CIO/NII
Enabling Net-Centric Operations

DoD Information Assurance (IA) Certification & Accreditation (C&A) Process (DIACAP)

for

2nd Annual NIST, NSA, DISA Security Automation Conference and Workshop

18 – 19 Sep 2006

Eustace King (eustace.king@osd.mil)
OSD/NII-IAD

Purpose

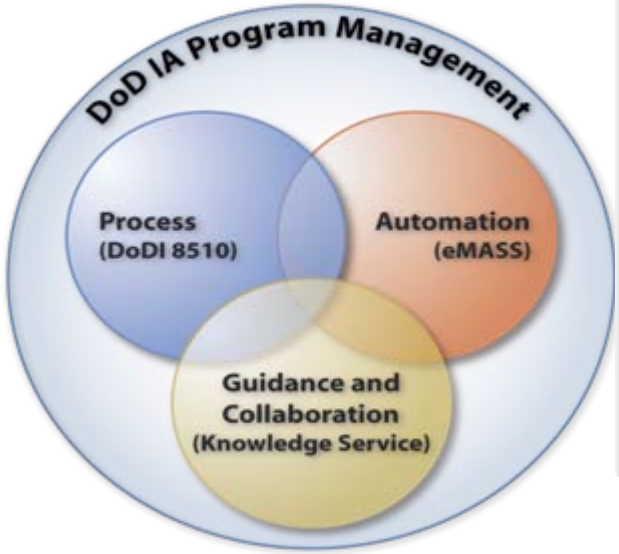
- Security Automation and the Department of Defense Information Assurance Certification & Accreditation Process (DIACAP)
  - Interim Guidance
  - The DIACAP Knowledge Service
  - The Enterprise Mission Assurance Support Service (eMASS)

- eMASS – the relevant security automation connection

Components of the DIACAP

DIACAP Interim Guidance

- Implements standard, enterprise-wide GiG-centric C&A process based on DoDI 8500.2 controls
- Supersedes DoDI 5200.40, DITSCAP, and DoDM 8510.1-M, DITSCAP Application Manual



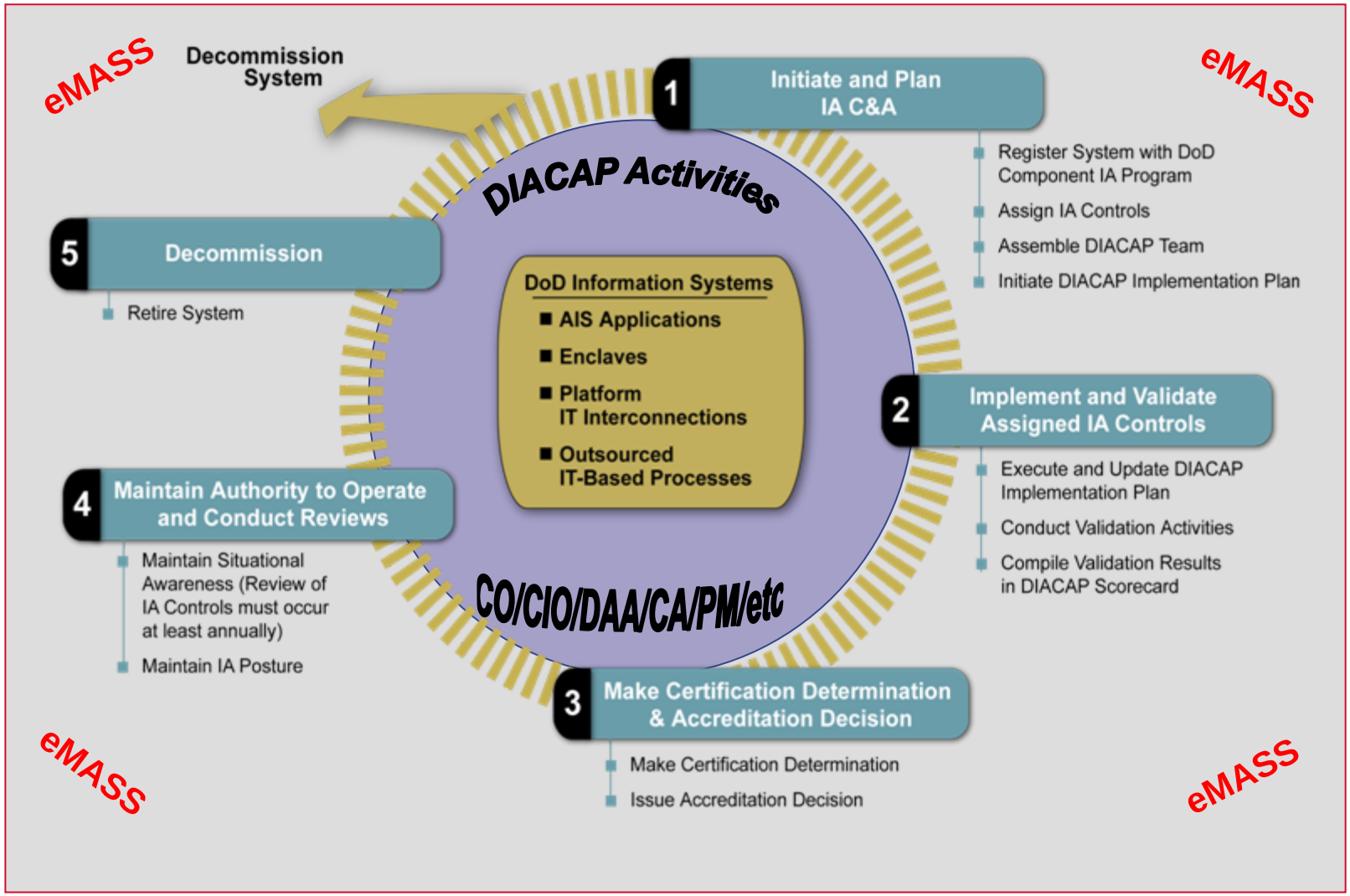
Enterprise Mission Assurance Support Service (eMASS)

