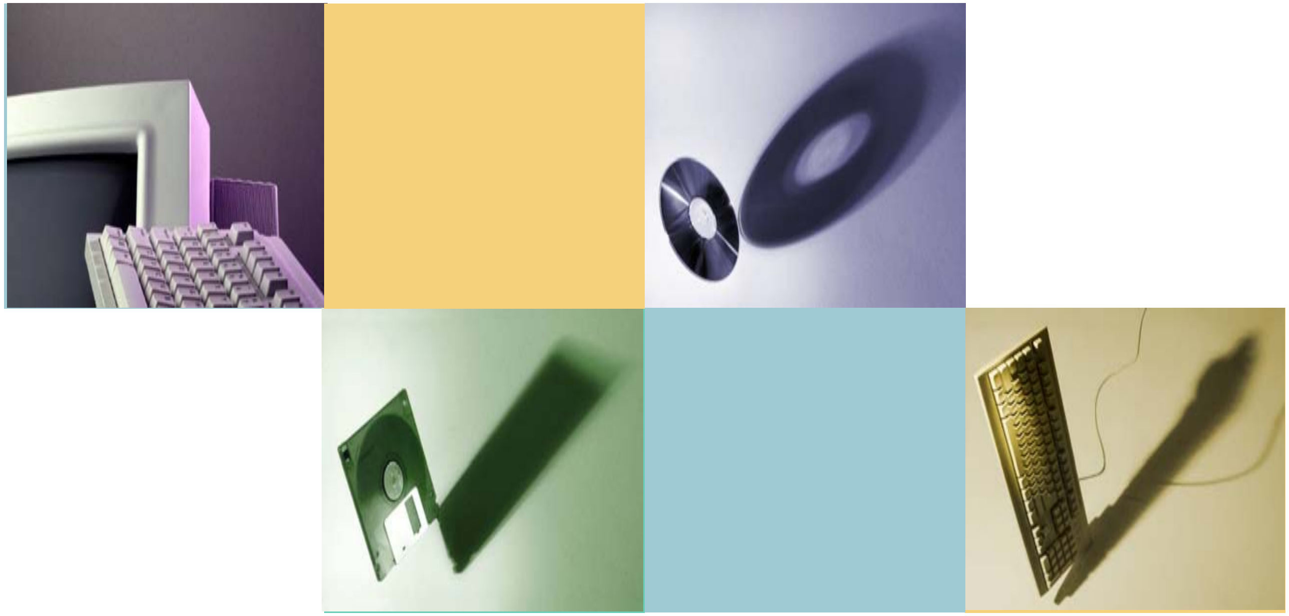
Applying the DOD Information Assurance C&A Process (DIACAP) – Overview



C&A, Risk, and the System Life Cycle

Agenda

Part 1

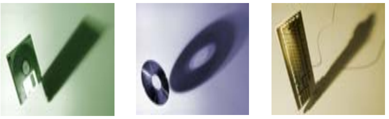
- The C&A Challenge
- DOD’s IA Framework
- Making C&A Dynamic & Net-Centric

Part 2

- The DIACAP
  - DIACAP Process & Package
  - Understanding DOD’s Concept of Enterprise Risk and Risk Management
  - DITSCAP – DIACAP Analysis: Similarities & Differences
  - DITSCAP to DIACAP Transition
- Applying DIACAP in the System Life Cycle

Part 3

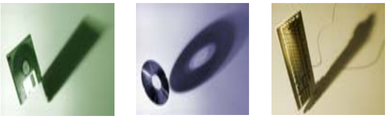
- Supporting Tools
  - Knowledge Service Overview
  - eMASS Overview
- Summary and Questions



Let’s Start with a Common Vocabulary

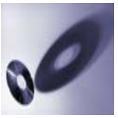
- Certification: Comprehensive evaluation of the technical and non-technical security features of an IS to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements. (CNSSI 4009)

- Accreditation: Formal declaration by a Designated Approving Authority (DAA) that an IS is approved to operate in a particular security mode at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards. (CNSSI 4009)



Let’s Start with a Common Vocabulary

- Certification & Accreditation: A set of procedures and assessments leading to a determination of the suitability of the system to operate in the targeted environment.
  - Procedures encompass the entire life cycle of the system
  - Required before operations begin and at least every three years thereafter, or whenever major security-relevant changes occur
  - Requires an annual IA Controls review



The Security Landscape

August 28, 2006 ■ Volume 23, Number 33

more heat
multiply

COMPUTERWORLD

IT Execs on Firing Line Over Security Breaches

BY JAIKUMAR VIJAYAN

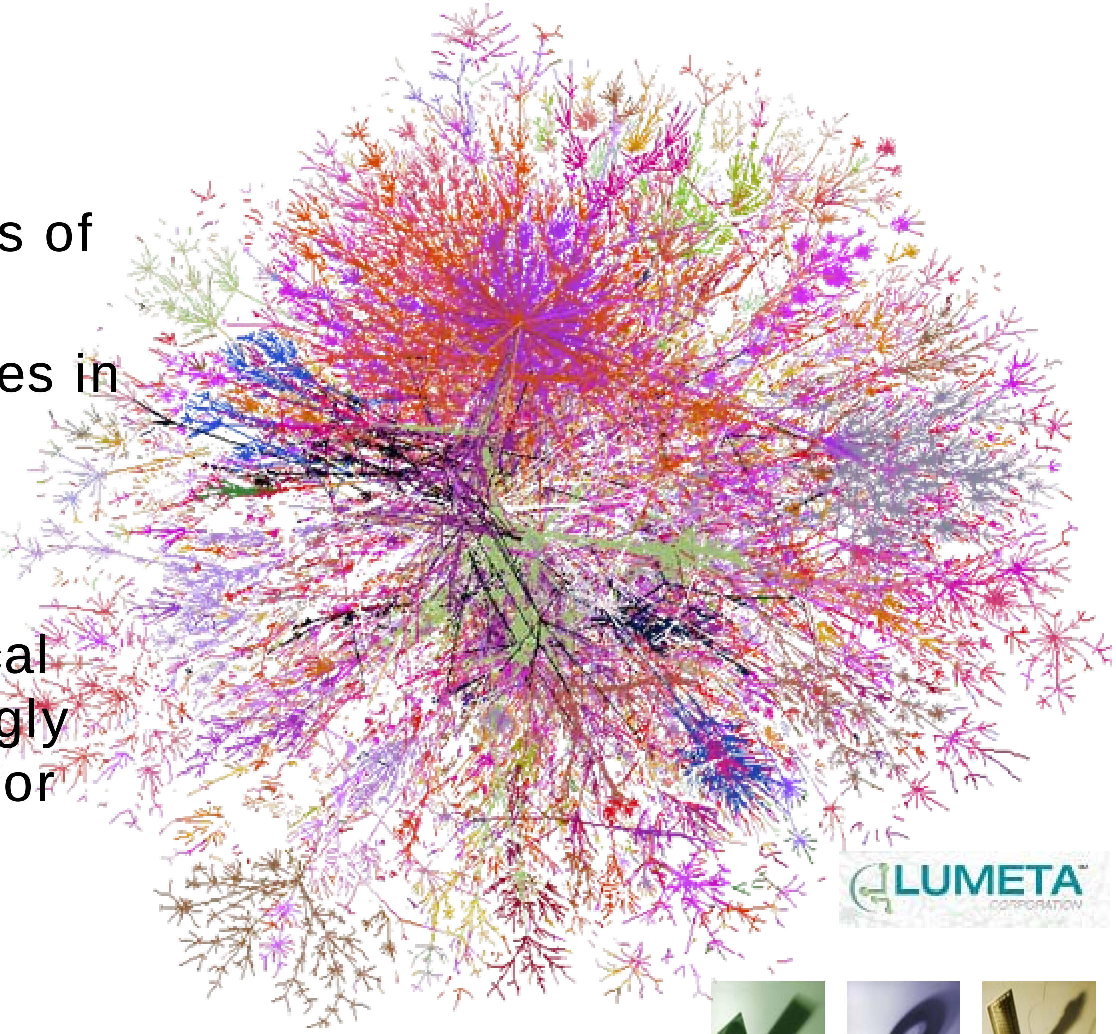
The cost of data breaches may be getting a lot higher for IT...

which was responsible for the release of the data and had been overseen by Govern...

- **Reputation**
  - Confidence and credibility of clients, partners, investors
- **Litigation**
  - Business interruption, confidentiality
- **Compliance**
  - GLBA, SOX, HIPAA, NERC, etc
  - Directors, management, auditors
- **Service**
  - Capacity to serve customers and maintain confidential data
- **Productivity**
  - Employee dependency
- **Technology**
  - IT Staffing, expertise, infrastructure

Security Needs are Continuously Evolving, Which Makes C&A Increasingly Challenging

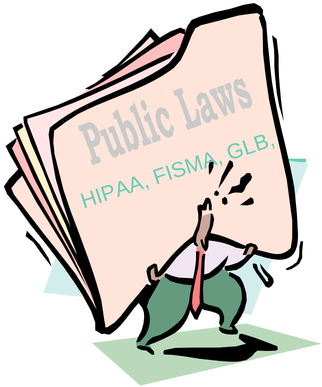
- Global interconnection
- Massive complexity
- Release of beta versions of software
- Exploitable vulnerabilities in technology
- Holes at the application layer
- Organizations and critical infrastructure increasingly rely upon the Internet for operations

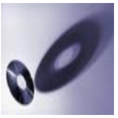


Courtesy of: LUMETA CORPORATION

Motivation – Why is DOD Changing Now?

- Federal Requirements and Guidelines
  - OMB A-130
    - Requires 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.

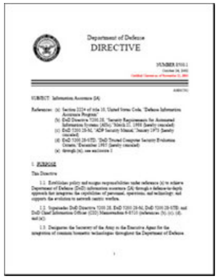




Motivation – Why is DOD Changing Now?

- 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
  - Title III of the E-Government Act, Federal Information Security Management Act (FISMA), requires Federal departments and agencies to develop, document, and implement an organization-wide program to provide information assurance.

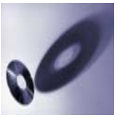
Motivation – Why is DOD Changing Now?


Department of Defense
DIRECTIVE

SUBJECT: Information Assurance (IA)

[illegible]

- DOD IA Implementation
  - DODD 8500.1 (2002)
    - Establishes policy and assigns responsibilities to achieve DOD IA [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]
- DIACAP ensures DOD C&A is consistent with FISMA, DODD 8500.1 and DODI 8500.2



Motivation – Why is DOD Changing Now?

