



DoD Information Assurance Certification and Accreditation Policy Formulation (DITSCAP to DIACAP)

Glenda Turner
OASD(NII)

Information Assurance Directorate
703-614-2196 / glenda.turner@osd.mil

Purpose

- **Provide status of DIACAP policy formulation initiative**



What's the Status of the Update?

- **DIACAP WG kickoff April 2003**
- **Three WG drafts**
- **Version 4 to be released for wide informal review this month along with annotated outline for Manual**
- **Next step is SD 106 – formal coordination**
- **Positioning ourselves to include both the Instruction and Manual in the formal coordination package. Still working whether we will publish manual as document or online in more dynamic knowledge base.**
 - **IA Component of GIG Architecture**
 - **Core Enterprise Services**
 - **GIG Mission Areas and Domains**



Why Update?

Policy Objectives

1. **Comply with FISMA and synchronize with DoD 8500 Policy Framework**
2. **Support DoD transition to enterprise services**
3. **Provide better support to PMOs, DAAs and IAMs**
4. **Improve usability / reusability of C&A products**
5. **Improve compatibility with IC and federal processes**



FISMA Requirements

Agency Heads will delegate to CIOs the authority to ensure compliance.

Each Agency CIO shall:

1. Designate a senior agency information security officer who shall--
 - (i) possess professional qualifications, including training and experience, required to administer the functions described under this section (FISMA);
 - (ii) have information security duties as that official's primary duty; and
 - (iii) head an office with the mission and resources to assist in ensuring agency compliance with this section (FISMA);
2. Develop and maintain an agency-wide information security program
3. Develop and maintain information security policies, procedures, and control techniques
4. Train and oversee personnel with significant responsibilities for information security with respect to such responsibilities
5. Assist senior agency officials concerning their [IA] responsibilities
6. Report annually to Agency Head on program effectiveness and progress of remedial actions



-- PL 107-347, Dec 17, 2002

5

Power to the Edge 

FISMA Requirements

Agency IA Programs shall:

1. Periodically assess risks
2. Develop policies and procedures that are based on the risk assessments; cost-effectively reduce risks; and address IA across the information system life cycles
3. Develop plans for providing adequate information security for networks, facilities, and systems or groups of information systems
4. Provide IA / security awareness training
5. Periodically test and evaluate the effectiveness of information security policies, procedures, and practices, at a frequency depending on risk, but **no less than annually**
6. Testing will include the management, operational, and technical controls assigned to information systems



-- PL 107-347, Dec 17, 2002

6

Power to the Edge 

8500 Policy

- DoD IA program has 3 levels – Defense, DoD Component, and DoD information system
- DoD information system is defined by management boundary / security policy (networks, systems, groups of systems); 4 types
 - Enclave
 - AIS application /service
 - Outsourced IT-based process
 - Platform IT Interconnection
- DoD information systems are responsible for implementing the baseline DoD IA Controls
- Implementation of the DoD IA Controls will be tested via the DoD IA Certification and Accreditation Program (DITSCAP or DIACAP)
- Compliance with the DoD IA Controls is a necessary condition of IA Accreditation.



-- **DoDI 8500.2 Feb 6, 2003**

Power to the Edge 

8510 Overview

- Reinterprets IA C&A through the FISMA and 8500 lenses
- Defines C&A in context of the DoD and DoD Component IA Programs
- Reinforces 8500 IA Controls structure as basis for IA C&A
 - Describes process for making changes to the DoD baseline through **Department-level risk assessment** and interaction with Component IA programs
 - Describes process for Component supplementation of DoD baseline through **Component-level risk assessment** and evaluation of the Component's IA program effectiveness
 - Describes process for individual system supplementation of DoD+Component baseline through system-level risk assessment
- Requires **every** DoD information system to be under the authority of a DoD Component IA Program
- Requires the DoD Component IA Program to certify the implementation of DoD and DoD Component IA Controls



The DIACAP Big Picture – Roles

DOD IA PROGRAM

- Establish, maintain, and disseminate DoD IA Controls and IA Controls Implementation Guides
- Assign governing IA program; provide standards and process for IT acquisitions under OSD oversight
- Provide oversight over DoD Component IA Programs