- Automated life-cycle management of the DIACAP
- DoD Component and DoD CIO visibility of C&A process
- Data driven – policy and validation objects (IA Controls) can be easily and quickly updated across enterprise or tailored for COIs, applications

Web-Based DIACAP Knowledge Service (KS)

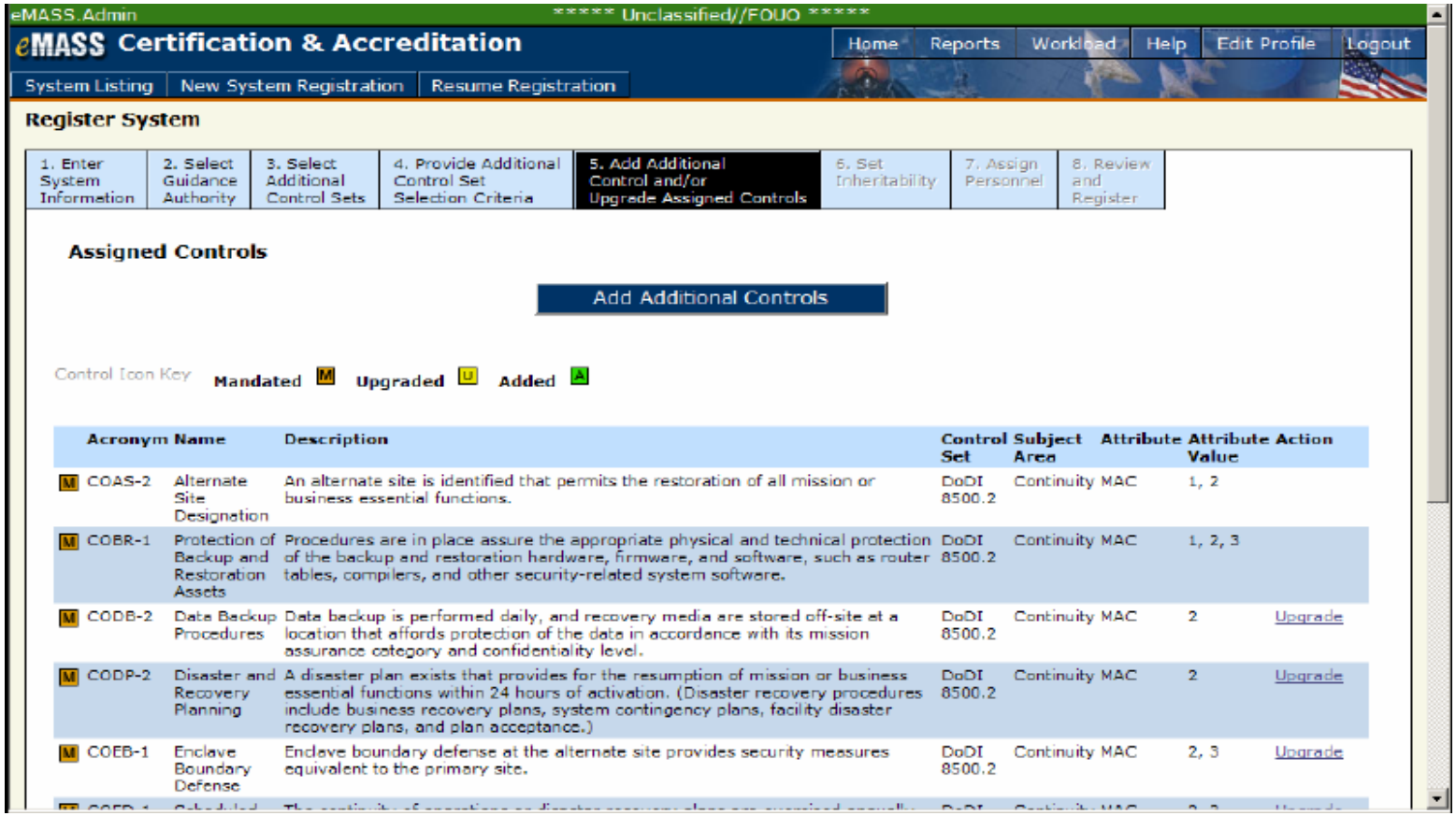
- Manages, standardizes, and makes available a C&A body of knowledge (Authoritative Source)
- Workspace for authoring, reviewing, and accepting changes to the enterprise body of knowledge (
- Collaborative space for solving C&A problems and sharing C&A news