- DOD Transformation
  - Information Technology is changing; the way DOD acquires, uses, and operates IT is changing; Federal requirements and guidelines have changed

- Global Information Grid (GIG)
  - C&A is a central component of GIG IA Strategy.
  - The GIG requires a dynamic, enterprise risk-based C&A process and net-centric applications which cannot be met with the current C&A methodology

Motivation ––Cost!!! And Questionable ROI

- The cost of C&A is high:
  - “Millions of dollars and thousands of hours are spent on C&A… In reality C&A is a 20-year-old paperwork exercise that does not yield improved security.” (Richard Bejtlich, President & CEO of TaoSecurity)

- The return on C&A was questionable:
  - Existing processes are not sufficiently flexible
    - to facilitate dynamic information sharing
    - To facilitate interoperability of enterprise systems
  - Each system determines its IA requirements and solutions independent of the larger environment
  - Paper-based “fire-and-forget” C&A documentation provides limited assurance that security information is current

Agenda

Part 1

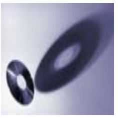
- The C&A Challenge
- DOD’s IA Framework
- Dynamic & Net-Centric C&A

Part 2

- The DIACAP
  - DIACAP Process & Package
  - Understanding DOD’s Concept of Enterprise Risk and Risk Management
  - DITSCAP – DIACAP Analysis: Similarities & Differences
  - DITSCAP to DIACAP Transition
- Applying DIACAP in the System Life Cycle

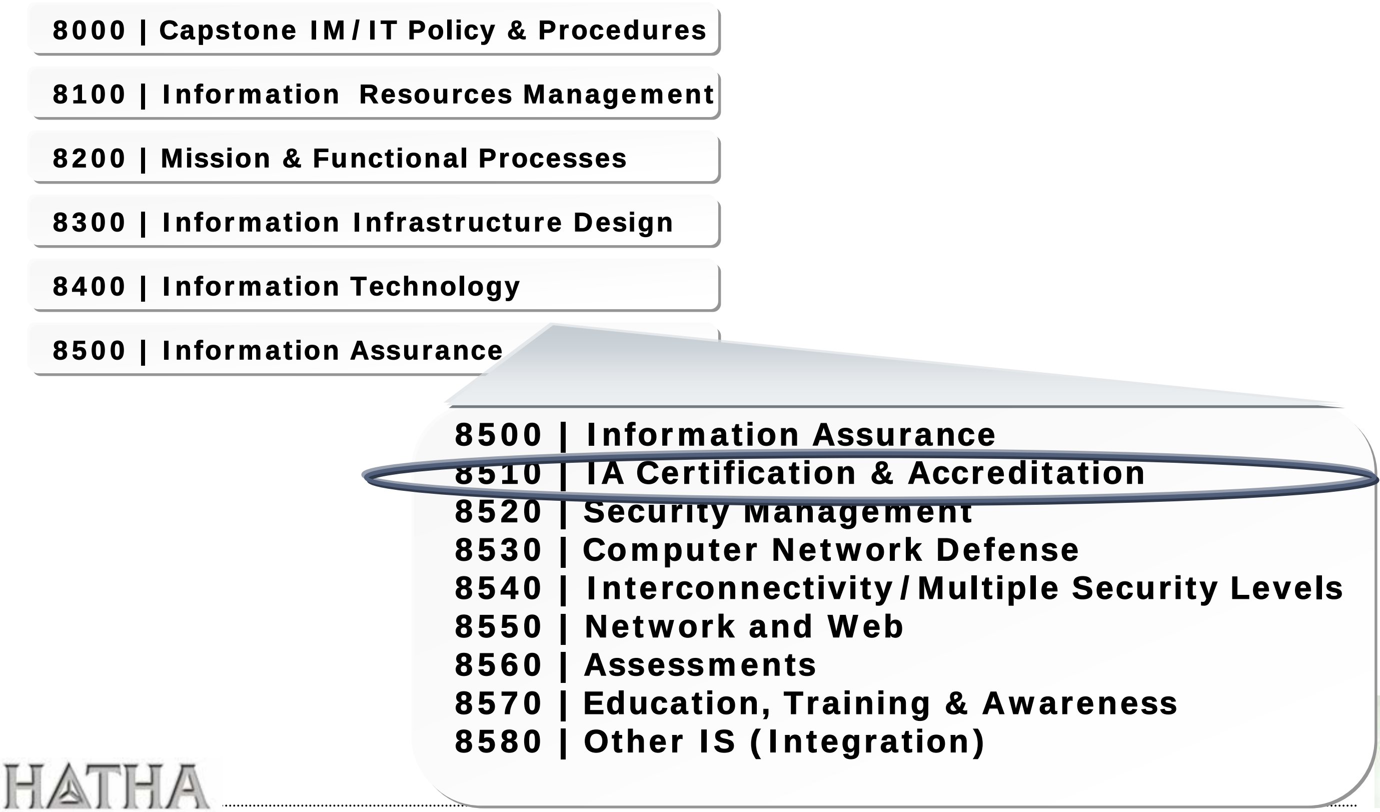
Part 3

- Supporting Tools
  - Knowledge Service Overview
  - eMASS Overview
- Summary and Questions



The Solution Begins with the DOD IA Policy Framework

- DOD has aligned all IM/IT policy, including IA policy to the 8000 series under the responsibility of the DOD CIO



8000 | Capstone IM/IT Policy & Procedures

8100 | Information Resources Management

8200 | Mission & Functional Processes

8300 | Information Infrastructure Design

8400 | Information Technology

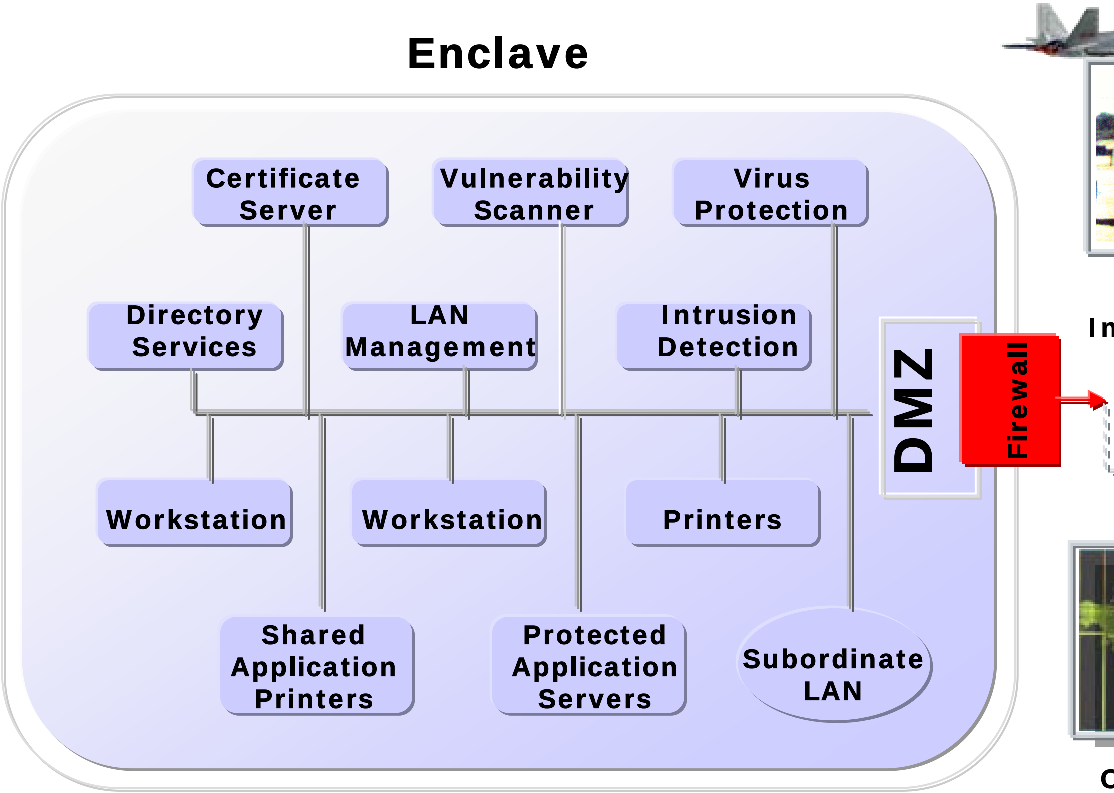
8500 | Information Assurance

8500 | Information Assurance
8510 | IA Certification & Accreditation
8520 | Security Management
8530 | Computer Network Defense
8540 | Interconnectivity/Multiple Security Levels
8550 | Network and Web
8560 | Assessments
8570 | Education, Training & Awareness
8580 | Other IS (Integration)

In the 8500 series, DOD has redefined IA & Information Systems

AIS Applications

Core Enterprise Services



Enclave

Certificate Server

Vulnerability Scanner

Virus Protection

Directory Services

LAN Management

Intrusion Detection

Workstation

Workstation

Printers

Shared Application Printers

Protected Application Servers

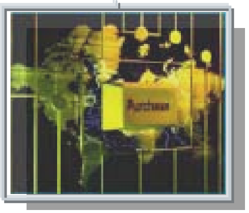
Subordinate LAN

DMZ

Firewall

- •The DOD Information System is the primary IA management unit
- •Enclave is **central**
  - •Provides majority of IA services/capabilities
  - •Enables 100% IA accountability at a manageable unit

Platform IT Interconnection



Outsourced IT-Based Processes

Agenda

Part 1

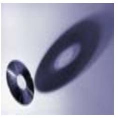
- The C&A Challenge
- DOD’s IA Framework
- Dynamic & Net-Centric C&A

Part 2

- The DIACAP
  - DIACAP Process & Package
  - Understanding DOD’s Concept of Enterprise Risk and Risk Management
  - DITSCAP – DIACAP Analysis: Similarities & Differences
  - DITSCAP to DIACAP Transition
- Applying DIACAP in the System Life Cycle

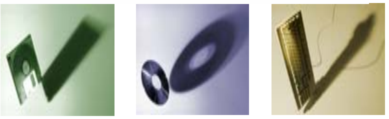
Part 3

- Supporting Tools
  - Knowledge Service Overview
  - eMASS Overview
- Summary and Questions



There are Significant Differences Between Traditional and Net-Centric C&A

Traditional	Net-Centric
IA requirements are locally established and are focused on mitigating perceived threat, vulnerabilities.	IA requirements are driven by enterprise architectures and are focused on delivery and operation of enabling capabilities.
Fixed-document formats, formal phases, stove-piped IA-unique processes, and off-line workflow and information management.	Distributed online collaboration to accomplish IA transactions that are integrated into planning, programming, requirements, architecture, system engineering, acquisition, and operations.
Information is "authored" by a team of IA professionals and has little reuse value, if any.	Most information is "fused" from distributed GIG services, data sources, and IA transactions.
Security authorizations are exchanged offline as paper documents (*e.g.*, SSAAs).	Digital-security credentials are associated with authenticated digital identifiers, and are dynamically asserted to enable connection, access to resources, or information exchange.
Operating authority is on/off based on manual 3-year assessment cycle.	Entity priviliges are dynamically adjusted based on the network's validation of conformance to security policies.



HATHA systems

Agenda

Part 1

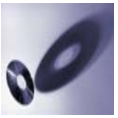
- The C&A Challenge
- DOD's IA Framework
- Making C&A Dynamic & Net-Centric

Part 2

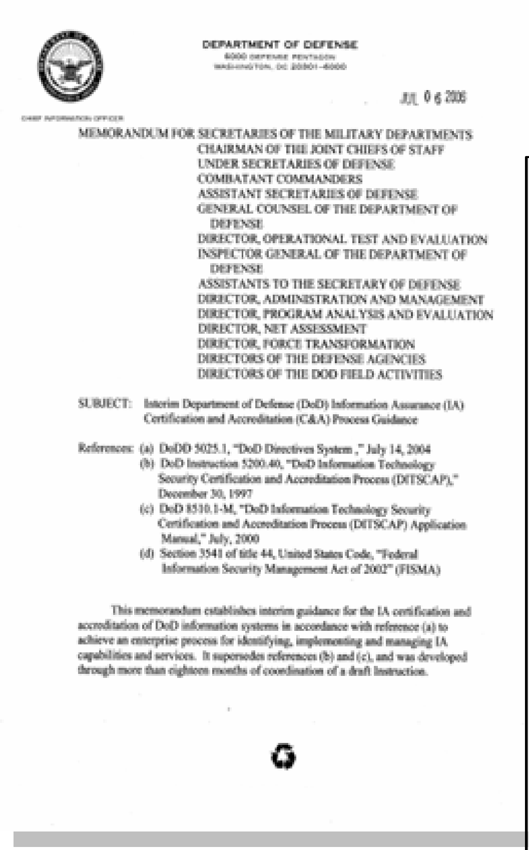
- The DIACAP
  - DIACAP Process & Package
  - Understanding DOD's Concept of Enterprise Risk and Risk Management
  - DITSCAP – DIACAP Analysis: Similarities & Differences
  - DITSCAP to DIACAP Transition

