

Compliance Challenges, Successes, and Improvements

- **President's Management Agenda, FISMA Requirements, and Achieving Secure Configurations and Vulnerability Management**
- **IT Security Program Management**
 - **Cyber Security Assessment and Management (CSAM)**
 - **Risk Assessment**
 - **Risk Control Requirements Determination**
 - **Security Category**
 - **Scope**
 - **Inheritance**
- **IT Security Dashboard**

National Security Automation Conference & Workshop

September 18, 2006



Planning

Implementing

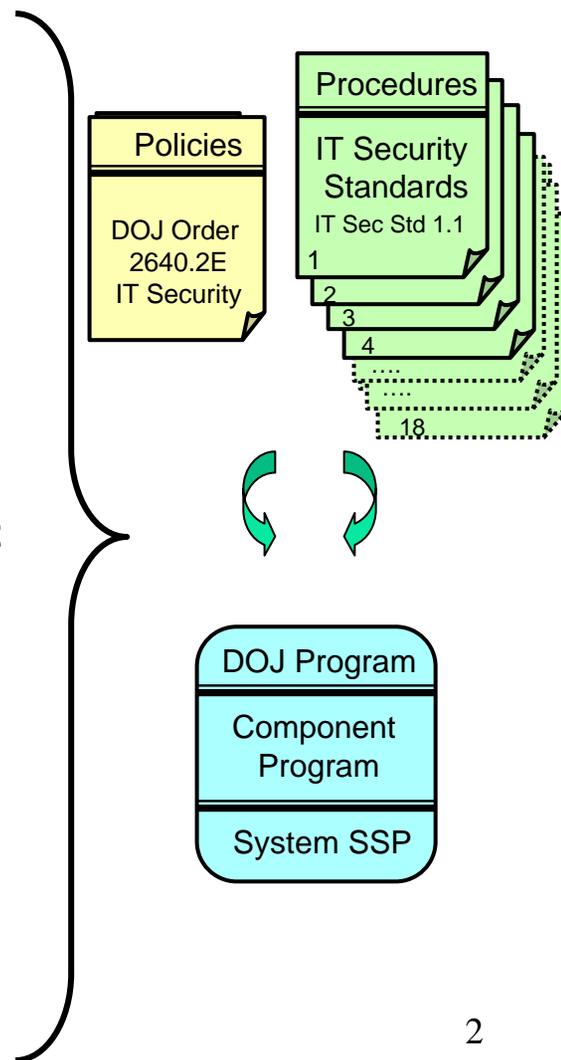
Dennis Heretick
Deputy CIO, IT Security
Department of Justice
Dennis.heretick@usdoj.gov



President's Management Agenda

FISMA Requirements: Department-wide IT Security Program

- **Maintain 100% C&A for Operational Systems.**
- **Evaluate 96% of security control implementation status against the IT Security Standards** (using the Department's
 - Up to Date IT Security Plan/Risk Assessment
 - Security Controls Evaluated (New Controls for 2006)
 - Incident Response and Contingency Plans Tested
 - Systems Installed IAW Security Configurations (CIS Std.)
- **Comprehensive Agency-wide Plan of Actions and Milestones (POA&M) for all Known System Weaknesses – Independently Verified by the Inspector General**
- **Achieve Secure Configurations and Vulnerability Management**
 - **Current Tools**
 - Conduct monthly vulnerability scans (commercial or open source), weekly if appropriate
 - Configuration security validation
 - Database applications vulnerability assessments
 - Web application vulnerabilities
 - Automated reporting
 - **Future tools**
 - NIST Checklist and automated commercial or open source tool

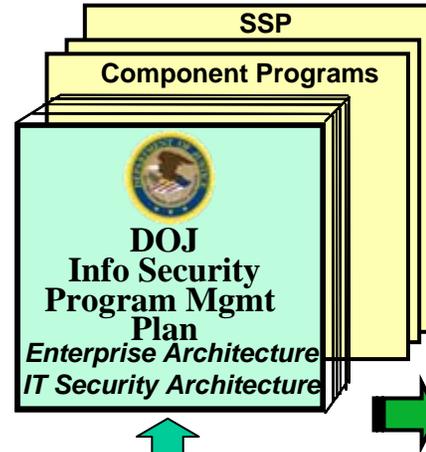
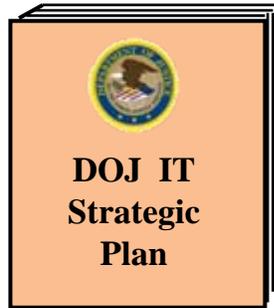




