Ongoing Authorization (OA)
ISPAB Briefing

June 14, 2013

Office of the Chief Information Security Officer
Outline

• Entrance Requirements
• Control Tailoring
• Audit Trails
• Policy
• Safeguards
• Supporting Tool
• Results
Entrance Requirements

The following are required to enter the DHS OA program:

• Components must have a(n):
  • Robust Continuous Monitoring program
  • Signed Memorandum of Agreement (MOA)
  • Operational Risk Management Board (ORMB)
  • OA Manager
  • Common Control Catalog

• Systems must have a:
  • Current ATO
  • Control Allocation Table (CAT)
Gateway into OA: CISO/AO Recommendation Letter

• Before entering OA, Components must complete a Recommendation Letter

• Serves as the AO’s decision on whether or not a system should operate under OA

• Additionally, anytime a trigger exceeds a defined risk threshold, the letter is again completed
Control Tailoring: Control Allocation Table (CAT)

- The **CAT** allows for risk-based tailoring of controls
- Outlines assessment **frequency** and **impact**
- Updated over time to meet changing risks
- This concept evolved with **NIST recommendations**

<table>
<thead>
<tr>
<th>Control</th>
<th>Enterprise Common Control</th>
<th>Component Common Control</th>
<th>System Specific</th>
<th>CDM</th>
<th>Risk Accepted</th>
<th>POA&amp;M</th>
<th>Frequency</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC-1</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td>6 Months</td>
<td>1 (H)</td>
</tr>
<tr>
<td>AC-2</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td>1 Month</td>
<td>2 (M)</td>
</tr>
<tr>
<td>AC-2 (1)</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td>3 Months</td>
<td>3 (L)</td>
</tr>
<tr>
<td>AC-3</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td>1 Month</td>
<td>1 (H)</td>
</tr>
<tr>
<td>AC-4</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>6 Months</td>
<td>2 (M)</td>
</tr>
<tr>
<td>AC-5</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td>1 Year</td>
<td>3 (L)</td>
</tr>
</tbody>
</table>

Identifies controls outside of their direct control

Outlines assessment frequency and impact
Audit Trails: TRigger Accountability Log (TRAL)

- Components document and **submit trigger events monthly**
- Serves as an **audit trail**
- Provides DHS with **visibility** into Component activities
- Components began submitting TRALs on **5/31**

<table>
<thead>
<tr>
<th>Risk Threshold</th>
<th>FISMA ID</th>
<th>Description</th>
<th>Category</th>
<th>Severity</th>
<th>Impacted Controls</th>
<th>Risk Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Moderate</td>
<td>TSA-06714-MAJ-06714</td>
<td>Vulnerability Management: average of 304 high vulnerabilities per asset detected in April Nessus scans.</td>
<td>Technology</td>
<td>2</td>
<td>SI-2, CM-7</td>
<td>No Escalation Needed</td>
</tr>
<tr>
<td>Moderate</td>
<td>TSA-06714-MAJ-06714</td>
<td>Hardware and Software Managed Assets: Operating System Data for 2003 servers was not returned in Monthly Nessus scans. SP inventory reflects 2003 servers.</td>
<td>Technology</td>
<td>3</td>
<td>CM-2, CM-3, CM-4, CM-8, CA-7, SA-10, PL-2, SI-3</td>
<td>No Escalation Needed</td>
</tr>
<tr>
<td>Low</td>
<td>TSA-06714-MAJ-06714</td>
<td>Status of Plans Actions and Milestones: There is currently one overdue POA&amp;M, however a waiver was submitted on 4/9/2013. TAF #24, Risk categorization Low, is 25 days overdue. Waiver is in route.</td>
<td>Technology</td>
<td>4</td>
<td>CA-5</td>
<td>No Escalation Needed</td>
</tr>
</tbody>
</table>
Policy: Memorandum of Agreement (MOA)

- The MOA enforces program expectations and policy
- It will eventually be incorporated into the DHS 4300
- It outlines the expectations of Components and DHS
- It is a signed by the Component CISO and AO
Safeguards: DHS OA Checklist

- To ensure **accountability**, DHS implemented safeguards
- DHS reviews **CISO/AO Recommendation Letters** for completeness and quality against the **DHS OA Checklist**
  - **90-days** for Components to fix issues, but if not fixed…
  - **90-days** to do a new Security Authorization (successful completion can provide allowance back into OA Program)
Supporting Tool: IACS

• DHS’ new compliance tool, IACS, supports OA
  • Focuses on controls and testing their effectiveness

• IACS allows for **Common Controls**
  • Provider results flow down to all consumers automatically

• IACS has “Risk Elements,” which supports the trigger concept in 2 ways:
  1. Users can **manually create a risk** from a non-technical trigger
  2. User can **auto-create risk elements** from test case failure

<table>
<thead>
<tr>
<th>Saved</th>
<th>Title</th>
<th>Location/Subject</th>
<th>Calc Risk</th>
<th>Adj Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Access Control for Mobile Devices [NIST 800-53 w/ DHS 4300A AC-19]</td>
<td>DC1</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>No</td>
<td>Alternate Processing Site [NIST 800-53 w/ DHS 4300A CP-7[1]]</td>
<td>DC1</td>
<td>High</td>
<td>High</td>
</tr>
</tbody>
</table>

**Example of Auto-Created Risk Element**
Results: Pilot Trigger Events

- **OA is working right now** at DHS HQ, ICE, and TSA
- As of 6/10, **21 trigger events** have been reported
- **28% have been resolved** (6 of 21)

<table>
<thead>
<tr>
<th>Component</th>
<th>High</th>
<th>Moderate</th>
<th>Low</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHS HQ</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>TSA</td>
<td>0</td>
<td>6</td>
<td>7</td>
<td>13</td>
</tr>
<tr>
<td>ICE</td>
<td>2</td>
<td>0</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td><strong>TOTALS</strong></td>
<td>2 (9.5%)</td>
<td>9 (42.9%)</td>
<td>10 (47.6%)</td>
<td>21</td>
</tr>
</tbody>
</table>
BACKUP SLIDES