Part 3

- Applying DIACAP in the System Life Cycle
- Supporting Tools
  - Knowledge Service Overview
  - eMASS Overview
- Summary and Questions



The DIACAP was released as policy on 18 July



DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

JUL 0 6 2006

CHIEF INFORMATION OFFICER

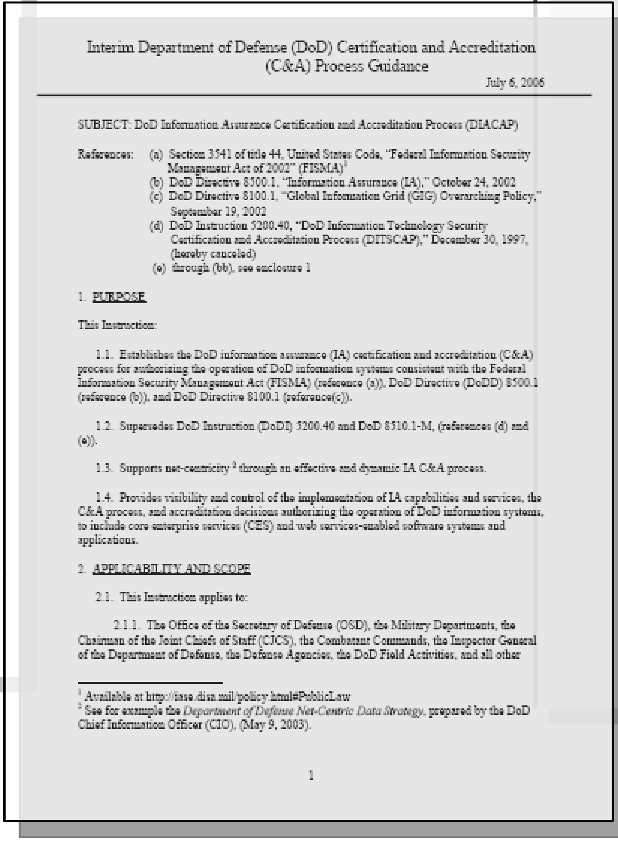
MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
COMBATANT COMMANDERS
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, PROGRAM ANALYSIS AND EVALUATION
DIRECTOR, NET ASSESSMENT
DIRECTOR, FORCE TRANSFORMATION
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Interim Department of Defense (DoD) Information Assurance (IA) Certification and Accreditation (C&A) Process Guidance

References: (a) DoDD 5025.1, "DoD Directives System ," July 14, 2004
(b) DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997
(c) DoD 8510.1-M, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual," July, 2000
(d) Section 3541 of title 44, United States Code, "Federal Information Security Management Act of 2002" (FISMA)

This memorandum establishes interim guidance for the IA certification and accreditation of DoD information systems in accordance with reference (a) to achieve an enterprise process for identifying, implementing and managing IA capabilities and services. It supersedes references (b) and (c), and was developed through more than eighteen months of coordination of a draft Instruction.

Directive-Type Memorandum



Interim Department of Defense (DoD) Certification and Accreditation (C&A) Process Guidance

July 6, 2006

SUBJECT: DoD Information Assurance Certification and Accreditation Process (DIACAP)

References: (a) Section 3541 of title 44, United States Code, "Federal Information Security Management Act of 2002" (FISMA)[1]
(b) DoD Directive 8500.1, "Information Assurance (IA)," October 24, 2002
(c) DoD Directive 8100.1, "Global Information Grid (GIG) Overarching Policy," September 19, 2002
(d) DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997, (hereby canceled)
(e) through (bb), see enclosure 1

1. PURPOSE

This Instruction:

1.1. Establishes the DoD information assurance (IA) certification and accreditation (C&A) process for authorizing the operation of DoD information systems consistent with the Federal Information Security Management Act (FISMA) (reference (a)), DoD Directive (DoDD) 8500.1 (reference (b)), and DoD Directive 8100.1 (reference(c)).

1.2. Supersedes DoD Instruction (DoDI) 5200.40 and DoD 8510.1-M, (references (d) and (e)).

1.3. Supports net-centricity [2] through an effective and dynamic IA C&A process.

1.4. Provides visibility and control of the implementation of IA capabilities and services, the C&A process, and accreditation decisions authorizing the operation of DoD information systems, to include core enterprise services (CES) and web services-enabled software systems and applications.

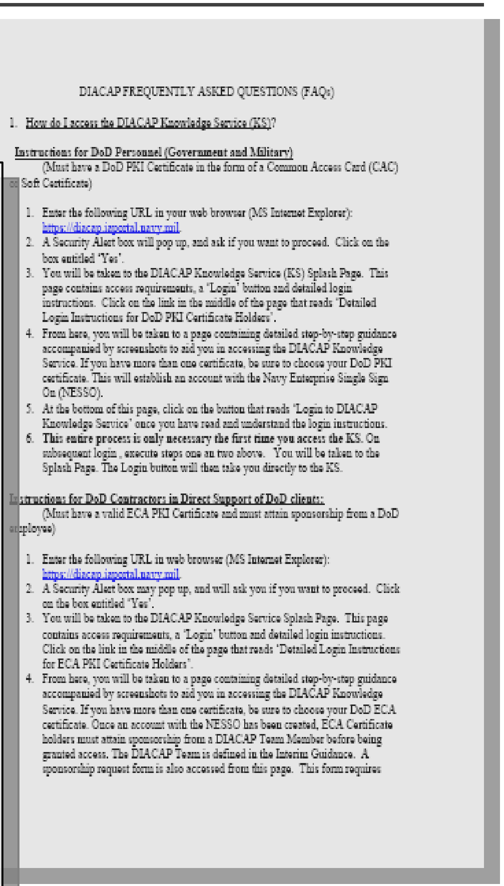
2. APPLICABILITY AND SCOPE

2.1. This Instruction applies to:

2.1.1. The Office of the Secretary of Defense (OSD), the Military Departments, the Chairman of the Joint Chiefs of Staff (CJCS), the Combatant Commands, the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other

[1] Available at http://iase.disa.mil/policy.html#PublicLaw
[2] See for example the *Department of Defense Net-Centric Data Strategy*, prepared by the DoD Chief Information Officer (CIO), (May 9, 2003).

Interim C&A Guidance



DIACAP FREQUENTLY ASKED QUESTIONS (FAQs)

1. How do I access the DIACAP Knowledge Service (KS)?

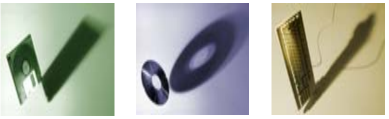
Instructions for DoD Personnel (Government and Military)
(Must have a DoD PKI Certificate in the form of a Common Access Card (CAC) or Soft Certificate)

1. Enter the following URL in your web browser (MS Internet Explorer): https://diacap.iaportal.navy.mil.
2. A Security Alert box will pop up, and ask if you want to proceed. Click on the box entitled 'Yes'.
3. You will be taken to the DIACAP Knowledge Service (KS) Splash Page. This page contains access requirements, a 'Login' button and detailed login instructions. Click on the link in the middle of the page that reads 'Detailed Login Instructions for DoD PKI Certificate Holders'.
4. From here, you will be taken to a page containing detailed step-by-step guidance accompanied by screenshots to aid you in accessing the DIACAP Knowledge Service. If you have more than one certificate, be sure to choose your DoD PKI certificate. This will establish an account with the Navy Enterprise Single Sign On (NESSO).
5. At the bottom of this page, click on the button that reads 'Login to DIACAP Knowledge Service' once you have read and understand the login instructions.
6. **This entire process is only necessary the first time you access the KS. On** subsequent login , execute steps one an two above. You will be taken to the Splash Page. The Login button will then take you directly to the KS.

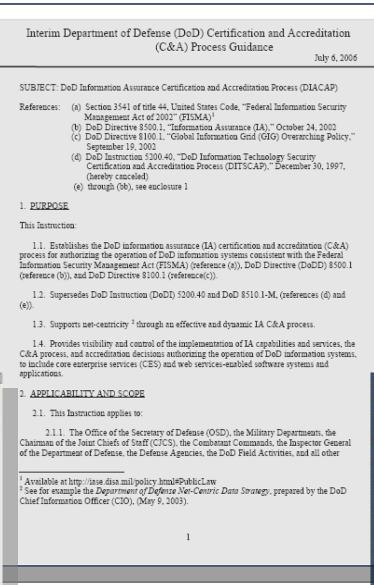
Instructions for DoD Contractors in Direct Support of DoD clients:
(Must have a valid ECA PKI Certificate and must attain sponsorship from a DoD employee)

1. Enter the following URL in web browser (MS Internet Explorer): https://diacap.iaportal.navy.mil.
2. A Security Alert box may pop up, and will ask you if you want to proceed. Click on the box entitled 'Yes'.
3. You will be taken to the DIACAP Knowledge Service Splash Page. This page contains access requirements, a 'Login' button and detailed login instructions. Click on the link in the middle of the page that reads 'Detailed Login Instructions for ECA PKI Certificate Holders'.
4. From here, you will be taken to a page containing detailed step-by-step guidance accompanied by screenshots to aid you in accessing the DIACAP Knowledge Service. If you have more than one certificate, be sure to choose your DoD ECA certificate. Once an account with the NESSO has been created, ECA Certificate holders must attain sponsorship from a DIACAP Team Member before being granted access. The DIACAP Team is defined in the Interim Guidance. A sponsorship request form is also accessed from this page. This form requires

DIACAP FAQ



The DIACAP combines with Tools to Offer a Dynamic, Net-Centric Approach to C&A



Interim Department of Defense (DoD) Certification and Accreditation (C&A) Process Guidance

July 6, 2006

SUBJECT: DoD Information Assurance Certification and Accreditation Process (DIACAP)

References: (a) Section 3541 of title 44, United States Code, "Federal Information Security Management Act of 2002" (FISMA)[1]
(b) DoD Directive 8500.1, "Information Assurance (IA)," October 24, 2002
(c) DoD Directive 8100.1, "Global Information Grid (GIG) Overarching Policy," September 19, 2002
(d) DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997, (hereby canceled)
(e) through (bb), see enclosure 1

1. PURPOSE

This Instruction:

1.1. Establishes the DoD information assurance (IA) certification and accreditation (C&A) process for authorizing the operation of DoD information systems consistent with the Federal Information Security Management Act (FISMA) (reference (a)), DoD Directive (DoDD) 8500.1 (reference (b)), and DoD Directive 8100.1 (reference(c)).

1.2. Supersedes DoD Instruction (DoDI) 5200.40 and DoD 8510.1-M, (references (d) and (e)).

1.3. Supports net-centricity [2] through an effective and dynamic IA C&A process.

1.4. Provides visibility and control of the implementation of IA capabilities and services, the C&A process, and accreditation decisions authorizing the operation of DoD information systems, to include core enterprise services (CES) and web services-enabled software systems and applications.

2. APPLICABILITY AND SCOPE

2.1. This Instruction applies to:

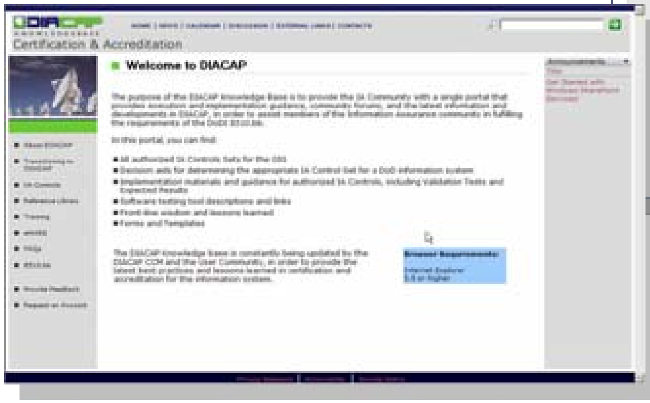
2.1.1. The Office of the Secretary of Defense (OSD), the Military Departments, the Chairman of the Joint Chiefs of Staff (CJCS), the Combatant Commands, the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other

[1] Available at http://iase.disa.mil/policy.html#PublicLaw

[2] See for example the *Department of Defense Net-Centric Data Strategy*, prepared by the DoD Chief Information Officer (CIO), (May 9, 2003).