IT Security Program Management

“Line of Sight” from Mission Goals to
IT Security Program Implementation Metrics

Public Law, National Level And DOJ IT Security Policy
& Direction



Central DOJ Focus



**Justice
IT Security Council**

- IT Security Project Teams
- Policy & Control Guidelines
- Implementation Planning & Priority
- Performance Metrics & Report Card
- Training



IT Security Projects/Performance Areas

1. Certification & Accreditation Mgmt

- Cyber Security Assessment & Mgmt (CSAM)
 - Trusted agent FISMA
 - C&A Client Application

2. Computing Environment & Enclave Boundary Defense (CEED)

- Boundary Defense (Firewalls, IDS, and Anti-Virus)
- Vulnerability Mgmt
- Configuration Mgmt
- Endpoint Security
- Security Operations Center
- Identity & Access Mgmt
- JutNet Security

3. Cyber Defense Operations

- Incident Response
- Patch management

4. Contingency Planning

5. Training

- Awareness
- IT Professional

6. Configuration Management

- CCB Charter
- CM Baseline

Security & Emergency Planning Staff

7. Personnel Security

8. Physical & Environmental Security

9. Production Input/Output Control



Cyber Security Assessment and Management (CSAM)

PRESIDENTS MANAGEMENT AGENDA

FISMA, DCID 6/3
DOJ IT SECURITY STDS
FISCAM, FIPS/NIST 800-53



Management Controls

Cost + Implementation Guidance

- RA-1 Risk Assessment and Procedures
- PL-1 Security Planning Policy and Procedures.
- SA-1 System & Services Acquisition Policy & Procedures
- CA-1 Certification & Accreditation & Security Assessment Policies and Procedures.

Operational Controls

Cost + Implementation Guidance

- PS-1 Personnel Security Policy & Procedures
- PE-1 Physical Environmental Protection Policy & Procedures
- CP-1 Contingency Planning Policy & Procedures
- CM-1 Configuration Management Policy & Procedures.

Technical Controls

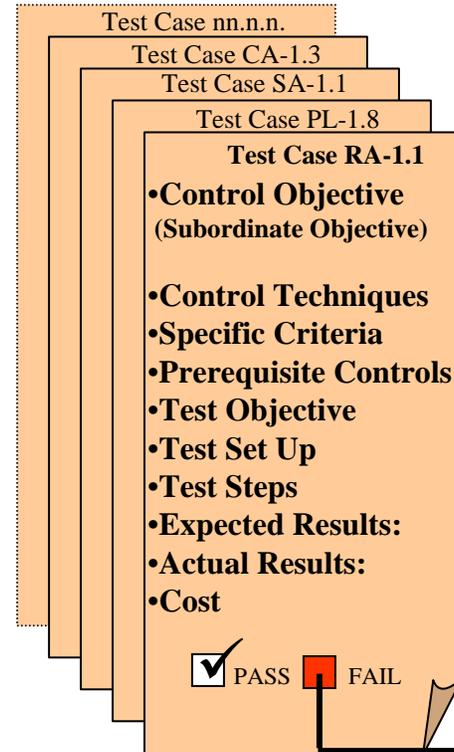
Cost + Implementation Guidance

- IA-1 Identification and Authentication Policy & Procedures
- AC-1 Access Control Policy & Procedures
- AU-1 Audit & Accountability Policy & Procedures
- SC-1 System & Comm Protection Policy & Procedures.

