
- Determinations and Decisions



# Phase Description

---

Unlike the distinct steps of the DITSCAP, the iterative nature of DIACAP melds into a “lifecycle” support scheme very well



Re-assessment of security posture/compliance and ATO status no less than once per year

# DIACAP Phases

PHASE	PROCEDURE	PHASE #
Initiate & Plan	Register System with DoD Component	1
	Assign IA Controls	
	Assemble DIACAP Team	
	Review DIACAP Intent	
	Initiate Implementation Plan	
Implement & Validate	Execute and Update IA Implementation Plan	2
	Conduct Validation Activities	
	Compile Validation Results	
Make C&A Decisions	Analyze Residual Risk	3
	Issue Certification Determination	
	Make Accreditation Decisions	
Maintain ATO/Reviews	Lifecycle Implementation Begins	4
	Plan for IA Controls	
	Maintain Situational Awareness	
	Maintain IA Posture	
Decommission	Disposition of DIACAP Data	5

# DIACAP “Product”

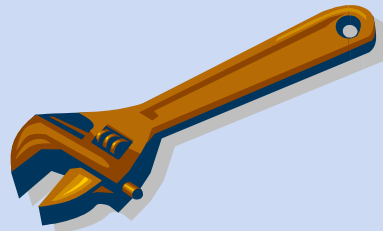
---

- No requirement for an SSAA any longer
- Packages are streamlined compared to DITSCAP packages
- Central certification document is the DIACAP Scorecard
  - Identifies requirements based on MAC/CL
  - Displays deficiencies in terms of security controls

# DIACAP Tools

---

DIACAP Packages are created with the help of:



Knowledge Service (KS) – web-based database of C&A efforts, DoD-wide

Enterprise Mission Assurance Support System (eMASS) – automates management functions

# KS

- Provides DIACAP process information
  - Implementation Guides
  - Generic Forms/Templates
- C&A News
  - Updates to controls
  - Central point for process data dissemination



# eMASS



- Aids document production
  - Automates status reporting, workflows, artifact creation
  - Security control look-up
- Acts as storehouse for infrastructure documents
  - Tracks all enterprise systems
  - Links C&A efforts across organization



# DIACAP Executive Package



## Minimum information for accreditation decision

- System Identification Profile
- Scorecard
- Certification Determination
- POA&M
- Accreditation Decision



# Comprehensive Package

---

## Comprehensive Package

- System Identification Profile
- DIACAP Strategy
- Implementation Plan
  - Security Control Requirements
  - Relevant Artifacts, Validation Procedures, etc.
- Scorecard
- Certification Determination & Artifacts
- POA&M
- Accreditation Decision



# System Identification Profile (SIP)

---

- Initial product of the DIACAP
- Describes Mission and System for Review
- Specifies DIACAP Team
- Formal System Registration
- Determination of MAC and CL



# Implementation Plan

---

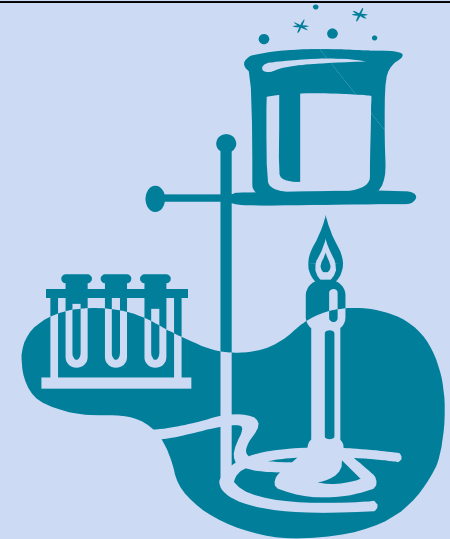
- Relevant Security Controls
- Lifecycle Analysis
- Configuration Description



Once the Implementation Plan is set, its execution kicks off the Validation Process.

# Validation & POA&M

- System Tests/Test Plan
- Validation Results
- POA&M with discrepancies

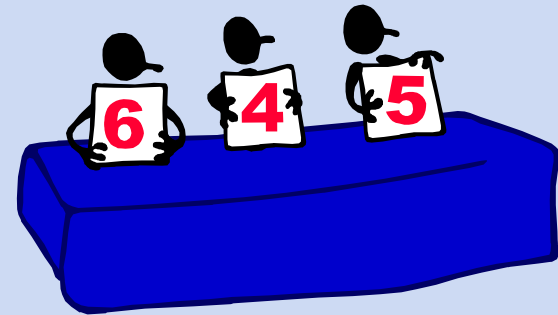


Note that these are completed prior to the formal Scorecard creation.