1

Policy



DIACAP KNOWLEDGE BASE
Certification & Accreditation
HOME | NEWS | CALENDAR | DISCUSSION | EXTERNAL LINKS | CONTACTS
About DIACAP
Transitioning to DIACAP
IA Controls
Reference Library
Training
eMASS
FAQs
8510.bb
Provide Feedback
Request an Account
Announcements
Tips
Get Started with Windows SharePoint Services
Privacy Statement | Accessibility | Security Notice

Welcome to DIACAP

The purpose of the DIACAP Knowledge Base is to provide the IA Community with a single portal that provides execution and implementation guidance, community forums, and the latest information and developments in DIACAP, in order to assist members of the Information Assurance community in fulfilling the requirements of the DoDI 8510.bb.

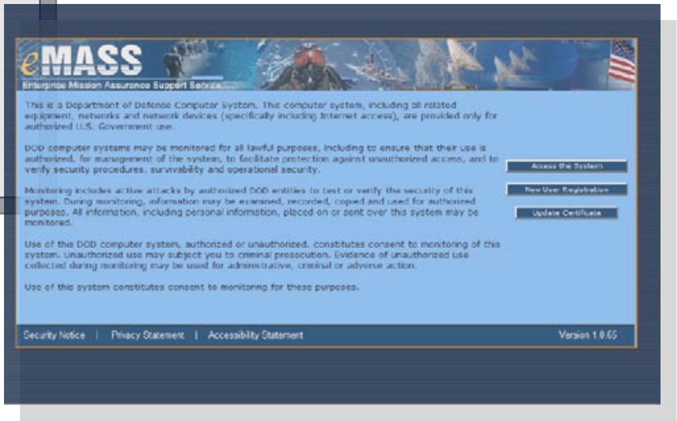
In this portal, you can find:

- All authorized IA Controls Sets for the GIG
- Decision aids for determining the appropriate IA Control Set for a DoD information system
- Implementation materials and guidance for authorized IA Controls, including Validation Tests and Expected Results
- Software testing tool descriptions and links
- Front-line wisdom and lessons learned
- Forms and Templates

The DIACAP Knowledge Base is constantly being updated by the DIACAP CCM and the User Community, in order to provide the latest best practices and lessons learned in certification and accreditation for the information system.

Browser Requirements:
Internet Explorer 5.5 or higher

Web-Based Knowledge Service



eMASS
Enterprise Mission Assurance Support Service
Access the System
New User Registration
Update Certificate
Security Notice | Privacy Statement | Accessibility Statement
Version 1.0.65

This is a Department of Defense Computer System. This computer system, including all related equipment, networks and network devices (specifically including Internet access), are provided only for authorized U.S. Government use.

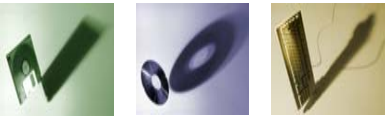
DOD computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability and operational security.

Monitoring includes active attacks by authorized DOD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored.

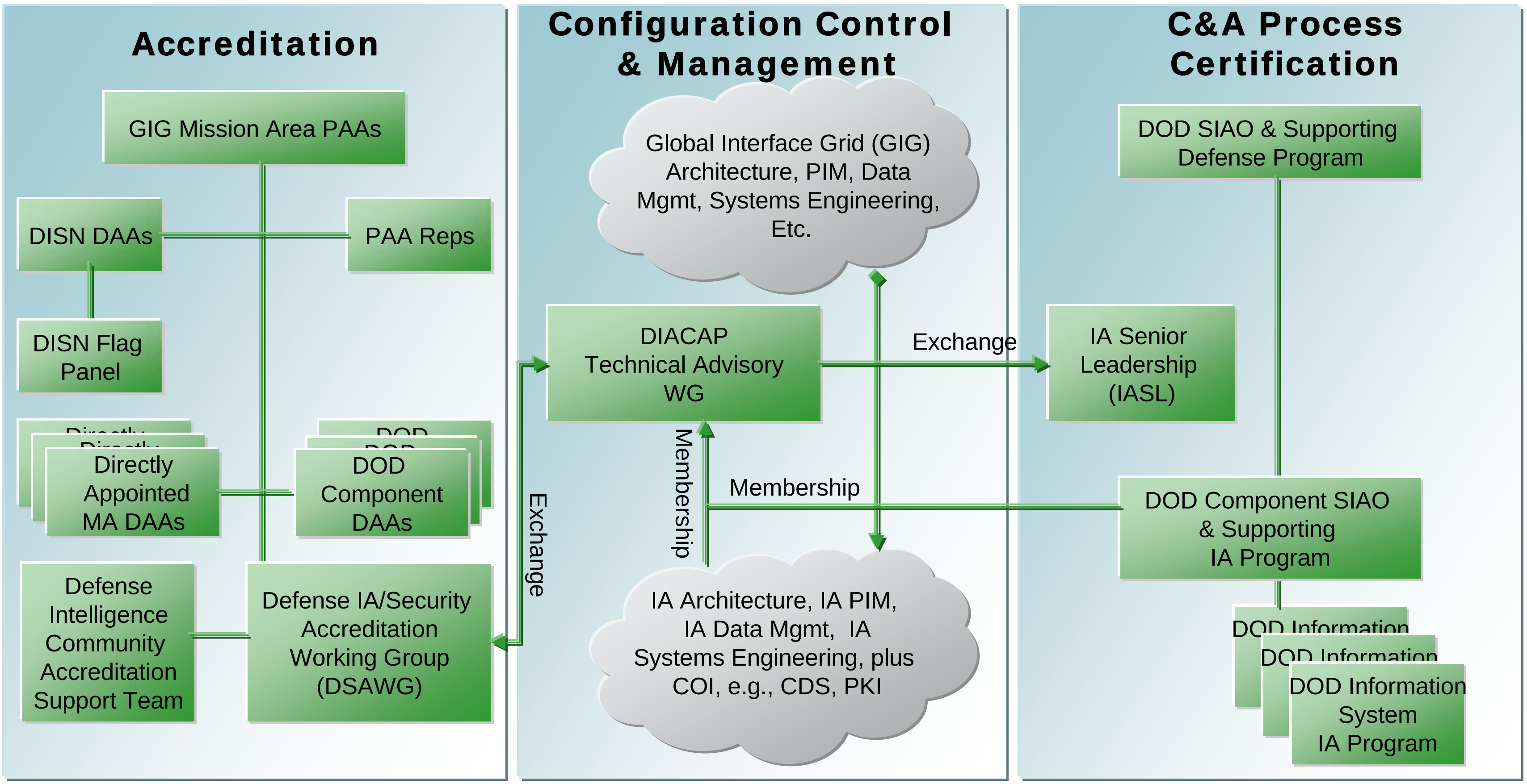
Use of this DOD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal or adverse action.

Use of this system constitutes consent to monitoring for these purposes.

***e*MASS - Automated C&A Management**



DIACAP Has a New Governance Structure



Accreditation

GIG Mission Area PAAs

DISN DAAs

PAA Reps

DISN Flag Panel

Directly Appointed MA DAAs

DOD Component DAAs

Defense Intelligence Community Accreditation Support Team

Defense IA/Security Accreditation Working Group (DSAWG)

Configuration Control & Management

Global Interface Grid (GIG) Architecture, PIM, Data Mgmt, Systems Engineering, Etc.

DIACAP Technical Advisory WG

Exchange

Membership

Membership

Exchange

IA Architecture, IA PIM, IA Data Mgmt, IA Systems Engineering, plus COI, e.g., CDS, PKI

C&A Process Certification

DOD SIAO & Supporting Defense Program

IA Senior Leadership (IASL)

DOD Component SIAO & Supporting IA Program

DOD Information System IA Program

DIACAP Knowledge Service

Enterprise Content Managed by the DIACAP TAG

COI-, DOD Component IA Program, & DSAWG Content managed by Owning Entity according to DIACAP TAG Protocols

The IA Controls are the foundation of the DIACAP

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

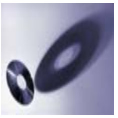
Confidentiality

	MAC III	MAC II	MAC I
Classified			110
Sensitive			
Public	73		

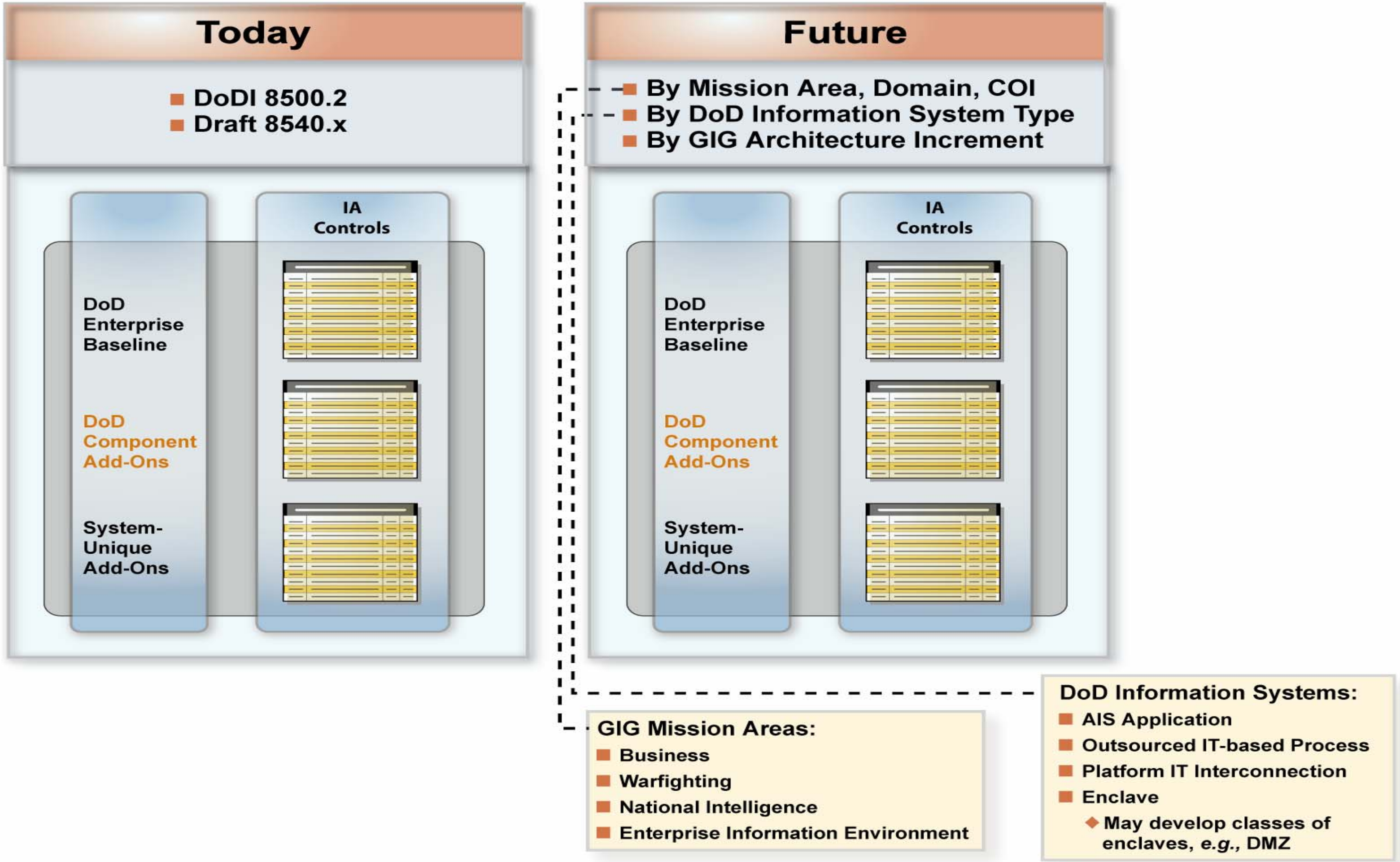
Importance to Warfighter
Integrity, Availability