DOD COMPONENT- LEVEL IA PROGRAMS

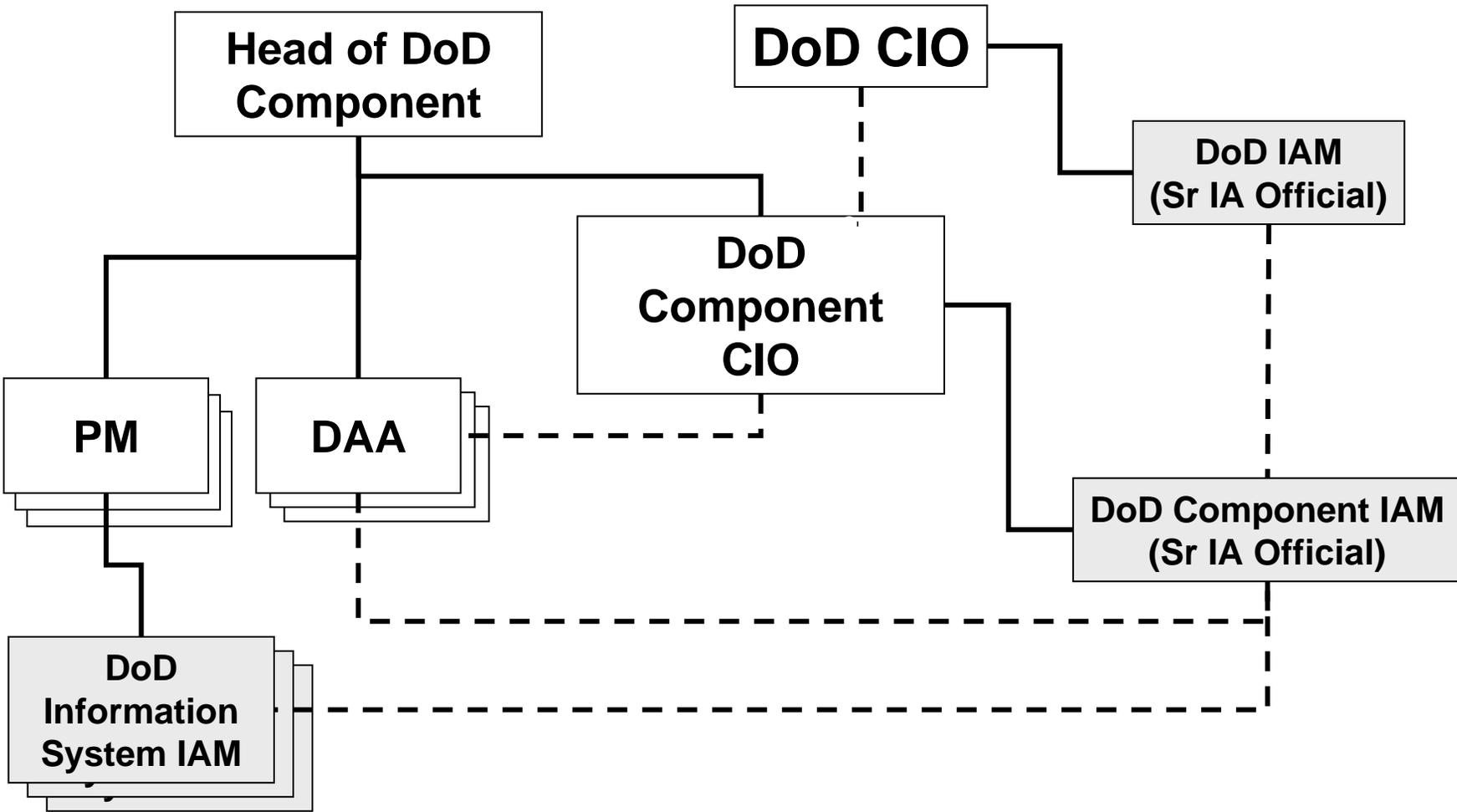
- Establish, maintain, and disseminate DoD Component IA Controls and IA Controls Implementation Guides
- Provide standards and processes for IT acquisitions under Component oversight
- Provide oversight over DoD Information System IA Programs
- Track Component information systems and their DIACAP status
- Function as the Certifying Agent for Component information systems – apply expertise and lessons learned to “help desk” like support and to improving/maintaining IA Controls and Implementation Guides (FISMA-required agency-level risk assessment)
- Provide IA management information / support to DAAs and PMOs
- Provide continuous or on-going IA Certification (e.g., assessing vulnerability scans, penetration tests, exercises, and IAVA compliance; periodically testing selected IA Controls) (FISMA required evaluation NLT annually)
- Participate in the DoD process for maintaining DoD baseline IA Controls and Implementation Guides (FISMA-required agency level-risk assessment)

DOD INFORMATION SYSTEM IA PROGRAMS

- Design, implement, administer, and maintain IA capabilities



DoD IA Program Structure (Single DoD Component View)



Legend:

- Chain of Command
- Technical Direction, Coordination
- The DoD IA Program, as defined in DoDI 8500.2

Note: Some PMs and DAAs may report to the DoD Component CIO.