DIACAP/eMASS
Life-Cycle Management of C&A



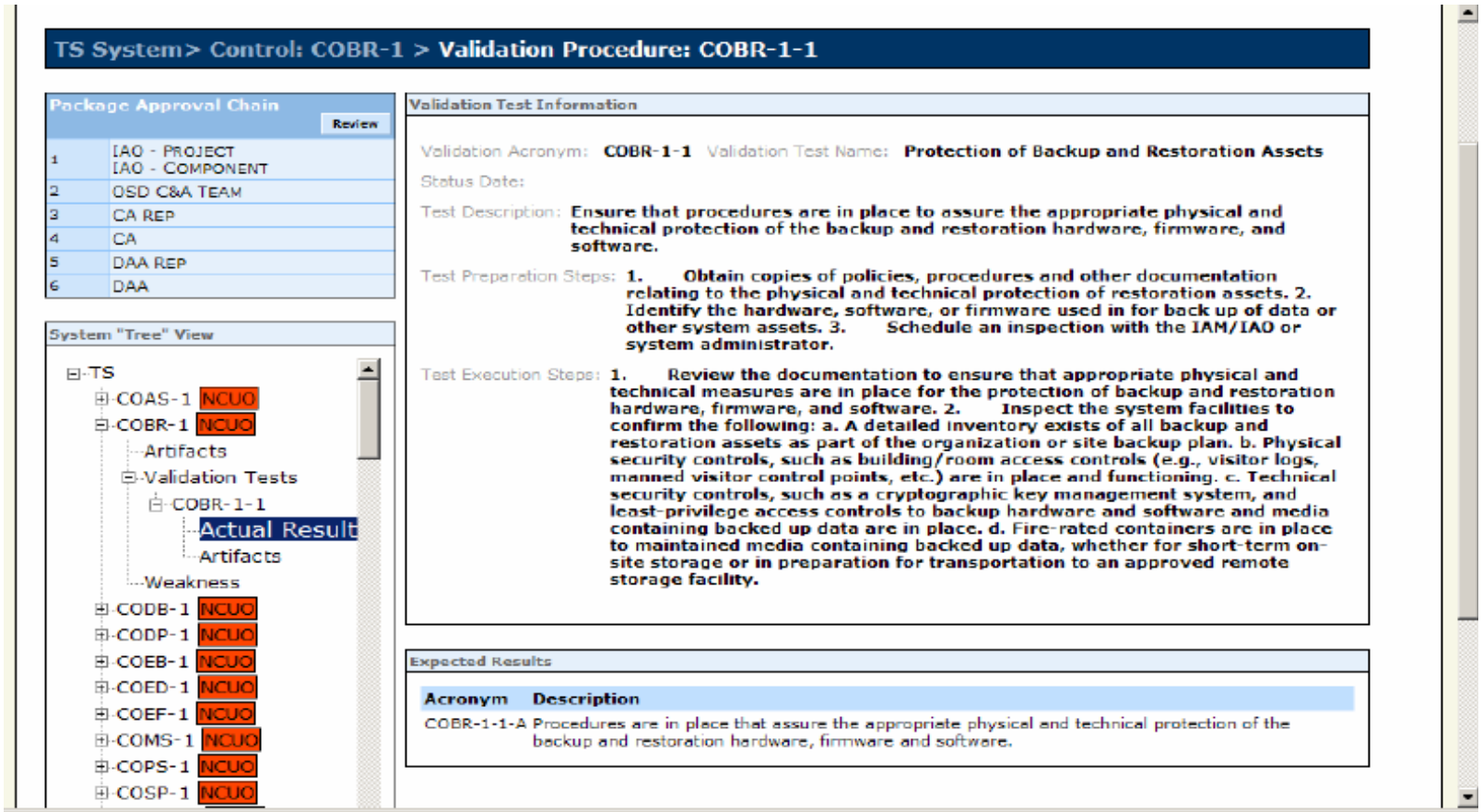
CIO/NII Enabling Net-Centric Operations

eMASS and Security Automation



	Acronym	Name	Description	Control Set	Subject Area	Attribute	Attribute Value	Action
M	COAS-2	Alternate Site Designation	An alternate site is identified that permits the restoration of all mission or business essential functions.	DoDI 8500.2	Continuity	MAC	1, 2	
M	COBR-1	Protection of Backup and Restoration Assets	Procedures are in place assure the appropriate physical and technical protection of the backup and restoration hardware, firmware, and software, such as router tables, compilers, and other security-related system software.	DoDI 8500.2	Continuity	MAC	1, 2, 3	
M	CODB-2	Data Backup Procedures	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.	DoDI 8500.2	Continuity	MAC	2	Upgrade