MAC = Mission Assurance Category

GOAL: Adequate security, Scalable, interoperable IA capabilities, Visibility/Situational Awareness, Federal compliance



Future IA Controls Will Be Developed To Support Other Functions



Today

- DoDI 8500.2
- Draft 8540.x

Future

- By Mission Area, Domain, COI
- By DoD Information System Type
- By GIG Architecture Increment

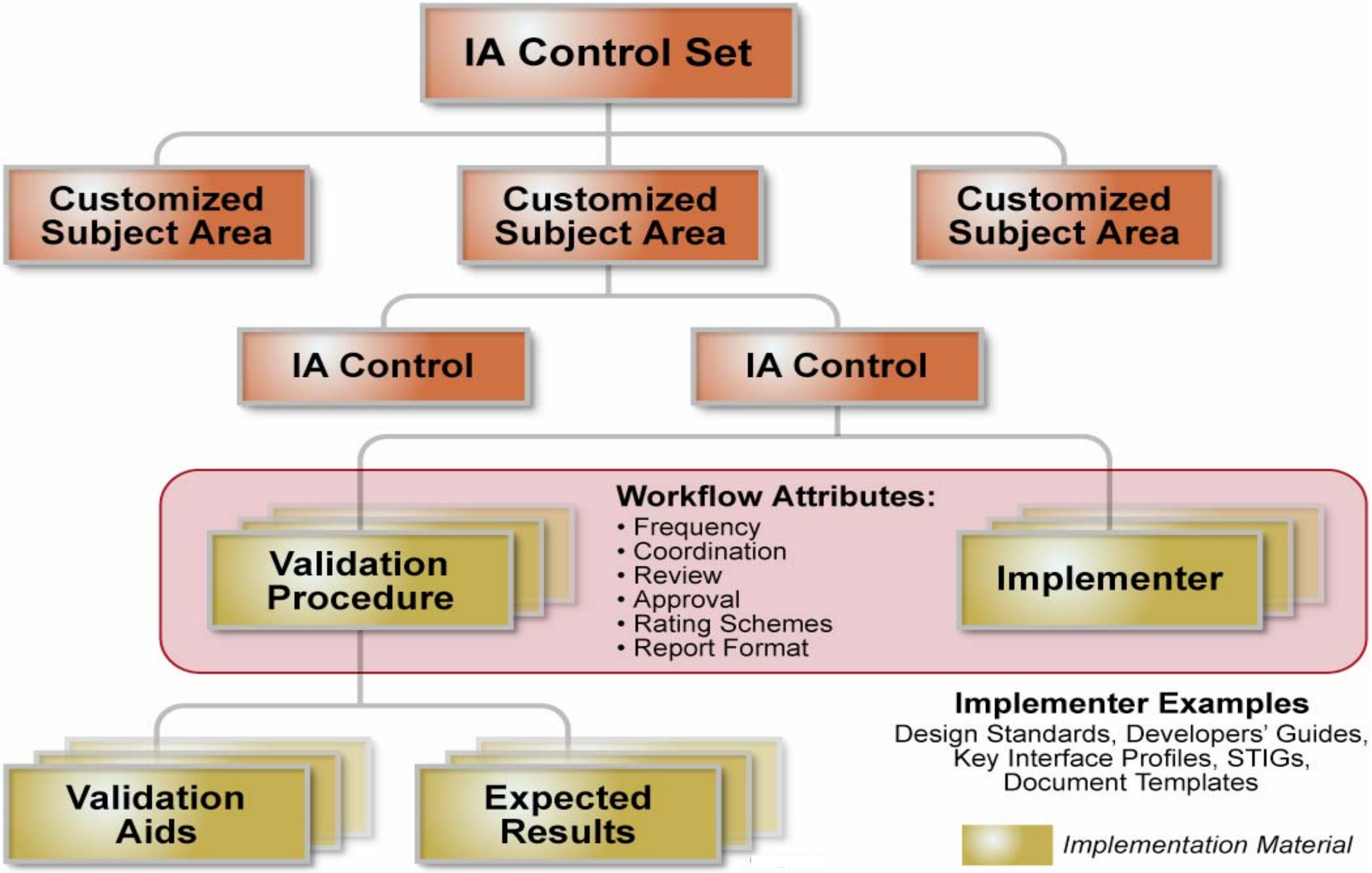
GIG Mission Areas:

- Business
- Warfighting
- National Intelligence
- Enterprise Information Environment

DoD Information Systems:

- AIS Application
- Outsourced IT-based Process
- Platform IT Interconnection
- Enclave
  - May develop classes of enclaves, *e.g.*, DMZ

The DOD IA Controls Provide Comprehensive Guidance



IA Control Set

Customized Subject Area

Customized Subject Area

Customized Subject Area

IA Control

IA Control

Validation Procedure

Workflow Attributes:

- Frequency
- Coordination
- Review
- Approval
- Rating Schemes
- Report Format

Implementer

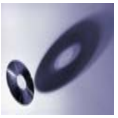
Validation Aids

Expected Results

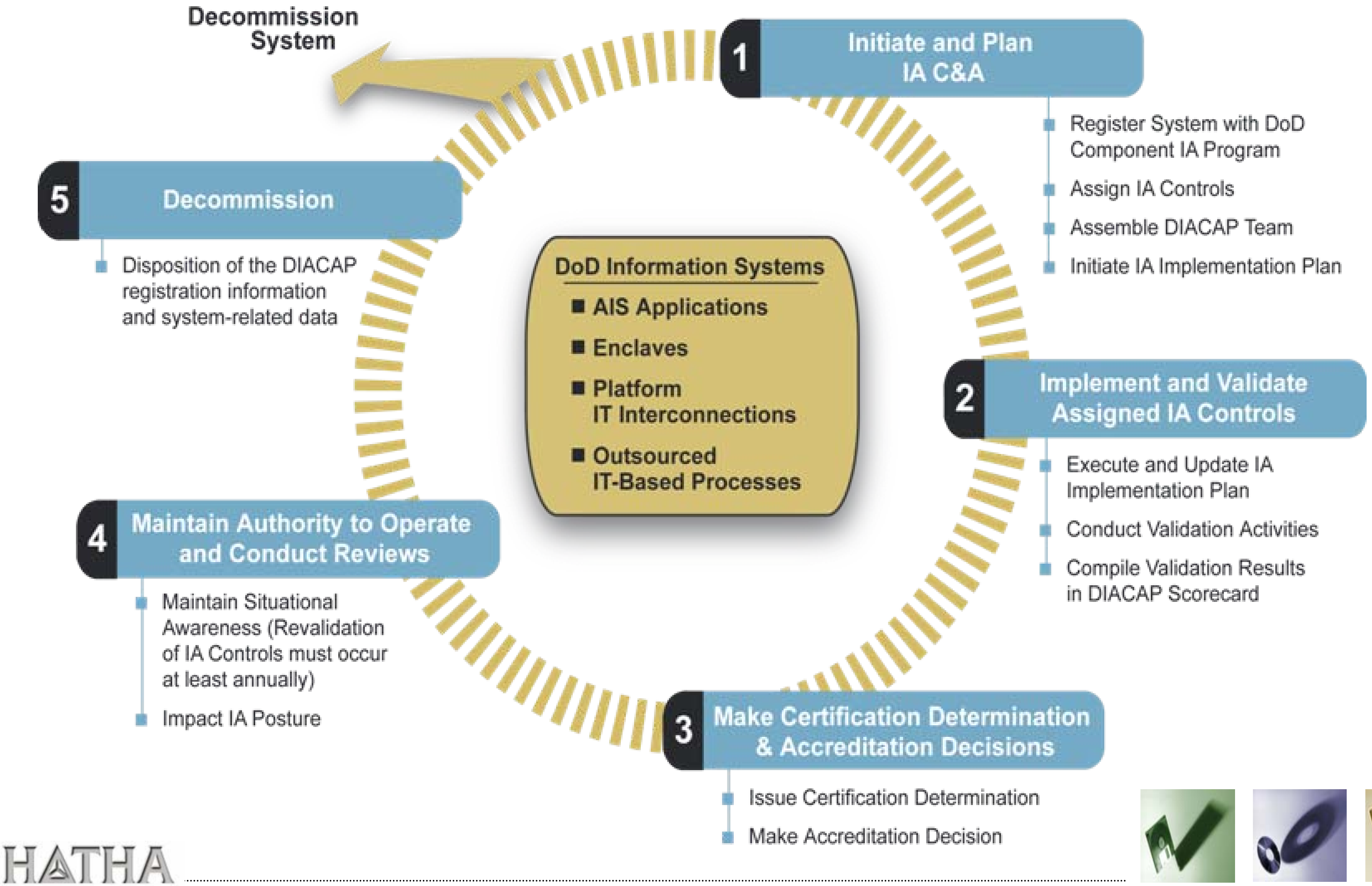
Implementer Examples

Design Standards, Developers' Guides, Key Interface Profiles, STIGs, Document Templates

▨ *Implementation Material*



The DIACAP is Distinguished by a Continuous Set of Activities



DoD Information Systems

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

1 Initiate and Plan IA C&A

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

2 Implement and Validate Assigned IA Controls

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

3 Make Certification Determination & Accreditation Decisions

- Issue Certification Determination
- Make Accreditation Decision

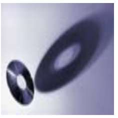
4 Maintain Authority to Operate and Conduct Reviews