The DIACAP Big Picture – Roles

- Assign Governing IA Program
- Standards & Oversight



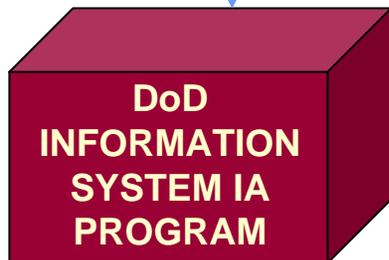
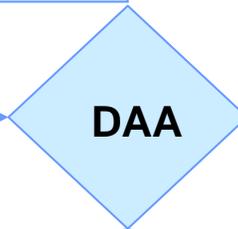
- DoD IA Controls¹
- Oversight

- IA Management & Readiness Reporting
- CM Support for DoD IA Controls



- DoD Component IA Controls
- Registration/Tracking
- “Help Desk” Support
- Certification
- Oversight

- Authorization Recommendations
- Support / Status



- Status
- Incremental & Completed Plans
- System Access/support for certification
- Maintenance of secure configuration

Certification

Authorization



¹With Maps/Interfaces to National and IC

The DIACAP Big Picture – Activities

START

1. SCOPE & REGISTER

- Appoint & train the DIACAP Team.
- Establish MAC and Confidentiality Levels.
- Register with DoD Component IA Program.

2. PLAN & DESIGN

- Identify all assigned IA Controls & Guides.
- If operational, conduct compliance assessment. If new start, develop initial IA/Security Architecture
- Develop IA Controls Implementation Plan.
- Develop a timeline and identify resource requirements.
- Obtain DoD Component IA Program and DAA reviews.

3. IMPLEMENT

- If new start, develop and implement detailed IA/Security design.
- Implement assigned IA Controls.

4. CERTIFY

- CES and AIS Application certification has two parts:
 - One time only (per baseline), the acquisition PM obtains certification that security features and functions organic to the service or application function as intended. NIAP or Common Criteria evaluations meet this need for IA and IA-enabled products for both enclaves and AIS applications.
 - At each hosting enclave, the IT operations PM obtains certification that the security configuration settings of a newly hosted service or application are correct.
- If a CES, the acquisition PM must also obtain certification that the hosting enclave meets any special IA Controls for hosting a CES.

- Certification Scorecard/Residual Risk Assessment
- ID of any implementation that contradicts DoD Guide or use of IA/Security CES plus rationale

5. AUTHORIZE or DENY

- ATO.
- IATO with IATO Action Plan.
- IATT.
- DATO.

- *Enclaves*
- *Core Enterprise Services*
- *AIS Applications (Domain or COI Services & Applications)*

7. REVIEW IA PROGRAM

- Conduct IA monitoring as specified in the IA Implementation Plan.
- Conduct assigned / scheduled vulnerability scans and penetration tests
- Re-certify identified IA Controls
- Update IA Controls and Guides

6. MANAGE SECURE CONFIGURATION

- Exercise configuration management portion of IA Controls Implementation Plan for operational system, which permits IT component swaps and minor software releases
- Incorporate newly assigned IA Controls into IA Implementation Plan
- Acquisition PM supports IAVAs, corrections of other identified security vulnerabilities

- CES and AIS Applications initiate DIACAP cycle for each Major Software Release

Communicating DIACAP Status

Standard Reports, Varying Levels of Information

- FISMA requirements are being incorporated into IT Registry
 - DoD Information System, DAA, MAC, Confidentiality Level, Accreditation Decision and Date
- DIACAP Certification Scorecard -- NOTIONAL
 - Report One - Summarizes Compliance by Number of IA Controls, (e.g., MAC 1, Sensitive = 107 Controls; System complies with 103 plus 5 Augmented Controls) plus optional narrative, POAM
 - Report Two – Identifies the IA Controls for which the System does not comply; Identifies Augmented Controls; optional narrative, POAM
 - Report Three – Provides summary information of salient DoD Component IA Control Guides
- DoD Component IA Programs, as certifiers, have access to all C&A artifacts
- DoD IAM has access to all C&A artifacts for OSD-over-sighted program