M	CODP-2	Disaster and Recovery Planning	A disaster plan exists that provides for the resumption of mission or business essential functions within 24 hours of activation. (Disaster recovery procedures include business recovery plans, system contingency plans, facility disaster recovery plans, and plan acceptance.)	DoDI 8500.2	Continuity	MAC	2	Upgrade
M	COEB-1	Enclave Boundary Defense	Enclave boundary defense at the alternate site provides security measures equivalent to the primary site.	DoDI 8500.2	Continuity	MAC	2, 3	Upgrade

eMASS and Security Automation



CIO/NII Enabling Net-Centric Operations

eMASS and Security Automation

Summary Scorecard Report

Generated on 14-Apr-2006 at 8:46

Controls

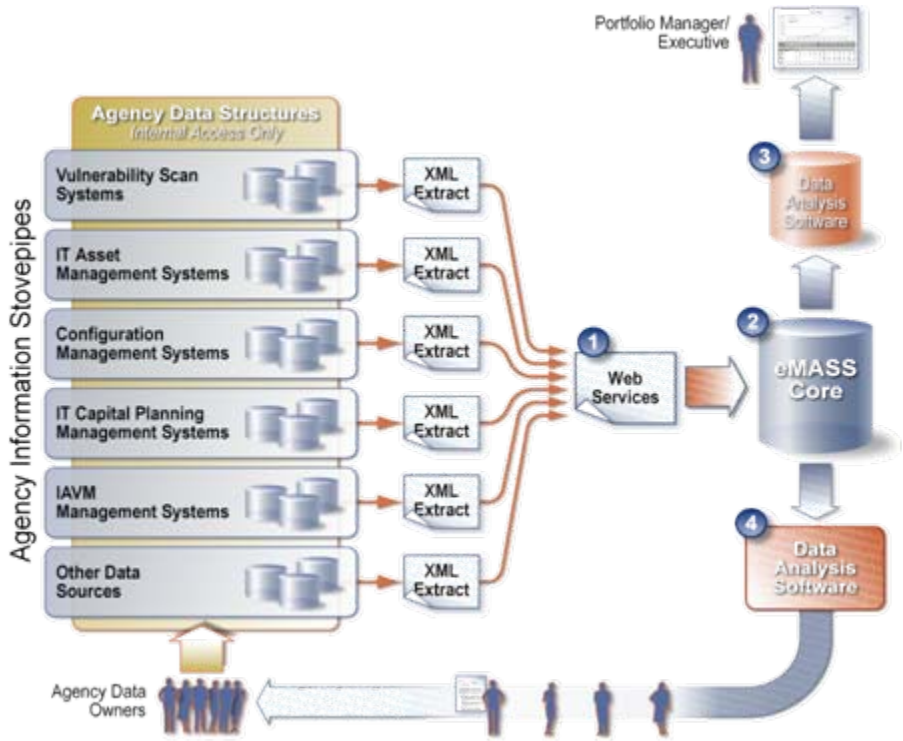
Guidance Authority: DoDI 8500.2 Control Set

