

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



CIO/NII Enabling Net-Centric Operations



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





ntroductio

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)

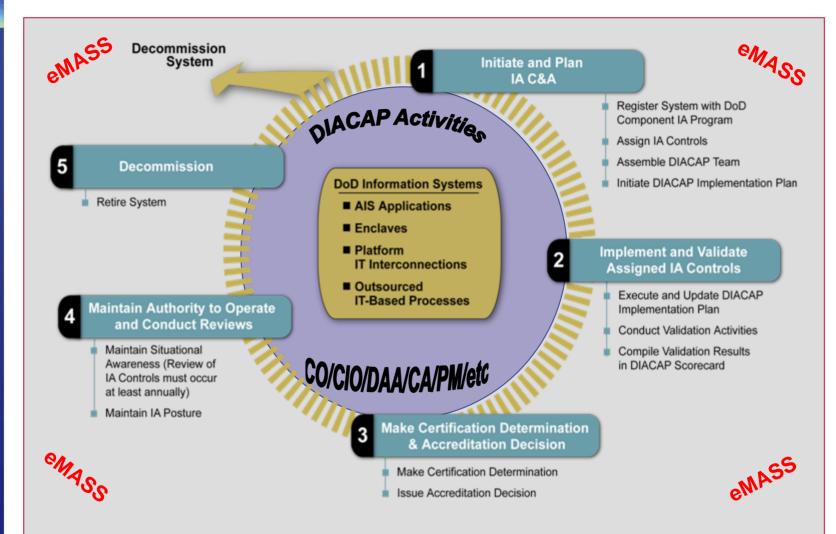
- Automated life-cycle management of the DIACAP
- DoD Component and DoD CIO visibility of C&A process
- Data driven policy and validation objects (IA Controls) can be easily and quickly updated across enterprise or tailored for COIs, applications

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

MASS Cer	tificatio	n & Accr	editation			Home	Reports	Work	load	Help	Edit Pr	ofile	Logou
ystem Listing		m Registratior		stration			1	T. J.	PA	N	5		
egister Syst	tem					Provide and						_	
System	Guidance A	dditional 0	4. Provide Additiona Control Set Selection Criteria	Control ar		6. Set Inheritabi		onnel a	8. Revier Ind Register				
Assigned	Controls												
-					different Control								
				Add Ad	ditional Control	s							
Control Icon F	(ey Mandat	ad M Haar	adad 🛄 Addad	4 A									
Control Icon H	^{(ey} Mandat	ed 📶 Upgr	aded 😐 Addeo	i 🔺									
Control Icon F	Key Mandat	ed M Upgr	aded 🛄 Addeo	1									
Control Icon F	nangat	ed M Upgr	aded 😐 Addeo	j 🔺				ol Subject	t Attri			Action	
	nangat		aded 😐 Addeo	1			Contro Set	ol Subject Area	t Attri		ttribute / alue	Action	
	Name	Description	ite is identified that		estoration of all mis	sion or		Area Continui		V		Action	
Acronym	Alternate Site Designation	Description An alternate si business esser	ite is identified that tial functions.	permits the re	estoration of all mis		Set DoDI 8500.2	Area Continui	ty MAC	V : 1,	alue	Action	1
Acronym M COAS-2	Alternate Site Designation Protection of Backup and	Description An alternate si business esser Procedures are of the backup	ite is identified that ntial functions. e in place assure th	permits the re he appropriate dware, firmwa	physical and techniare, and software, s	ical protecti	Set DoDI 8500.2	Area Continui Continui	ty MAC	V : 1,	alu c , 2	Action	1
Acronym M COAS-2	Alternate Site Designation Protection of Backup and Restoration Assets Data Backup	Description An alternate si business esser Procedures an of the backup tables, compile Data backup is location that a	ite is identified that ntial functions. and restoration har ers, and other secu s performed daily, a flords protection of	permits the re dware, firmwa rity-related sys and recovery n the data in ac	physical and techniare, and software, s	ical protecti such as rout ff-site at a	Set DoDI 8500.2	Area Continui Continui	ity MAC	V : 1,	alue , 2 , 2, 3	Action	
Acronym M COAS-2 M COBR-1 M CODB-2	Alternate Site Designation Protection of Backup and Restoration Assets Data Backup Procedures	Description An alternate si business esser Procedures an of the backup tables, compile Data backup is location that a assurance cate	ite is identified that ntial functions. and restoration har ers, and other secu s performed daily, a fords protection of egory and confident	permits the re dware, firmwa rity-related sys and recovery n the data in ao tiality level.	physical and techn are, and software, s stem software. media are stored of cordance with its m	ical protecti such as rout ff-site at a hission	Set DoDI 8500.2 on DoDI =r 8500.2 DoDI 8500.2	Area Continui Continui	Ity MAC	1, 1, 2	alue , 2 , 2, 3	<u>Upgrade</u>	
Acronym M COAS-2	Alternate Site Designation Protection of Backup and Restoration Assets Data Backup Procedures	Description An alternate si business esser Procedures an of the backup tables, compile Data backup is location that a assurance cate A disester plan essential funct include busine	ite is identified that ntial functions. e in place assure th and restoration har ers, and other secu s performed daily, ffords protection of spory and confiden n exists that provid- ions within 24 hour	permits the re dware, firmwa rity-related sy: and recovery n the data in ao tiality level. es for the resu s of activation. system conting	physical and techn are, and software, s stem software. media are stored of	ical protecti such as rout ff-site at a nission or business y procedure	Set DoDI 8500.2 DoDI er 8500.2 DoDI 8500.2 DoDI	Area Continui Continui Continui	Ity MAC	1, 1,	alue , 2 , 2, 3		
Acronym M COAS-2 M COBR-1 M CODB-2	Alternate Site Designation Protection of Backup and Restoration Assets Data Backup Procedures Disaster and Recovery	Description An alternate si business esser Procedures arro of the backup tables, compile Data backup is location that a assurance cott A disaster plan essential funct include busine recovery plane Enclave bound	ite is identified that atial functions. and restoration has ers, and other secu fords protection of egory and confident n exists that provid- ions within 24 hour ss recovery plans, s, and plan accepta	permits the re dware, firmwa rity-related sys and recovery n the data in ac tiality level. es for the resu s of activation. system conting ncc.)	physical and techn are, and software, s stem software. media are stored of cordance with its m imption of mission of . (Disaster recover	ical protecti such as rout ff-site at a nission or business y procedure r disaster	Set DoDI 8500.2 DoDI er 8500.2 DoDI 8500.2 DoDI	Area Continui Continui Continui Continui	ity MAC ity MAC ity MAC	2 2	alue , 2 , 2, 3	<u>Upgrade</u>	