-- PL 107-347, Dec 17, 2002

14

Power to the Edge 

Toward Net-Centricity

Identity, IA Credentials, IA Posture

TODAY

CAC



Plug & Play Devices



Signed SW

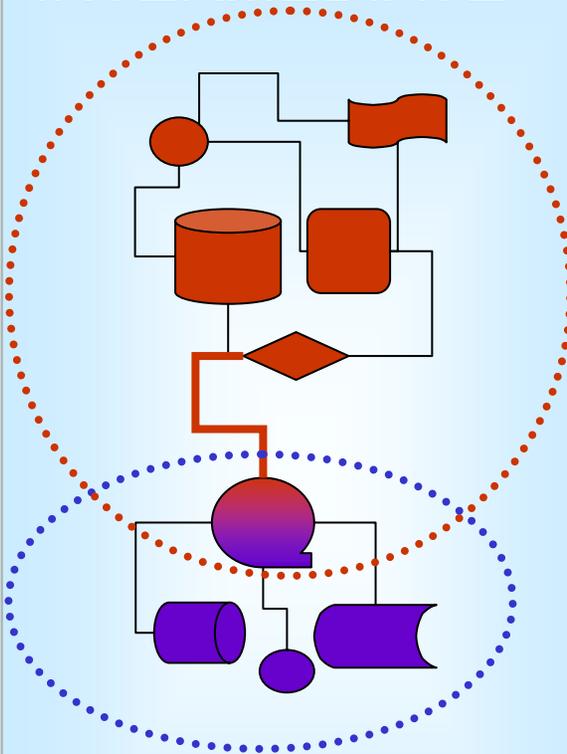


IFF



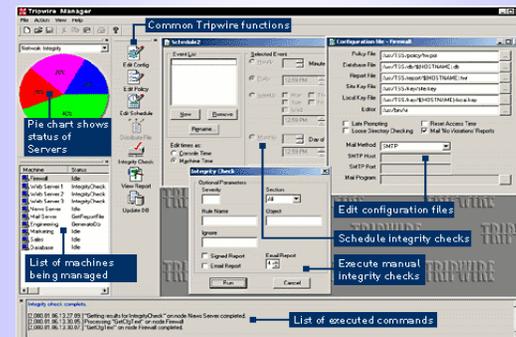
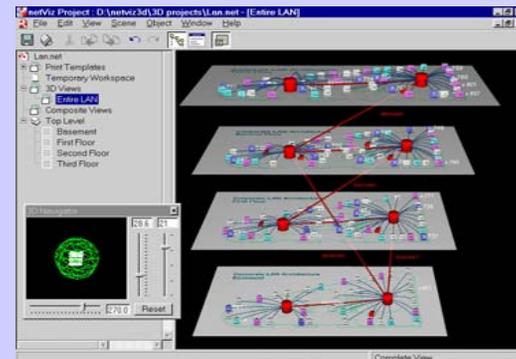
*Non-Interoperable Point Solutions
...Foundation for Future ...*

INTERMEDIATE



Global Unique Digital Identity and IA Credentials for all IT Components and Complex Entities

TARGET



IA Privileges Dynamically Adjusted to Reflect IA Posture of GIG or Entity



Toward Net-Centricity

Identity, IA Credentials, IA Posture

DITSCAP

- System-Unique Requirements and Metrics (Risk Assessment)
- System-Unique IA Architecture
- **DAA Signature is the System IA Credential**
- Information is Seldom Current
- No Information on Many Systems

- *Slow, Manual, Frustrating*
- *Non-Standard Solutions*
- *Abdicated Responsibility*
- *Difficult to Share*

DIACAP

- Baseline DoD Controls, Standards, Tests, Metrics (DoDI 8500.2 and DoD 8510.x-M)
- Emerging GIG and DoD Component Architectures
- Reviews NLT Annual
- Status in Online Repositories
- Expanded System Boundaries = Greater Coverage

- *Integrated with FISMA; Standard Terms and Reports*
- *Integration with Other IA Management Processes*

TARGET

- Mature knowledge-base Integrates DoD, Component, Mission Area, Domain, and COI IA Controls & Standards
- Robust plug-and-play Enterprise IA Services
- Continuous Automated Certification of IA Posture and Smart Adjustments to Digital Policies
- IA Posture Visible

- *IA Privileges Dynamically Adjusted to Reflect IA Posture of GIG or Entity*



Enterprise Mission Assurance Support System (eMASS)

- Joint R&D initiative focused on applying egov/ebusiness principles and technologies to Information Assurance Management
 - Enterprise database with integrated schema
 - Web Services architecture
 - Core is C&A – data oriented approach
 - Transactional processes
 - Reusable data (e.g., between enclaves and applications)
 - Intelligent RTM based on DoD 8500, DCID 6/3, special cases (e.g., CDS)
- Schedule
 - DLA conducting agency-wide pilot now
 - Working with IC to incorporate their requirements
 - DCID 6/3 controls and registration info
 - PL-3 compliance
 - OSD is a candidate pilot for Mar 03 and next release
 - NGA is designated IC pilot for Mar 03 and next release
 - eMASS is candidate for Core Enterprise Service under NCES



Conclusion

- **What we have:**
 - Reasonably mature policy
 - Good start on the Implementation Guides
 - Promising automated tools
- **What we need**
 - IA Portal, DIACAP knowledge-base and processes for authoring and managing content
- **Biggest challenge in DIACAP will be unlearning old habits and seeing things with fresh eyes**
- **Sometimes the strength of a policy or process is in the “white space”**
- **Many, many changes ahead with transformation to net-centricity**



BACKUPS



How DoDI 8500.2 Helps Today

Recasts IA to be:

1. Bounded and measurable.
2. Directly tied to mission and information value.
3. Expressed as things that you do.
4. Easily communicated and compared.

