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
• 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

- DOJ Strategic Plan Goals
- DOJ IT Strategic Plan
- DOJ Info Security Program Mgmt Plan

Central DOJ Focus

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

Information Security Initiative Project Plans

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**

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

**Operational Controls**

- Risk Assessment and Procedures
- Security Planning Policy & Procedures
- System & Services Acquisition Policy & Procedures
- Certification & Accreditation & Security Assessment Policies & Procedures

**Technical Controls**

- Identification and Authentication Policy & Procedures
- Access Control Policy & Procedures
- Audit & Accountability Policy & Procedures
- System & Comm Protection Policy & Procedures

**Implementation Requirements**

<table>
<thead>
<tr>
<th>Risk</th>
<th>System Controls</th>
<th>Common Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Weight</td>
<td>L</td>
<td>M</td>
</tr>
<tr>
<td>4</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>4</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>4</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>2</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>4</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>2</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

**Test Case for Each Requirement**

- RA-1.1
- PL-1.8
- SA-1.1
- CA-1.3
- PS-1.8
- PE-1.8
- CP-1.8
- CM-1.8

**Risk Assessment**

- Vulnerability Control
- Threat Level
- Significance Level
- Total Risk

**Plans of Action & Milestones (POA&M)**

- OMB
- FISMA
- Reporting
- Cyber Security Assessment & Mgmt
- TrustedAgent (CSAM)

**Vulnerabilities Requiring Correction**

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

**Cost + Implementation Guidance**

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

- 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

- 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
## Risk Assessment

<table>
<thead>
<tr>
<th>Vulnerability/Countermeasures and Threat Pairing (Security Controls)</th>
<th>Vulnerability Level</th>
<th>Threat Level</th>
<th>Significance Level</th>
<th>Total Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Logical Access Controls</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security controls can detect unauthorized access attempts.</td>
<td>Exploitability (Hi=5, Low=1)</td>
<td>Capability (Hi=2, Low=1)</td>
<td>Attributable/Detectable (Easy=2, Difficult=0)</td>
<td>Loss of Life (Yes=4, No=0)</td>
</tr>
<tr>
<td>8.1, 11.1, 12.1, 13.1, 16.1</td>
<td>5</td>
<td>3</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Access control software prevents fraudulent activity without collusion.</td>
<td>6.1, 8.1, 11.1, 12.1, 13.1, 16.1</td>
<td>4</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

### Risk Scale

<table>
<thead>
<tr>
<th>Risk Scale</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very High</td>
<td>&gt;75</td>
</tr>
<tr>
<td>High</td>
<td>55 to 75</td>
</tr>
<tr>
<td>Medium</td>
<td>19 to 54</td>
</tr>
<tr>
<td>Low</td>
<td>6 to 18</td>
</tr>
<tr>
<td>Very Low</td>
<td>&lt;6</td>
</tr>
</tbody>
</table>

### Vulnerability Level

- Very High: 5
- High: 4
- Medium: 3
- Low: 2
- Very Low: 1
Residual Risk Report

- 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

Access Control
Risk Mgmt
Incident Management
Security Program Mgmt
Security Configuration Mgmt
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

- 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.
Inheritance

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

<table>
<thead>
<tr>
<th>Task</th>
<th>Overdue</th>
<th>Due</th>
<th>Coming Due</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>60 or more days</td>
<td>30 to 60 days</td>
<td>0 to 30 days</td>
</tr>
<tr>
<td>Implementation Tasks</td>
<td>0/0</td>
<td>0/0</td>
<td>0/0</td>
</tr>
<tr>
<td>Ready / Not Ready</td>
<td>0/0</td>
<td>0/0</td>
<td>0/0</td>
</tr>
<tr>
<td>Validation Tasks</td>
<td>0/0</td>
<td>0/0</td>
<td>0/0</td>
</tr>
<tr>
<td>Ready / Not Ready</td>
<td>0/0</td>
<td>0/0</td>
<td>0/0</td>
</tr>
<tr>
<td>Evaluation Tasks</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Weaknesses</td>
<td>1</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Milestones</td>
<td>1</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Self-Assessments</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Certification and Accreditations</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Risk Assessments</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Contingency Plan Tests</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Security Test and Evaluation</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Grade</td>
<td>% Controls Eval</td>
<td>% Controls Impl</td>
<td>POA&amp;M Timeliness # Late/Total</td>
</tr>
<tr>
<td>-------</td>
<td>----------------</td>
<td>----------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>Goal</td>
<td>96% 96% 96% 96% 96% 96% 96% 96% 96% 96% 96% 96% 96% 96% 96%</td>
<td>96% 96% 96%</td>
<td></td>
</tr>
</tbody>
</table>