# Agenda

---

- From DITSCAP to DIACAP
- C&A and the Grid
- DIACAP Structure
- Completing the Process
- **The Scorecard**
- Determinations and Decisions



# DIACAP Scorecard



The Scorecard shows the certification status of a system in a concise format

Displays:

- Number of Controls Required
- Number of Compliant/Non-compliant Areas
- Assessed Risk Status of Each Non-compliant area



# Mission Assurance Category



MAC level determination remains unchanged

- MAC = importance of data relative to meeting system's objectives
- MAC translates into the Integrity & Availability requirement for the system

MAC	Availability	Integrity
I	High	High
II	Medium	High
III	Basic	Basic



# Confidentiality Level



- CL represents the degree of protection data requires to prevent unauthorized access
- CL is independent of MAC (and vice versa)

<b>CL</b>	<b>Confidentiality</b>
<b>Classified</b>	<b>High</b>
<b>Sensitive</b>	<b>Medium</b>
<b>Public</b>	<b>Basic</b>



# MAC & CL in Context

Required Controls (8500) Defined by the MAC & CL of the system under review:

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

# Scorecard Example - Overview



## Compliance Audit

- Items Assessed (and note on procedures)
- Controls Out of Compliance (listed individually)

## Risk Assessment

- List of Non-compliant Controls
- Indication of Risk (High, Medium, & Low - with brief explanation of decision calculus if applicable)



# Scorecard Example – Remediation

## POA&M Brief

- Findings Requiring PO&AM Inclusion
- List of Findings that can/will be Remediated
- List of Findings that cannot/will not be Remediated

## Residual Risk Brief

- Findings + Remediation Level (i.e.: % “fixed”)
- Employed Countermeasures

# Scorecard Example - Table

SYSTEM NAME:

Test System – Example 1

8500 Control Name	8500 Control Number	Compliant	Risk	Reference & Notes
Best Security Practices	DCBP-1	No	High	Internet Explorer allows all mobile/local code execution
Enclave Boundary Defense	COEB-1	No	High	Router ACLs not in place
Instant Messaging	ECIM-1	Yes	N/A	
Incident Response Planning	VIIR-1	No	Medium	No Incident Response Plan identified

# Agenda

---

- From DITSCAP to DIACAP
- C&A and the Grid
- DIACAP Structure
- Completing the Process
- The Scorecard
- **Determinations and Decisions**



# Certification & Accreditation Decisions

---

- Package + Risk Assessment Presented to Certification Authority
- CA Makes Certification Determination and Issues Endorsement Letter
- DAA Takes the CA Recommendation and DIACAP Package to Make Accreditation Decision

# Authority To Operate

---

Accreditation Decision Takes the Form of:

ATO – Authority to Operate (no provisions)

IATO – Interim ATO (provisions set forth in POA&M required)

IATT – Interim Authority To Test (inside given timeline only)

DATO – Denial of ATO (Reassess Implementation Plan...)



# ATO Maintenance

---

- Monitor IA-Relevant Issues (vulnerabilities, exploits, policy changes, best practices, etc.)
- Conduct Annual (at minimum) Reviews
- Complete Re-Accreditation Process (3 Years)
- Identify Decommission Point



# C&A's Enhanced Role

---

Much more effort will be concentrated in the production system

- DITSCAP required a great deal of effort at the outset, and then nebulous “lifecycle support”
- DIACAP involves C&A Validation for systems in production (through constant security control/configuration review and annual assessments)

# C&A Will Enable Technology

---

- C&A teams will now be able to share their tremendous validation efforts among other groups
- Reciprocity will lighten program initiation costs, allow for more thorough validation testing, provide for quicker security engineering plans/changes

# Additional Information

---

## Reciprocal: DIACAP Review

<http://www.infectionvectors.com/vectors/reciprocal.htm>

## DISA's DIACAP Site

<http://iase.disa.mil/ditscap/>

## NSA GIG Information

<http://www.nsa.gov/ia/industry/gig.cfm?MenuID=10.3.2.2>