Adequate security means security **commensurate with the risk and magnitude of the harm** resulting from the loss, misuse, or unauthorized access to or modification of information. This 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.**

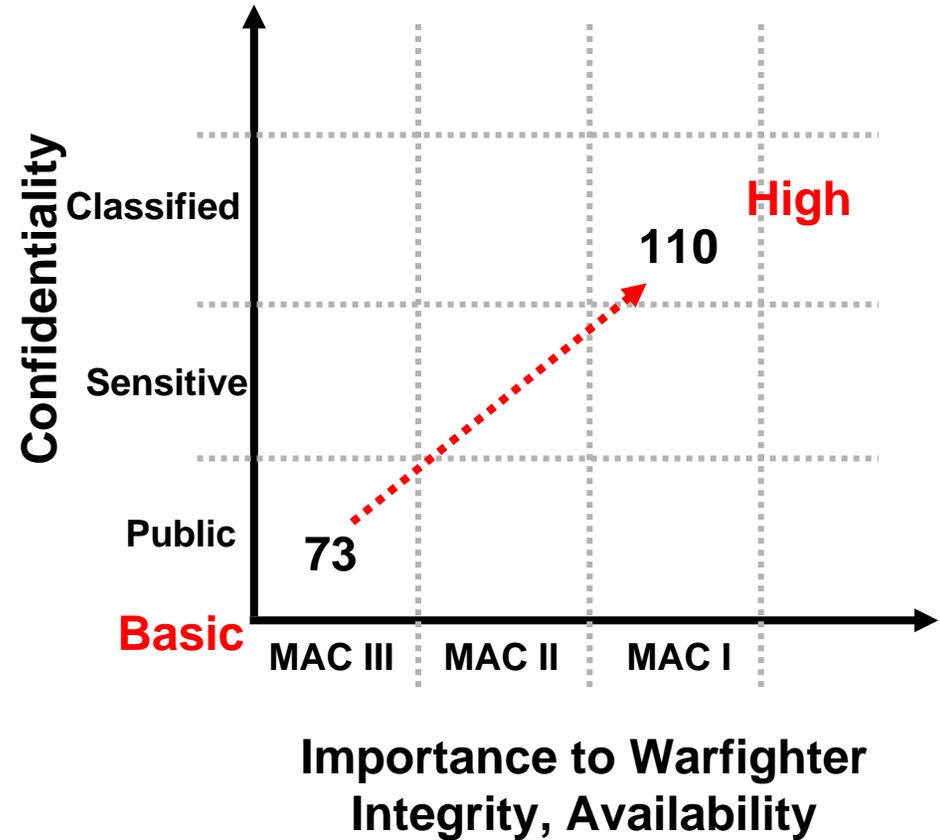
- OMB A-130



Banded IA Levels ... DoD IA Controls

SUBJECT AREAS

1. Security Design & Configuration
2. Identification & Authentication
3. Enclave & Computing Environment
4. Enclave Boundary Defense
5. Physical & Environmental
6. Personnel
7. Continuity
8. Vulnerability & Incident Management