Implementation Requirements

Risk Weight	System Controls			Common Controls		
	L	M	H	L	M	H
4	X			X		
2	X	X		X	X	
2	X		X	X		X
5				X		
4	X			X		
2		X			X	
2		X			X	
2		X			X	
4	X			X		
2	X	X		X	X	
4	X			X		
2	X	X	X	X	X	X
4	X			X		
2		X	X		X	
2	X			X		
2	X			X		
2		X			X	
2		X			X	
4				X		
2		X			X	
2	X	X		X	X	
4	X			X		
2				X		
5				X		
4	X			X		
3				X		
2	X		X	X		X
3	X	X		X	X	

Test Case for Each Requirement



Risk Assessment

$$\begin{matrix} \text{Vulnerability} \\ \text{Control Level} \end{matrix} \times \begin{matrix} \text{Vulnerability} \\ \text{Level} \end{matrix} \times \begin{matrix} \text{Threat} \\ \text{Level} \end{matrix} \times \begin{matrix} \text{Significance} \\ \text{Level} \end{matrix} = \text{Total Risk}$$

Plans of Action & Milestones (POA&M)

OMB
FISMA
Reporting



Cyber Security Assessment & Mgmt Trusted Agent (CSAM)



Vulnerabilities Requiring Correction

- Risk Impact: _____
- Plan Start: _____
- Actual Start: _____
- Planned Finish: _____
- Actual Finish: _____
- Validation Date: _____
- Cost: _____



Risk Assessment

Vulnerability/ Countermeasures and Threat Pairing (Security Controls)	Vulnerability Level X Threat Level X Significance Level = Total Risk													
	EX-CT = Total				C+H+G-A-D = Total				DL+Ops+Equip = Total					
Vulnerability/ Countermeasures	Threat/s	Exploitability (HI=5 Low=1)	(Actual) Counter Measures (Weak=0 Very Strong=2)	Total (0-5)	Capability (HI=2 Low=1)	History/Gain (HI=2 Low=1)	Attributable/Detectable (Easy=2 Difficult=0)	Total (0-6)	Loss of Life (Yes=4 No=0)	Sensitivity (Yes=4 No=0)	Ops Impact (Yes=2 No=0)	Equipment Loss (Yes=2 No=0)	TOTAL (0-4)	RISK TOTAL (VL*TL*SL) (0-120) RISK Ranking
Logical Access Controls														
Security controls can detect unauthorized access attempts.	8.1, 11.1, 12.1, 13.1, 16.1	5	3	2	2	2	1	4 (Med)	0	2	2	0	4	32 (Medium)
Access control software prevents fraudulent activity without collusion.	6.1, 8.1, 11.1, 12.1, 13.1, 16.1	4	2	2	2	2	1	4 (Med)	0	2	2	0	4	32 (Medium)

Vulnerability Level	
Very High	5
High	4
Medium	3
Low	2
Very Low	1

Risk Scale	
Very High	>75
High	55 to 75
Medium	19 to 54
Low	6 to 18
Very Low	<6



Residual Risk Report

Residual Risk Report for: USAO JCON ILA

Component: EOUSA

Non-Compliant Controls					
DOJIT Sec Std Number	AC-1	RBD:	No	Complete:	No
		Risk Ranking:			M

Control Text: The organization develops, disseminates, and periodically reviews updates: (i) a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.

Test Objective: Verify the existence, dissemination, and review of the organization's access control policy.

Non-Compliant Test Results

Expected: AC-01.01-01 *Not Attained* TestedBy: TestDate 12/21/2005 Test No. 1 Type: SA

Access control policy and procedures exist and are documented.

Actual:

Step	Task	Corrective Action Plan	Start	Finish
1	<i>Need to complete this.</i>	Due: <i>1/20/2006</i>	Planned: 12/21/2005 Actual: Remediator: Me	1/20/2006
2	<i>asdfasdfasdf</i>	Due: <i>2/19/2006</i>	Planned: 12/21/2005 Actual: Remediator: Me	2/19/2006
3	<i>asdfasdfasdfasdf</i>	Due: <i>6/19/2006</i>	Planned: 12/21/2005 Actual: Remediator: Me	6/19/2006

Cost: 0

Weakness: *The system lacks a formal, documented, access control policy that is disseminated to appropriate elements within the organization, is periodically reviewed, and is updated when required.*

Impact: *Lack of a formal, documented, access control policy that is disseminated to appropriate elements within the organization, is periodically reviewed, and is updated when required, can facilitate insider threats, hacker penetration, eavesdropping, and espionage.*

Comments:

- Residual Risk Report is automatically generated by the CSAM Client Application.
- Identifies Moderate and High Risk Weaknesses.
- Documents POA&M to Correct Weaknesses.
- Provides Impacts and the Costs to Correct Identified Weaknesses.