Subject Area	Control Acronym	Control	Comments	Weakness Exists	Status	Impact Code
Continuity	COAS-1	Alternate Site Designation	Months	No	Non-Compliant	H
	COBR-1	Protection of Backup and Restoration Assets		No	Non-Compliant	H
	CODB-1	Data Backup Procedures		No	Non-Compliant	M
	CODP-1	Disaster and Recovery Planning		No	Non-Compliant	M
	COED-1	Enclave Boundary Defense		No	Non-Compliant	H
	COED-1	Scheduled Exercises and Drills		No	Non-Compliant	M
	COET-1	Identification of Essential Functions		No	Non-Compliant	M
	COMS-1	Maintenance Support		No	Non-Compliant	M
	COPS-1	Power Supply		No	Non-Compliant	M
	COSP-1	Spares and Parts		No	Non-Compliant	M
	COSW-1	Backup Copies of Critical SW		No	Non-Compliant	H
	COTR-1	Trusted Recovery		No	Non-Compliant	H
Security Design and Configuration	DCAR-1	Procedural Review		No	Non-Compliant	M
	DCAS-1	Acquisition Standards		No	Non-Compliant	H
	DCBP-1	Best Security Practices		No	Non-Compliant	M
	DCCB-1	Control Board		No	Non-Compliant	M
	DCCS-1	Configuration Specifications		No	Non-Compliant	H
	DCCT-1	Compliance Testing		No	Non-Compliant	M
	DCDS-1	Dedicated IA Services		No	Non-Compliant	M
	DCFA-1	Functional Architecture for AIS Applications		No	Non-Compliant	M
	DCHW-1	HW Baseline		No	Non-Compliant	H
	DCID-1	Interconnection Documentation		No	Non-Compliant	H
	DCII-1	IA Impact Assessment		No	Non-Compliant	M
	DCIT-1	IA for IT Services		No	Non-Compliant	H
	DCMC-1	Mobile Code		No	Non-Compliant	M
	DCNR-1	Non-repudiation		No	Non-Compliant	M
	DCPD-1	Public Domain Software Controls		No	Non-Compliant	M
	DCPP-1	Ports, Protocols, and Services		No	Non-Compliant	M
	DCPR-1	CM Process		No	Non-Compliant	H
	DCSD-1	IA Documentation		No	Non-Compliant	H
	DCSL-1	System Library Management Controls		No	Non-Compliant	M
	DCSQ-1	Software Quality		No	Non-Compliant	M
	DCSR-2	Specified Robustness - High		No	Non-Compliant	H
	DCSS-1	System State Changes		No	Non-Compliant	H
	DCSW-1	SW Baseline		No	Non-Compliant	H
Enclave Boundary Defense	EBBD-3	Boundary Defense		No	Non-Compliant	B
	EBCR-1	Connection Rules		No	Non-Compliant	M
	EBRP-1	Remote Access for Privileged Functions		No	Non-Compliant	H
	EBRU-1	Remote Access for User Functions		No	Non-Compliant	H
	EBVC-1	VPN Controls		No	Non-Compliant	M
Enclave Computing Environment	ECAF-1	Affiliation Display		No	Non-Compliant	M
	ECAN-1	Access for Need-to-Know		No	Non-Compliant	H
	ECAR-3	Audit Record Content - Classified Systems Audit of Security Label Changes		No	Non-Compliant	B

Impact Code: H = High; M = Medium; B = Basic

eMASS: Integrating Information in a Service Oriented Architecture

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



Bottom Line

- **Security Automation**
  - **A good thing for eMASS and the DIACAP**