MAC = Mission Assurance Category



How DoDI 8500.2 Helps Today

Establishes Multi-Echelon Management Structure

Policy, Architecture, Standards, & Accountability

GIG Portfolios and Governance

Defense-Wide IA Program

Comp IAP

Comp IAP

Comp IAP

DoD Information System IA Program

Services & Applications

Lightweight Application

Application Service

Application Service

Core Enterprise Services

Reusable

Storage Service

Utility Services

IA/Security Services

Messaging Services

Standard Computing Enclaves

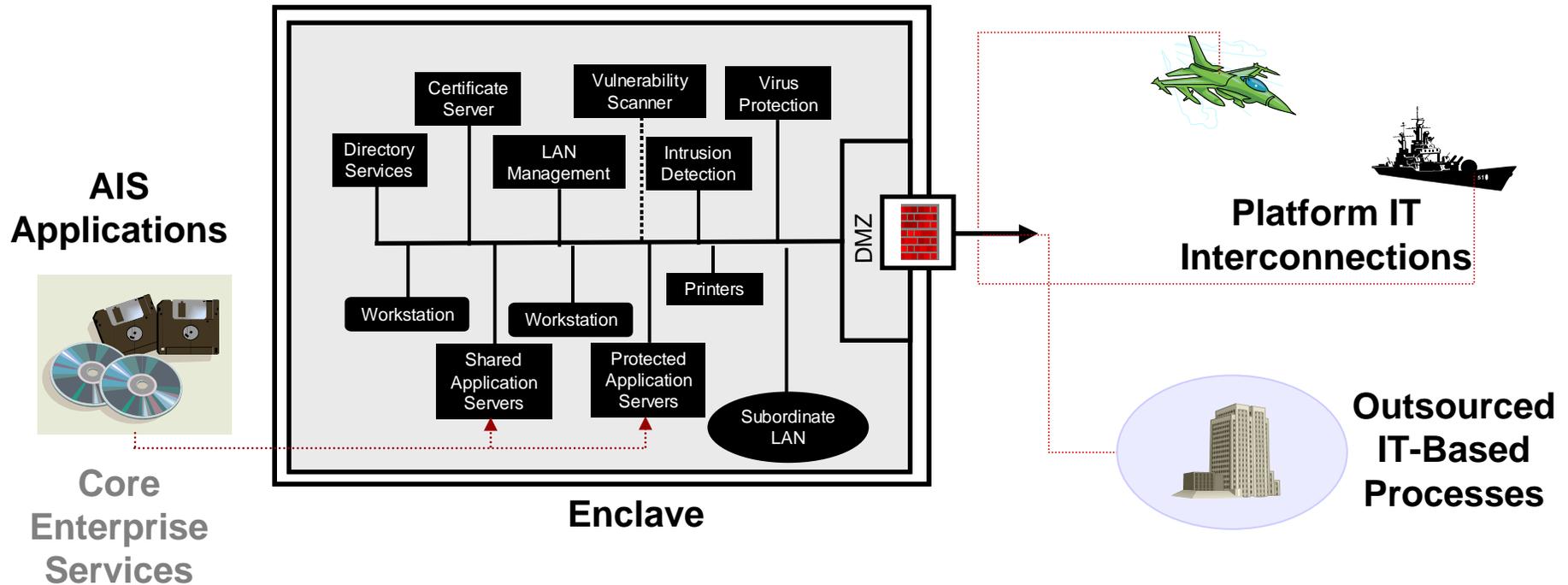
Common Network Transport

Comp = DoD Component



How DoDI 8500.2 Helps Today

Concept of System Based on Management Boundaries



- “Units” of C&A should be to management/IA program boundaries.
- Don’t need IA programs for individual applications and utilities.



How DoDI 8510 Continues The Transformation

Emphasizes "WHAT" not "HOW"

In Net-Centric terms ... separates data from application

DoD Baseline Controls

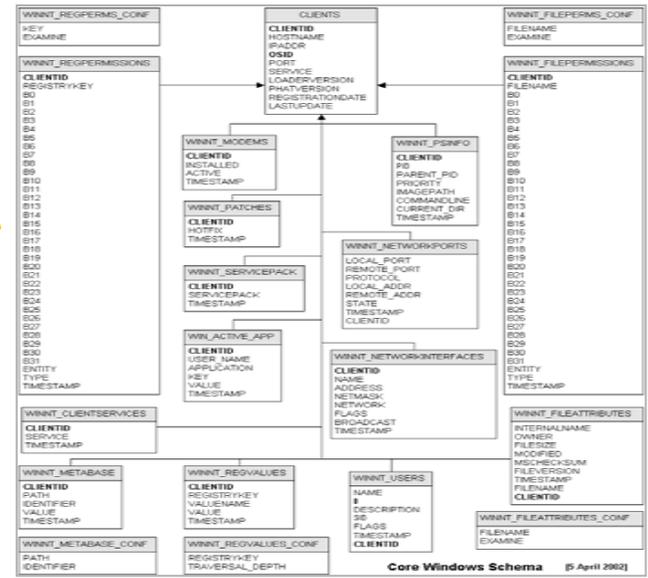
DDIA Controls					
Control ID	Control Text	Q1	Q2		
DDSI1	...				
DDSI2	...				
DDSI3	...				
DDSI4	...				
DDSI5	...				
DDSI6	...				
DDSI7	...				
DDSI8	...				
DDSI9	...				
DDSI10	...				
DDSI11	...				
DDSI12	...				
DDSI13	...				
DDSI14	...				
DDSI15	...				
DDSI16	...				
DDSI17	...				
DDSI18	...				
DDSI19	...				
DDSI20	...				
DDSI21	...				
DDSI22	...				
DDSI23	...				
DDSI24	...				
DDSI25	...				
DDSI26	...				
DDSI27	...				
DDSI28	...				
DDSI29	...				
DDSI30	...				
DDSI31	...				
DDSI32	...				
DDSI33	...				
DDSI34	...				
DDSI35	...				
DDSI36	...				
DDSI37	...				
DDSI38	...				
DDSI39	...				
DDSI40	...				