Cyber Security Assessment and Management (CSAM)

C&A Client Application

SSP

1. System Identification
2. System Operational Status
3. General Description/ Purpose
4. System Environment
5. System Interconnections/Information Sharing
6. Sensitivity of Information Handled
7. Planning for Security in the Life Cycle
8. Security Control Measures

SSP Appendices

- Appendix D: Requirements (RTM)
- Appendix E: ST&E Plan And Procedures
- Appendix F: Certification Results
- Appendix G: Risk Assessment (RA) Results
- Appendix H: Certifier's Recommendation
- Appendix I: System Security Policy
- Appendix J: System Rules of Behavior (ROB)
- Appendix K: Security Operating Procedures
- Appendix L: Contingency Plan(s)
- Appendix M: Security Awareness Training Plan
- Appendix O: Incident Response Plan
- Appendix P: MOA/Service Level Agreements (SLA)
- Appendix Q: Configuration Management Plan
- Appendix R: Accreditation Statement & Documentation
- Appendix S & T: Hardware & Software Listings
- Appendix U: C&A Schedule

Automate

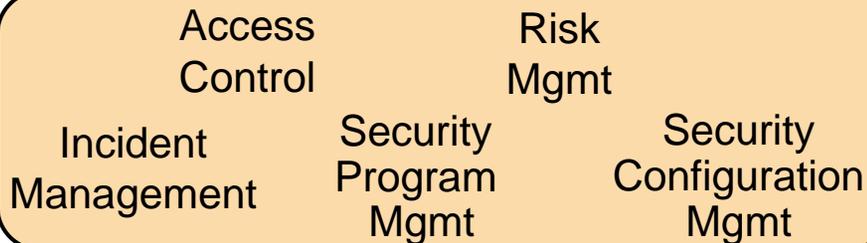
- C&A Documentation
- Knowledge Mgmt
- Workflow Mgmt
- Performance Mgmt Dashboard (Report Card)

CSAM-TrustedAgent/ CSAM FSSI

- Annual FISMA Report
- Quarterly FISMA Report
- System Inventory
- System Security Status
- Justice Component Report Card
- POA&Ms
- IT 300 C&A Data

Inventory UIC Funding Code
FISMA Status Data

IT Security Architecture Support Technology





Risk Control Requirements Determination

- **Security Category**

- ✓ **Mission Impact for:**

- **Confidentiality (H, M, L)**
 - **Integrity (H, M, L)**
 - **Availability (H, M, L)**

- **Scope**

- **Inheritance**



Security Categories

Data Type Details

Select a Mission Area: All DataType: []

Data Classification: SBU **FIPS-199 Guidelines:**

The NIST 800-60 recommended levels are displayed when you select a data category. If you select one not on the list you should follow the FIPS-199 Guidance displayed to the right to select the proper value for the following fields:

	Selected	Recommended
Confidentiality	[]	[]
Integrity	[]	[]
Availability	[]	[]

Explain if you are not using the recommended level:

[]

Save and Close Cancel

- Sensitivity of Information Processed by the System is Reviewed for Levels of Confidentiality, Integrity, and Availability.
- Security Categories of Low, Moderate, and High are Determined by Use of FIPS 199 Criteria.



Scope

- Scope of the System Being Evaluated is Documented to Identify the Applicable Security Controls for a Security Requirements Traceability Matrix (SRTM).
- Considerations Include Whether the System is a General Support System, Major Application, or a Minor Application.
- Additionally, Determinations are made as to Whether the System is Web based, along with other SRTM Factors.

SSP Name: Enterprise Network System

General (1.0) POCs (1.3) Narrative Info Incl'd Systems (1.4) Cert Level RTM Inheritance Appendices Actions

View RTM

System Scope: *General Support System* ▼

System Categorization:

<i>General Support System</i>	<i>Computing Environm</i>
<i>Major Application</i>	<i>Application System</i>
<i>Minor Application</i>	<i>Application System</i>
<i>Low</i>	<i>Non-Sensitive</i>

Classified: Sensitive Compartmented Information (SCI)

Applicable Control Sets:

-- NIST-based Control Set --

NIST 800-53

FISCAM Supplemental

DCID 6/3 Supplemental

Other RTM Factors:

Websites are not part of this system

Privacy Act DOES NOT Apply

This system is not networked (stand-alone)



Inheritance

SSP Name: Enterprise Network System

General (1.0) | POCs (1.3) | Narrative Info | Incl'd Systems (1.4) | Cert Level | RTM | **Inheritance** | Appendices | Actions

Hosted in Data Center or Accredited Computing Environment?