eMASS and Security Automation

TS System> Control: COBR-1 > Validation Procedure: COBR-1-1

Pac	kage Approval Chain		Validation Test Information
		Review	
1	IAO - PROJECT IAO - COMPONENT		Validation Acronym: COBR-1-1 Validation Test Name: Protection of Backup and Restoration Assets Status Date:
2	OSD C&A TEAM		Status Date:
3	CA REP		Test Description: Ensure that procedures are in place to assure the appropriate physical and
4	CA		technical protection of the backup and restoration hardware, firmware, and software.
5	DAA REP		The base of the second se
6	DAA		Test Preparation Steps: 1. Obtain copies of policies, procedures and other documentation relating to the physical and technical protection of restoration assets. 2. Identify the hardware, software, or firmware used in for back up of data or other system assets. 3. Schedule an inspection with the IAM/IAO or
Syst	em "Tree" View		system administrator.
•	TS DECOAS-1 NCUO DECOBR-1 NCUO COBR-1 NCUO COBR-1-1 COBR-1-1 COBR-1-1 COBR-1-1 COBR-1-1 COBR-1-1 COBR-1-1 CODB-1 NCUO DECODP-1 NCUO	esult	Tast Execution Steps: 1. Review the documentation to ensure that appropriate physical and technical measures are in place for the protection of backup and restoration hardware, firmware, and software. 2. Inspect the system facilities to confirm the following: a. A detailed inventory exists of all backup and restoration assets as part of the organization or site backup plan. b. Physical security controls, such as building/room access controls (e.g., visitor logs, manned visitor control points, etc.) are in place and functioning. c. Technical security controls, such as a cryptographic key management system, and least-privilege access controls to backup hardware and software and media containing backed up data are in place. d. Fire-rated containers are in place to maintained media containing backed up data, whether for short-term onsite storage facility.
	D-COEB-1 NCUO		Expected Results
	B-COED-1 NCUO		Acronym Description
	D-COEF-1 NCUO		COBR-1-1-A Procedures are in place that assure the appropriate physical and technical protection of the
	COMS-1 NCUO		backup and restoration hardware, firmware and software.
	D-COPS-1 NCUO		
	COSP-1 NCUO		