DoD Component or Domain Add-Ons

Table with red headers and red text (DoD Component or Domain Add-Ons)

System-Unique Add-Ons

Table with blue headers and blue text (System-Unique Add-Ons)

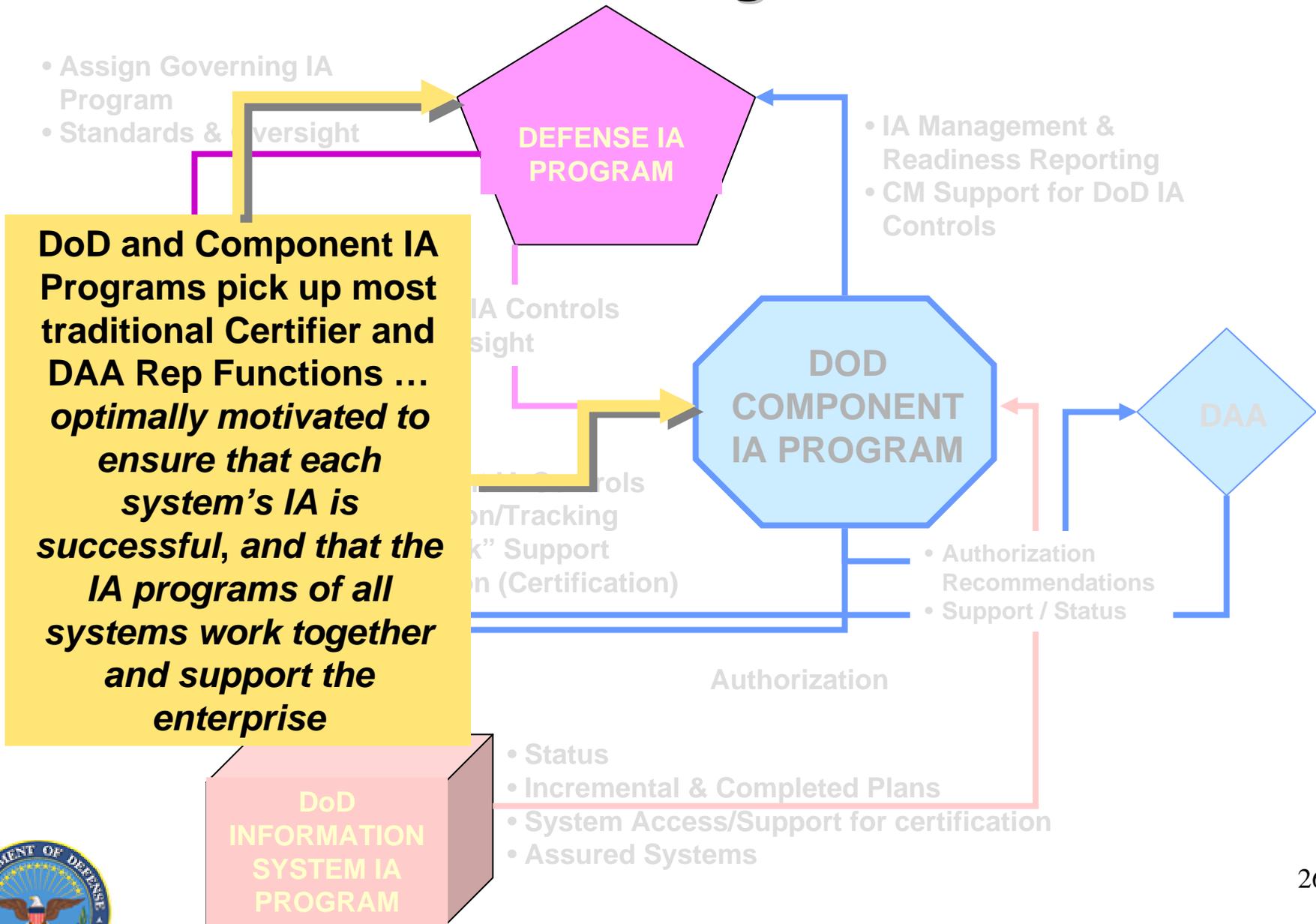


Standard Implementation Guides, Tests, and Report Formats

IA Controls and Implementers may vary in level of required detail, time and effort to implement, testing frequency, and frequency of change. New IA Controls don't have to restart the DIACAP clock.