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

5 Decommission

- Disposition of the DIACAP registration information and system-related data

Decommission System



Agenda

Part 1

- The C&A Challenge
- DOD’s IA Framework
- Making C&A Dynamic & Net-Centric

Part 2

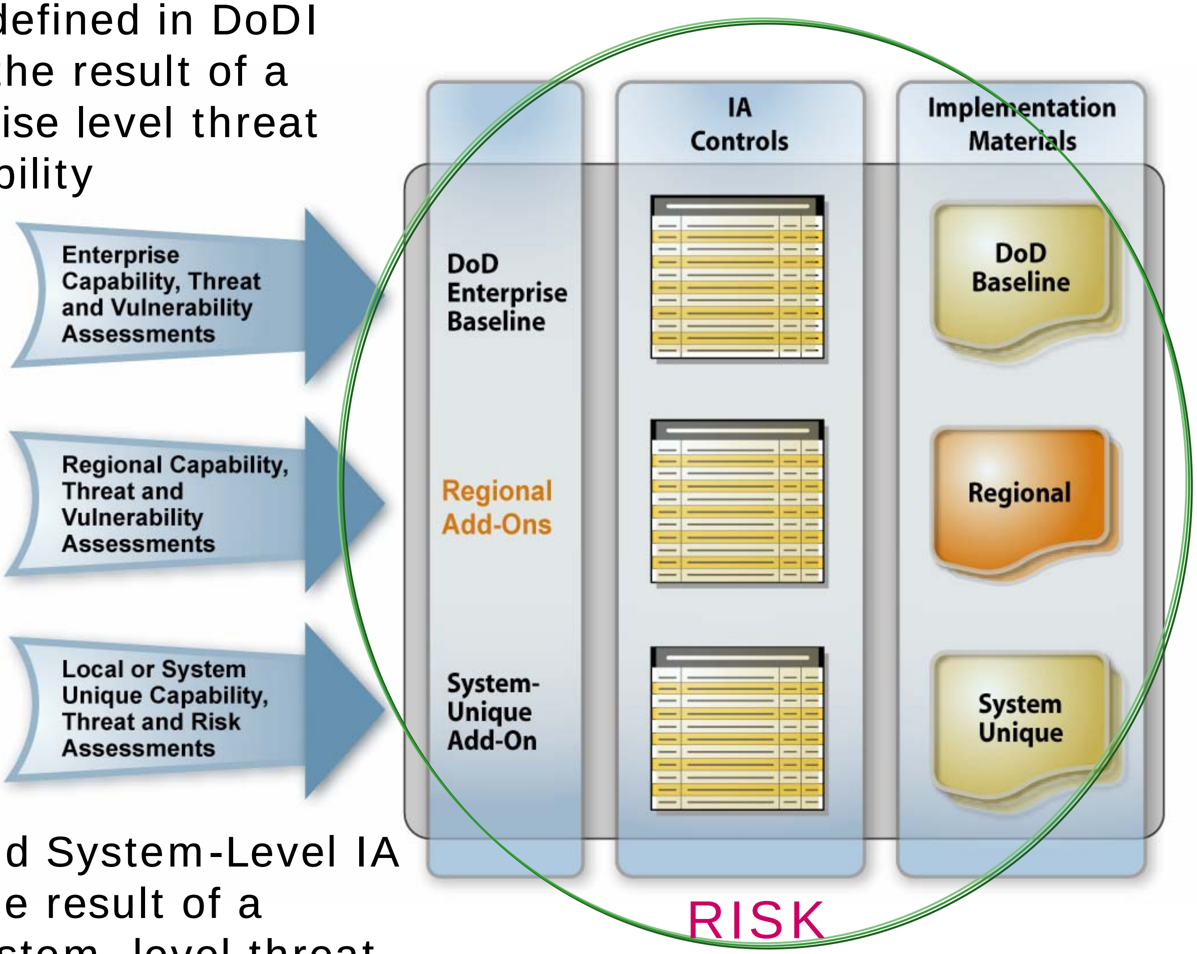
- The DIACAP
  - DIACAP Process & Package
  - Understanding DOD’s Concept of Enterprise Risk and Risk Management
  - DITSCAP – DIACAP Analysis: Similarities & Differences
  - DITSCAP to DIACAP Transition
- Applying DIACAP in the System Life Cycle

Part 3

- Supporting Tools
  - Knowledge Service Overview
  - eMASS Overview
- Summary and Questions

DIACAP Approach to Risk Management

IA controls defined in DoDI 8500.2 are the result of a DoD enterprise level threat and vulnerability assessment


Enterprise Capability, Threat and Vulnerability Assessments
Regional Capability, Threat and Vulnerability Assessments
Local or System Unique Capability, Threat and Risk Assessments
IA Controls
Implementation Materials
DoD Enterprise Baseline
Regional Add-Ons
System-Unique Add-On
DoD Baseline
Regional
System Unique

Less than Fully Implemented IA Controls = Residual Risk

Operational Impact Must be Assessed at All Levels

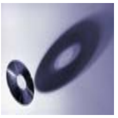
RISK MANAGEMENT

Component and System-Level IA controls are the result of a component/system level threat and vulnerability assessment.

The DIACAP Risk Decision

- The risk decision is based on an analysis of the vulnerabilities/threat posed by the partial or unsatisfactory implementation of the IA Controls

- The analysis is based on three factors:
  - The IA Control status (C/NC/NT/NA)
  - The Impact Code
  - The Severity Code



Agenda

Part 1

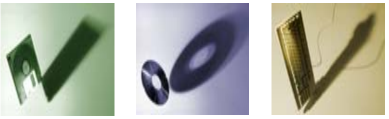
- The C&A Challenge
- DOD’s IA Framework
- Making C&A Dynamic & Net-Centric

Part 2

- The DIACAP
  - DIACAP Process & Package
  - Understanding DOD’s Concept of Enterprise Risk and Risk Management
  - DITSCAP – DIACAP Analysis: Similarities & Differences
  - DITSCAP to DIACAP Transition

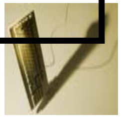
Part 3

- Applying DIACAP in the System Life Cycle
- Supporting Tools
  - Knowledge Service Overview
  - eMASS Overview
- Summary and Questions



Fundamental Differences between DITSCAP and DIACAP

Category	DITSCAP	DIACAP
System Security	• Security requirements and standards are uniquely defined by each system	• Baseline IA/Security Levels (Architecture and Controls) are established by the Enterprise
Accreditation Status	• Accreditation status is communicated via letter and status code (ATO, IATO)	• Accreditation status is communicated by assigned IA Controls and compliance ratings
Authorization Schedule	• System operation must be re-authorized not less than every three years	• IA posture must be continuously monitored and reviewed not less than annually.
C&A process	• Policy advocates tailoring, but process is hard-coded to phases.	• Steps are flexible, modular and continuous. Each system works to a POAM that aligns to SDLC
C&A Decision Structure	• Varies from component to component and from system to system • DAA and Certifier selected by/for the each system	• Is standardized and determined by the Enterprise • Certifier is a qualified, resourced, and permanent member of CIO staff
Package Format	• Narrative documents (e.g., reports and plans) • Manual process	• Structured data elements that are defined by the Enterprise • Automated tools, Enterprise managed knowledgebase



Agenda

Part 1

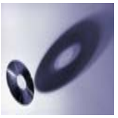
- The C&A Challenge
- DOD’s IA Framework
- Making C&A Dynamic & Net-Centric

Part 2

- The DIACAP
  - DIACAP Process & Package
  - Understanding DOD’s Concept of Enterprise Risk and Risk Management
  - DITSCAP – DIACAP Analysis: Similarities & Differences
  - DITSCAP to DIACAP Transition

Part 3

- Applying DIACAP in the System Life Cycle
- Supporting Tools
  - Knowledge Service Overview
  - eMASS Overview
- Summary and Questions



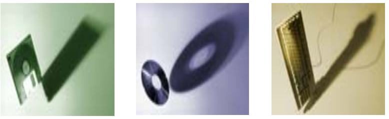
DOD faces numerous challenges to implement or transition to DIACAP effectively

- Transitioning Systems – transitioning legacy systems, and systems certified under the DITSCAP.

- Transitioning Organizations – transitioning organizations with expertise and familiarity with DITSCAP to the new DIACAP processes.

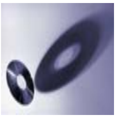
- New Starts – Implementing DIACAP for systems with no prior DITSCAP accreditation.

Addressing the need for immediate implementation and adoption of a significantly different C&A process.



DITSCAP to DIACAP Transition Timeline

- Unaccredited/new start → Initiate DIACAP now
- DIACAP initiated → Start transition now
- Phase I signed SSAA & identified IA Controls → Continue DITSCAP; develop DIACAP Implementation Plan
- Phase I signed SSAA & NO identified IA Controls → Continue DITSCAP; identify IA Controls & develop DIACAP Implementation Plan
- ATO current within 3 years → Within 180 days, develop DIACAP Implementation Plan
- ATO not current within 3 years → Initiate DIACAP



Agenda

Part 1

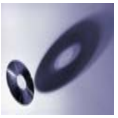
- The C&A Challenge
- DOD’s IA Framework
- Making C&A Dynamic & Net-Centric

Part 2

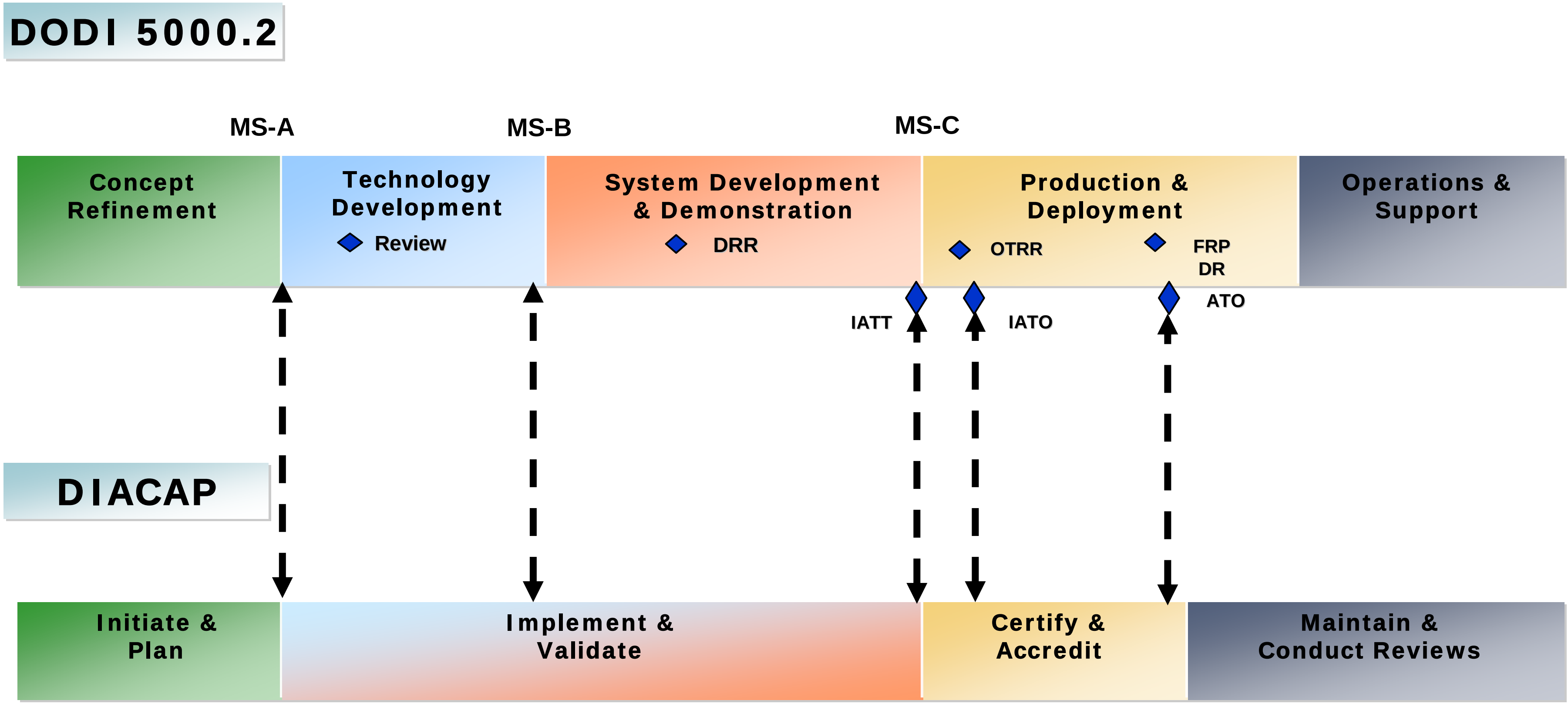
- The DIACAP
  - DIACAP Process & Package
  - Understanding DOD’s Concept of Enterprise Risk and Risk Management
  - DITSCAP – DIACAP Analysis: Similarities & Differences
  - DITSCAP to DIACAP Transition

Part 3

- Applying DIACAP in the System Life Cycle
- Supporting Tools
  - Knowledge Service Overview
  - eMASS Overview
- Summary and Questions



DIACAP – SLC Alignment & Activities



DODI 5000.2

MS-A

MS-B

MS-C

Concept Refinement

Technology Development

◆ Review

System Development & Demonstration

◆ DRR

Production & Deployment

◆ OTRR

◆ FRP DR

Operations & Support

IATT

IATO

ATO

DIACAP

Initiate & Plan

Implement & Validate

Certify & Accredit

Maintain & Conduct Reviews

Registration; IA Control Assignment; Assemble Team; SIP; Initiate DIACAP Implementation Plan