eMASS and Security Automation

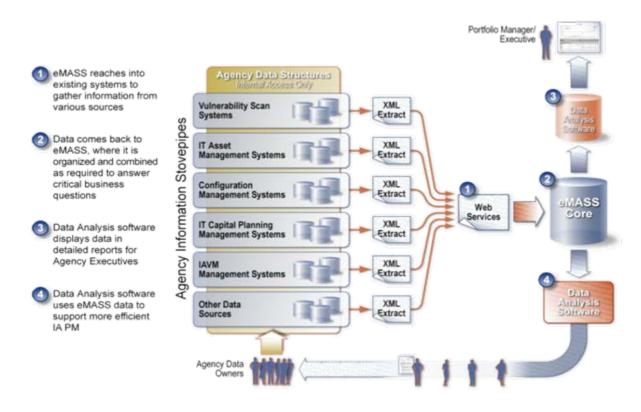
Summary Scorecard Report

Controls Guidance Authority: DoDI 8500.2 Control Set							
Subject Ares	Control Acronym	Control	Comments	West-rece Edele	Diskus	Code	
Continuity	COA9-1	Alternate Sile Designation	fénalda	No	Non-Compliant	н	
	COBR-1	Protection of Backup and Restoration Assets		No	Non-Complant		
		Cate Eachup Procedures		hio	Non-Compliant		
	0005-1	Disaster and Recovery Flancing		No	Non-Compliant		
	COE1-1	Endeve Boundary Defense		No	Non-Compliant	н	
		Scheduled Exercises and Drills		No	Non-Compliant		
	COEF-1	Identification of Essential Functions		No	Non-Cemplani		
		Mainienance Support		No	Non-Compliant		
		Fower Supply		No	Non-Compliant		
		Spares and Parts		No	Non-Compliant		
		Backup Copies of Onlical GW		No	Non-Compliant	н	
		Truded Recovery		No	Non-Compliant	н	
Security Design and Configuration		Procedural Review		No	Non-Compliant		
		Appliation Standards		No	Non-Compliant	н	
		Best Security Practices		No	Non-Compliant		
		Control Board Configuration Specifications		No	Non-Compliant		
				No	Non-Compliant		
		Compliance Testing Dedicated IA Services		110	Non-Compliant Non-Compliant	- 2	
		Punctional Architecture for AIS		No	Non-Compliant		
		Applications				_	
	DCHWH1	PW lassing		No	Non-Compliant		
	606-1	Interconnection Occurrentation		No	Non-Compliant	н	
	DC8-1	UA Impact Assessment		No	Non-Compliant	-	
	DOIT-1	UA for IT Dervices		No	Non-Compliant	н	
	DOMO-1	Mublie Code		110	Non-Compliant		
		Non-reputation		No	Non-Compliant		
	COP0-1	Public Domain Goffware Controls		No	Non-Compliant		
		Pots, Protocols, and Services		No	Non-Compliant		
		CM Process		No	Non-Compliant		
		UA Documentation		No	Non-Compliant	н	
		System Library Management Controls		No	Non-Compliant		
		Software Cuality		No	Non-Compliant		
		Operated Accounteess - High		110	Non-Compliant	н	
		System State Charges		No	Non-Compliant	H	
		GW Baseline		No	Non-Compliant		
Endow Boundary Colores		Boundary Defense		No	Non-Compliant Non-Compliant		
		Connection Rules Remote Access for Privileged		No	Non-Compliant		
		Punchana					
		Remain Ascess for User Functions		No	Non-Complian		
		VIN Costrals		No	Non-Compliant		
Endow Computing Endowment		Affiliation Clepiay		No	Non-Compliant		
		Access for Nand-Know Audit Record Content -		No	Non-Compliant Non-Compliant	H	



Impact Code: H = High; H = Hedlam; B = Back

eMASS: Integrating Information in a Service Oriented Architecture



CIO/NII Enabling Net-Centric Operations





Bottom Line

Security Automation