The DIACAP Big Picture – Roles

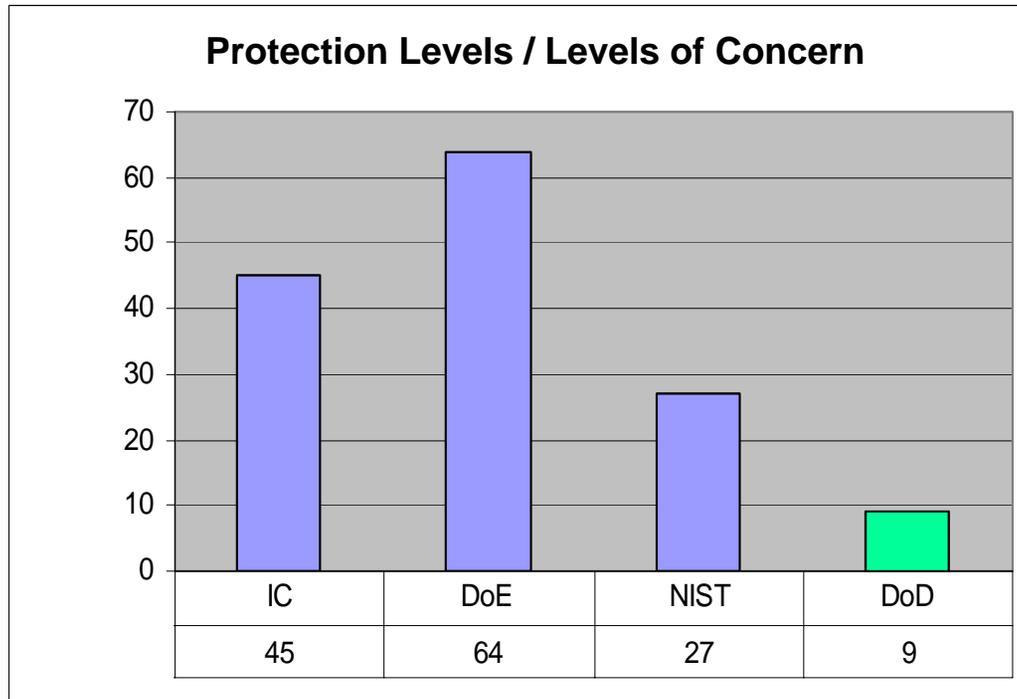


DIACAP Conclusion

- Discussed how DIACAP
 - Supports the GIG Transformation
 - Implements new federal requirements (FISMA)
 - Builds on and integrates new IA policy (8500 series)
- Shown that change is both evolutionary and revolutionary, and that you can start **today** implementing the DoD baseline IA Controls
- Confirmed that DIACAP is being worked in conjunction with federal guidelines (NIST SP 800-53 and 800-37) and with IC updates to DCID 6/3
- Highlighted issues relevant to discussion of GIG governance



Federal Models of Banded IA Levels



- IC and DoE models only address classified systems
- IC only addresses SCI
- DoD High Confidentiality (Classified) equivalent to DCID 6/3 PL-2
- NIST must address all federal systems other than National Security Systems
- DoD must address non-NSS & NSS, unclassified and classified, and ensure bridge to SCI



Example of an IA Control

IA Service: Availability
Control Number: CODB

Control Subject Area: Continuity
Control Name: Data Backup Procedures

CODB-1 Data backup is performed at least weekly.

CODB-2 Data backup is performed daily, and recovery media are stored off-site at a location that affords protection of the data in accordance with its mission assurance category and confidentiality level.

CODB-3 Data backup is accomplished by maintaining a redundant secondary system, not collocated, that can be activated without loss of data or disruption to the operation.



GIG Portfolios

GIG Architecture

Enterprise Portfolio

Governance

Users,
Providers

Business Mission Area

Governance

- Installations & Environment Domain
- Human Resources Management Domain
- Acquisition Domain
- Strategic Planning & Budget Domain
- Logistics Domain
- Accounting & Finance Domain

Warfighting Mission Area

Governance

JS/OSD Working Portfolio Definitions and Governance

National Intelligence Mission Area

Governance

IC/OSD Working Portfolio Definitions and Governance

Controlled UNCLASS
Classified



Enterprise Information Environment Mission Area

Governance

- Communications Domain
- Computing Infrastructure Domain
- Core Enterprise Services Domain

National Intelligence Enterprise Information Environment Mission Area

Governance

IC CIO/OSD Working Portfolio Definitions and Governance

Enterprise/Domain/COI Data

Enterprise/Domain/COI Data



Coalition

Federal

Other