Execute Plan; Validate Controls; Compile Results; DIACAP Implementation Plan, Certification Documentation, DIACAP Scorecard

Make C&A Determination; Issue Decision

Maintain Awareness; Annual Reviews; Maintain Posture

Agenda

Part 1

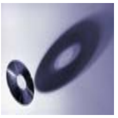
- The C&A Challenge
- DOD’s IA Framework
- Making C&A Dynamic & Net-Centric

Part 2

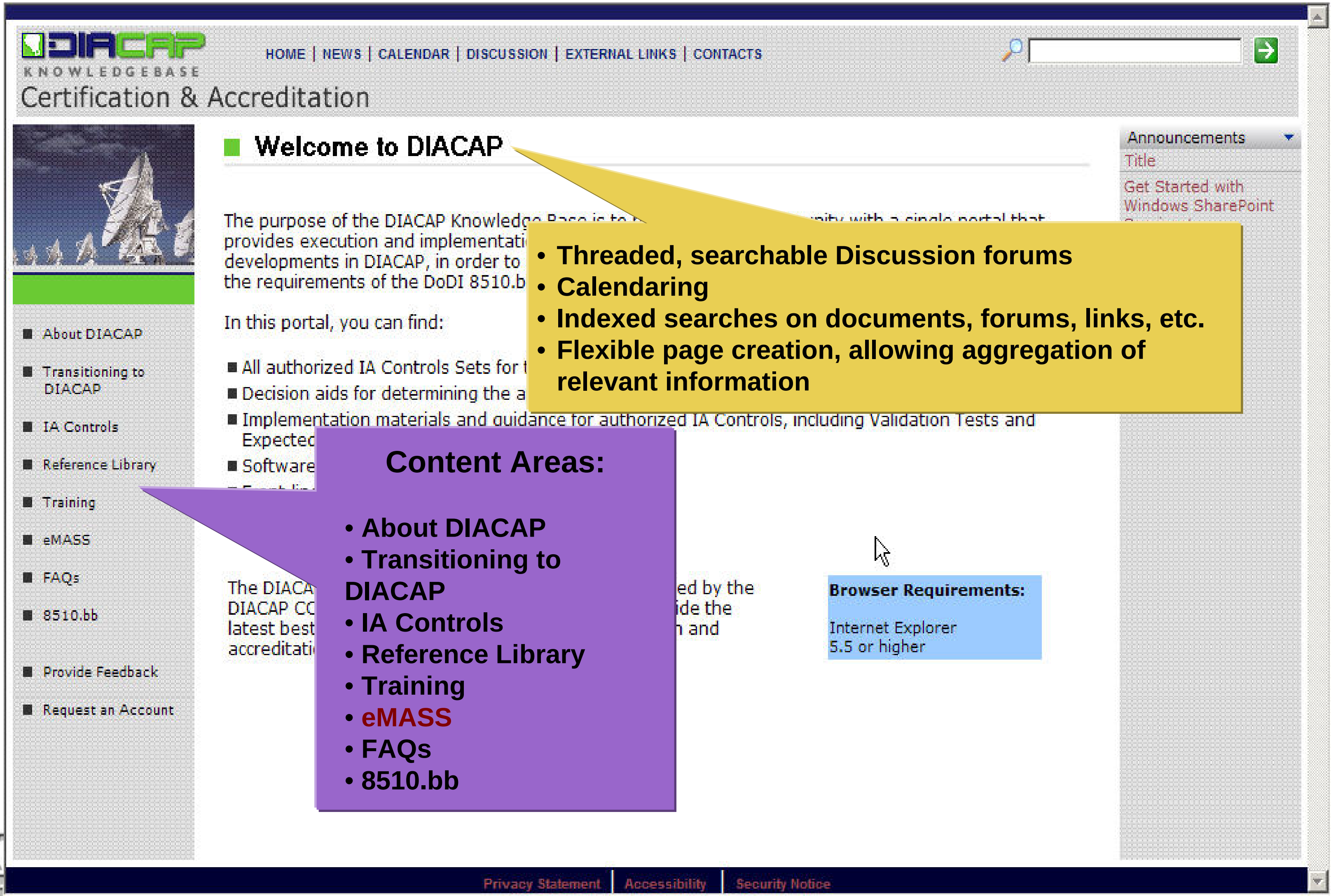
- The DIACAP
  - DIACAP Process & Package
  - Understanding DOD’s Concept of Enterprise Risk and Risk Management
  - DITSCAP – DIACAP Analysis: Similarities & Differences
  - DITSCAP to DIACAP Transition

Part 3

- Applying DIACAP in the System Life Cycle
- Supporting Tools
  - Knowledge Service Overview
  - eMASS Overview
- Summary and Questions



The Knowledge Service provides the gateway to DIACAP resources and content


DIACAP
KNOWLEDGEBASE
HOME | NEWS | CALENDAR | DISCUSSION | EXTERNAL LINKS | CONTACTS

Certification & Accreditation

Welcome to DIACAP

The purpose of the DIACAP Knowledge Base is to ... unity with a single portal that
provides execution and implementati...
developments in DIACAP, in order to ...
the requirements of the DoDI 8510.b...

In this portal, you can find:

- All authorized IA Controls Sets for t...
- Decision aids for determining the a...
- Implementation materials and guidance for authorized IA Controls, including Validation Tests and Expected...
- Software...

The DIACA... ed by the
DIACAP CC... ide the
latest best... n and
accreditati...

- About DIACAP
- Transitioning to DIACAP
- IA Controls
- Reference Library
- Training
- eMASS
- FAQs
- 8510.bb
- Provide Feedback
- Request an Account

Announcements

Title

Get Started with Windows SharePoint

Browser Requirements:

Internet Explorer 5.5 or higher

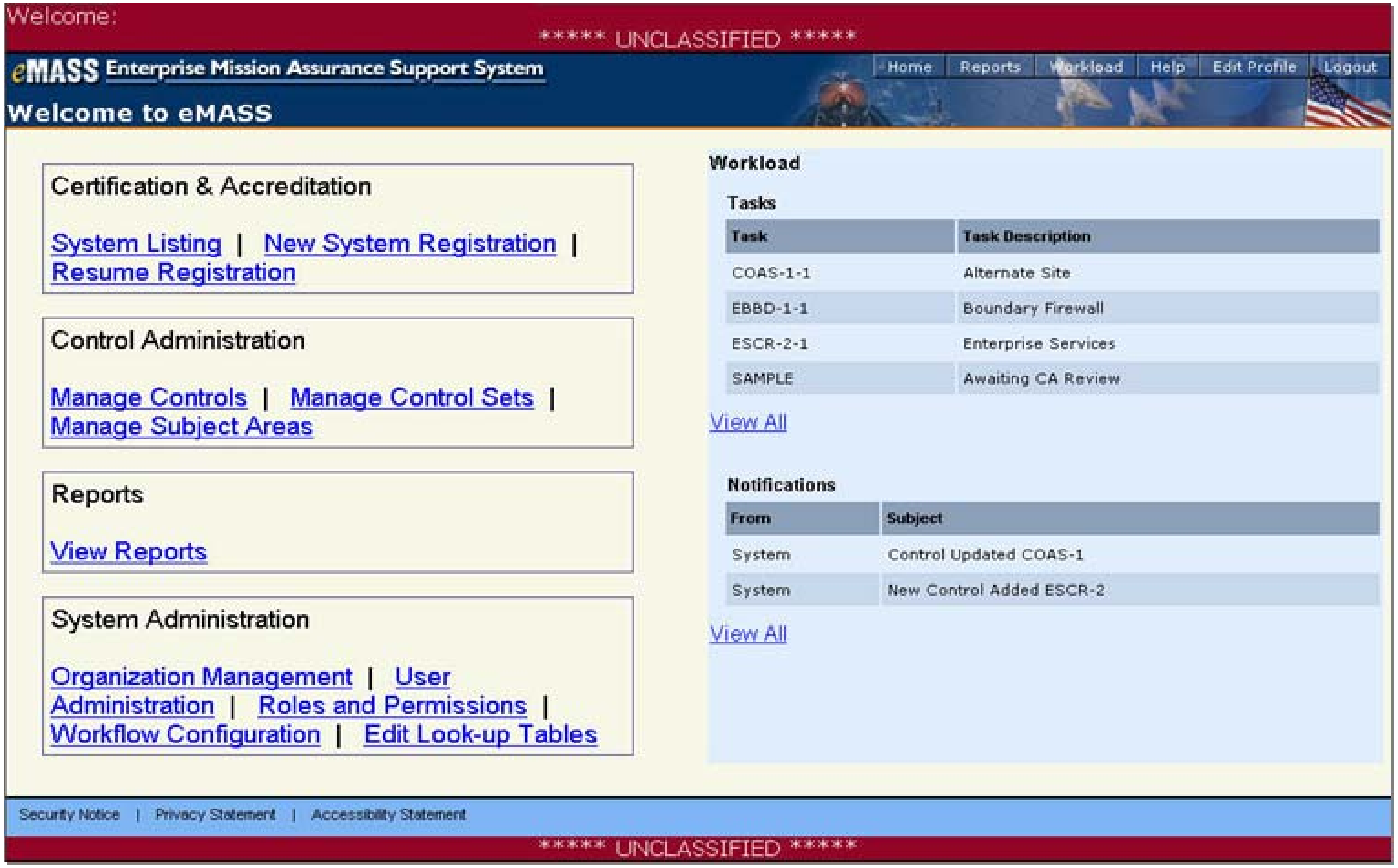
Privacy Statement | Accessibility | Security Notice

- **Threaded, searchable Discussion forums**
- **Calendaring**
- **Indexed searches on documents, forums, links, etc.**
- **Flexible page creation, allowing aggregation of relevant information**

Content Areas:

- **About DIACAP**
- **Transitioning to DIACAP**
- **IA Controls**
- **Reference Library**
- **Training**
- **eMASS**
- **FAQs**
- **8510.bb**

eMASS Landing Page Is The Gateway To Automated C&A Workflow



Welcome:

***** UNCLASSIFIED *****

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

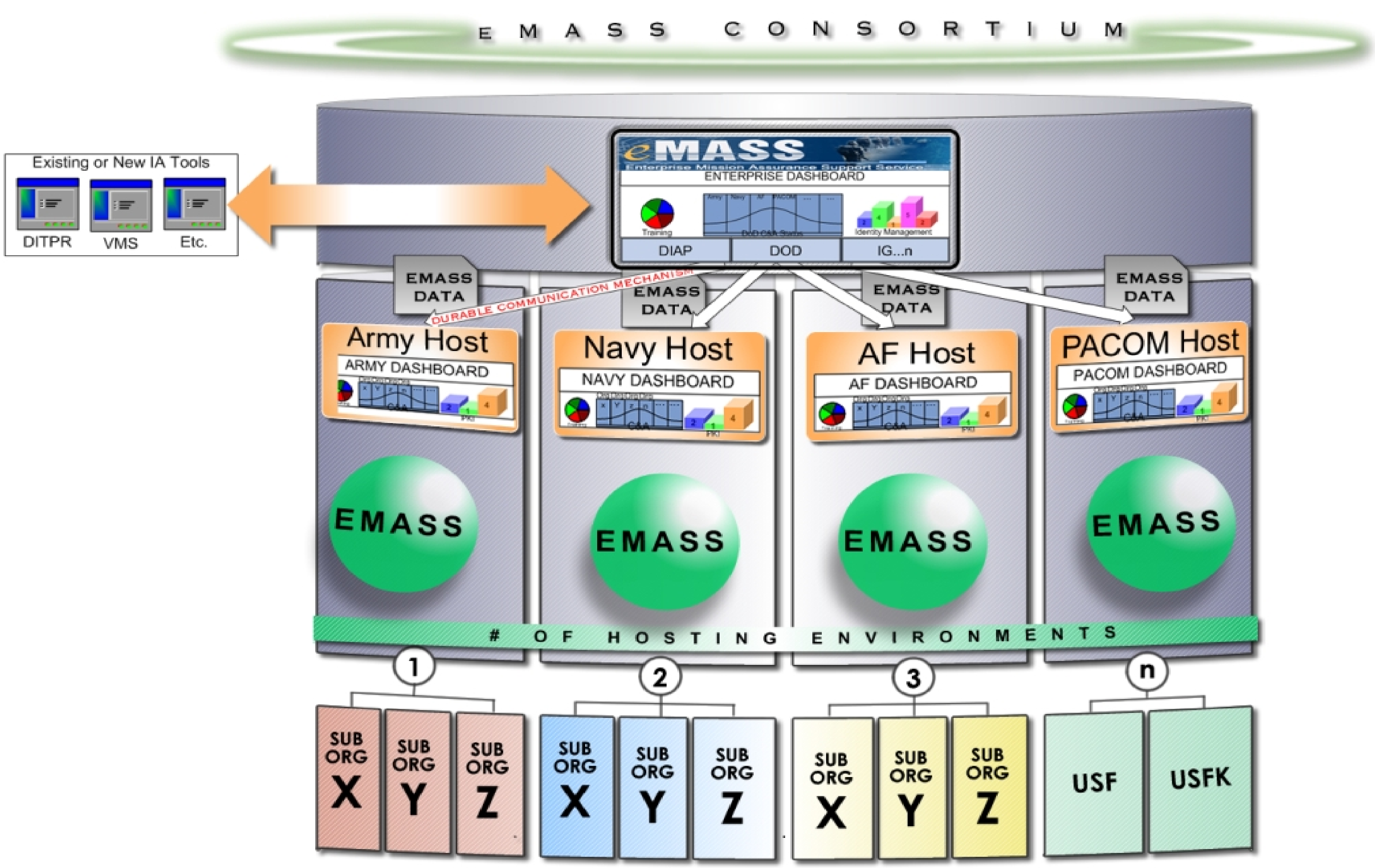
View All

Security Notice | Privacy Statement | Accessibility Statement

***** UNCLASSIFIED *****

HATHA systems

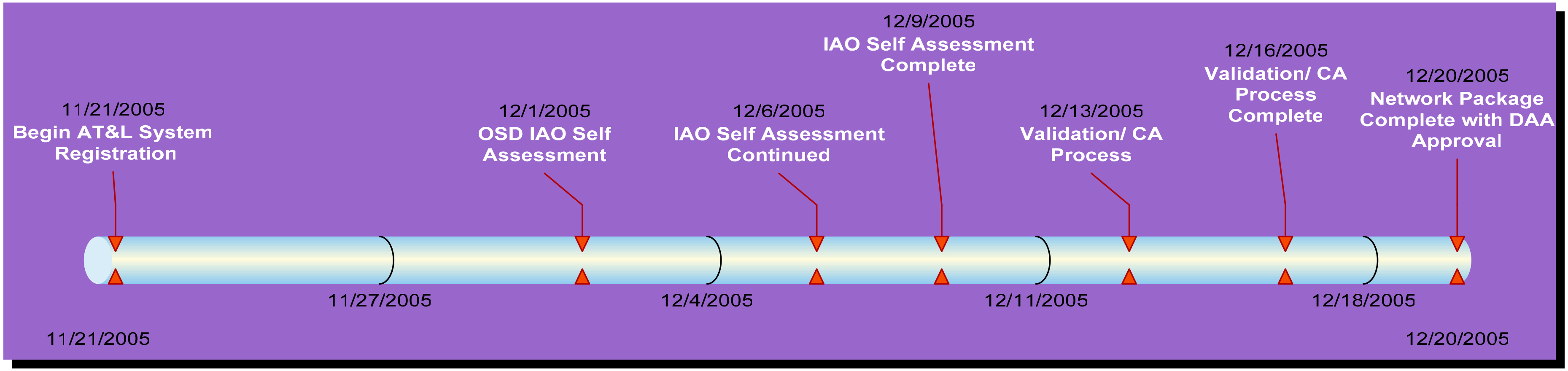
eMASS Implementation Model



HATHA systems

Using eMASS, a DOD agency was able to streamline a multi-system enclave to an IA Controls-based C&A process

- Transition timeline depicted assumed preliminary preparation:
  - Business process analysis & establishment of streamlined organization
  - Designation of responsibility & dedicated personnel
  - Training
  - Availability of comprehensive documentation



11/21/2005
Begin AT&L System Registration

12/1/2005
OSD IAO Self Assessment

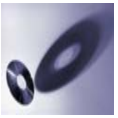
12/6/2005
IAO Self Assessment Continued

12/9/2005
IAO Self Assessment Complete

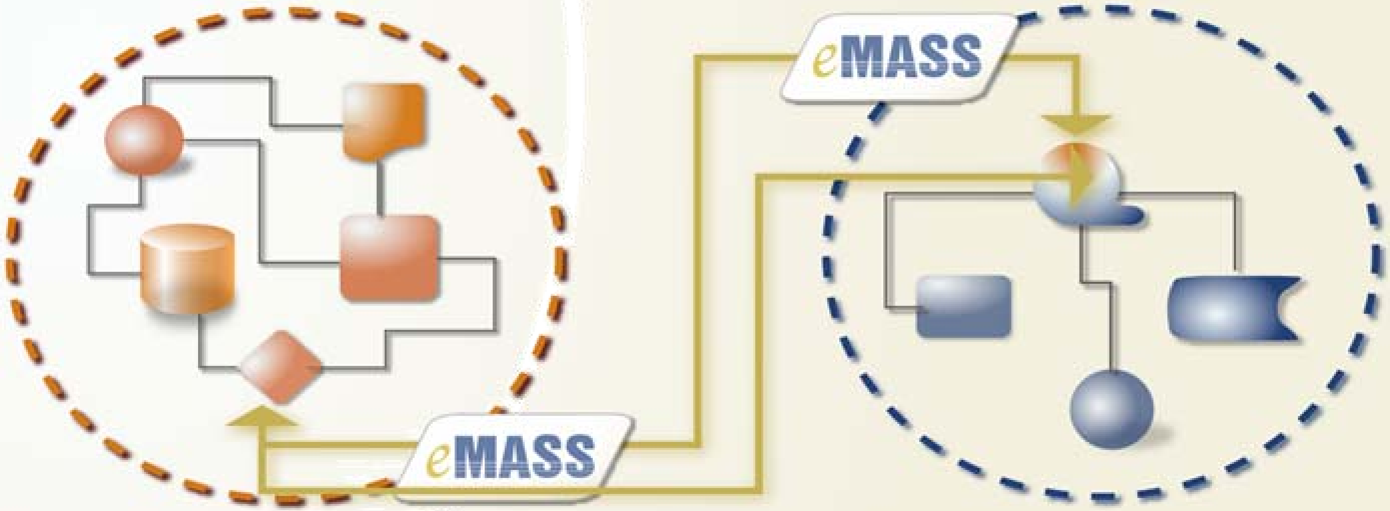
12/13/2005
Validation/ CA Process

12/16/2005
Validation/ CA Process Complete

12/20/2005
Network Package Complete with DAA Approval



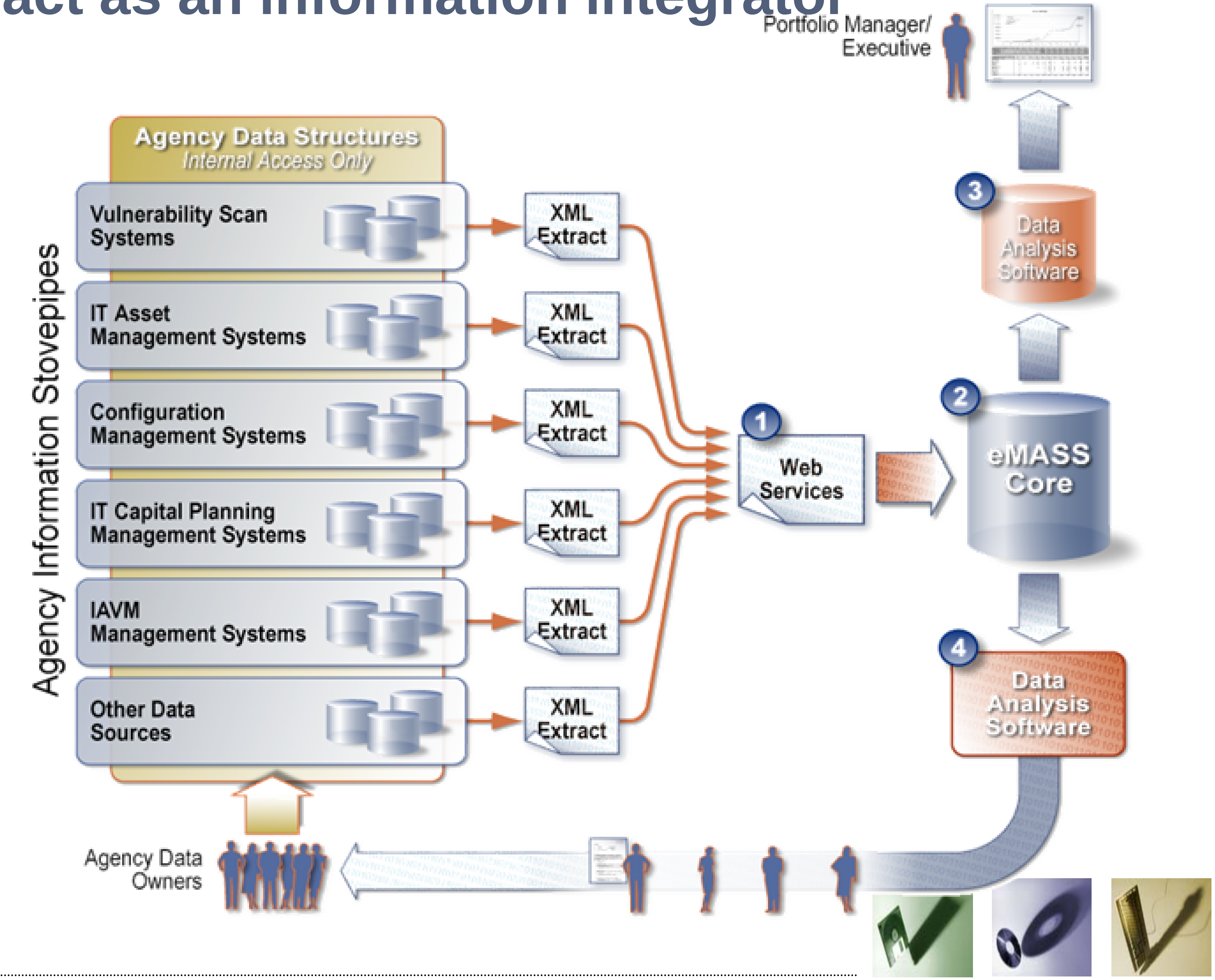
eMASS Anticipates Net-Centric need to fuse system security identity and enable the secure exchange of security credentials



- Globally Unique Digital Identity and Security Credentials for all IT Components and Complex Entities
- Privileges Dynamically Adjusted to Reflect IA Posture of GIG or Entity

An evolving suite of technologies will enable eMASS to act as an information integrator

1. eMASS reaches into existing systems to gather information from various sources
2. Data comes back to eMASS, where it is organized and combined as required to answer critical business questions
3. Data Analysis software displays data in detailed reports for Agency Executives
4. Data Analysis software uses eMASS data to support more efficient IA PM



References

- ASD NII Briefing, Department of Defense Information Assurance Workshop, February 2005
- IATAC Briefing to the FISMA IPT, June 2006

Questions & Discussion