Host Enclave Name:

Please check the services

- FW provided by host
- Host CCB covers this system
- Vulnerability Scans accomplished
- System/Data backups provided
- Host provides Physical and Environmental controls

Alliance Aviation Management	213
ATF Enterprise System Architect	96
ATF Lab Wireless Network	725
Automated Litigation Support	232
Blackberry Enterprise System	229
BOP Network	112
Business Management Services	296
Case Management Enterprise	1285

Enterprise Policy and Procedures are followed

- This Screen Identifies the System and Common Controls that are Supporting the System's Security Requirements.
- Supported Services may include Firewall, Scanning, Back up Capabilities, and Physical and Environmental Controls.



My Tasks

SAMPLE “My Tasks” screen.
 We will add a task for POA&M Management Review:

Task	Overdue			Due	Coming Due						
	60 or more days	30 to 60 days	0 to 30 days	Next 30 days	30 to 60 days	60 to 90 days	90 to 120 days	120 to 150 days	150 to 180 days	180 or more days	
Implementation Tasks Ready / Not Ready	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	
Validation Tasks Ready / Not Ready	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	
Evaluation Tasks	0	0	0	0	0	0	0	0	0	0	
Weaknesses	1	2	0	0	0	0	0	0	0	0	
Milestones	1	2	0	0	0	0	0	0	0	0	
Self-Assessments	0	0	0	0	0	0	0	1	0	2	
Certification and Accreditations	0	0	0	0	0	0	1	0	0	2	
Risk Assessments	1	0	0	0	0	0	0	0	0	2	
Contingency Plan Tests	1	0	0	0	0	0	0	2	0	0	
Security Test and Evaluation	1	0	0	0	0	0	0	0	0	2	
View By Week		View By Month				View By Quarter					

		Risk Controls and POA&Ms			C&A		Access Controls		Configuration Security		Incident and Contingency Mgmt				Awareness & Professional Security Training		
	GRADE	% Controls Eval	POA&M Impl	POA&M Timeliness #Late/Total#	Percent with ATO	ATO Quality	Firewalls and IDS	User ID & PWD	Config Mgmt	Vulnerability Mgmt	IRP Reporting	IRP Exercised	CP Developed	CP Exercised	Awareness Trained	IT Prof Trained	
Goal		96%	96%	96%	96%	96%	96%	96%	96%	96%	96%	96%	96%	96%	96%	96%	
Org'n A	B	 83%	 80%	 95% 40/729	 85%	 84%	62 Systems	 75%	 82%	 94%	 92%		 100%	 89%	 85%	 80%	 100%
Org'n B	A	 95%	 95%	 76% 7/29	 83%	 100%	6 Systems	 96%	 100%	 94%	 100%		 100%	 100%	 100%	 43%	 100%
Org'n C	B	 94%	 94%	 32% 197/289	 80%	 98%	15 Systems	 82%	 100%	 98%	 93%		 36%	 100%	 87%	 21%	 95%
Org'n D	A	 95%	 95%	 100% 0/5	 95%	 100%	21 Systems	 95%	 95%	 95%	 95%		 100%	 95%	 95%	 21%	 90%
Org'n E	C	 52%	 51%	 53% 242/455	 79%	 80%	130 Systems	 100%	 90%	 95%	 80%		 100%	 51%	 46%	 95%	 95%
Org'n F	A	 91%	 92%	 49% 133/260	 95%	 92%	41 Systems	 91%	 89%	 93%	 97%		 100%	 95%	 95%	 82%	 71%
Org'n G	B	 90%	 84%	 88% 32/258	 100%	 97%	10 Systems	 100%	 20%	 93%	 90%		 100%	 60%	 70%	 55%	 46%
Org'n H	A	 74%	 72%	 95% 2/40	 100%	 90%	8 Systems	 100%	 96%	 96%	 100%		 100%	 88%	 88%	 57%	 98%