Homeland Security

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**

Control	Enterprise Common Control	Component Common Control	System Specific	CDM	Risk Accepted	POA&M	Frequency	Impact
AC-1	X						6 Months	1 (H)
AC-2	X		X			X	1 Month	2 (M)
AC-2 (1)			X		X		3 Months	3 (L)
AC-3		X		X		X	1 Month	1 (H)
AC-4		X	X				6 Months	2 (M)
AC-5	X			X			1 Year	3 (L)

Identifies controls outside of their direct control

Outlines assessment frequency and impact

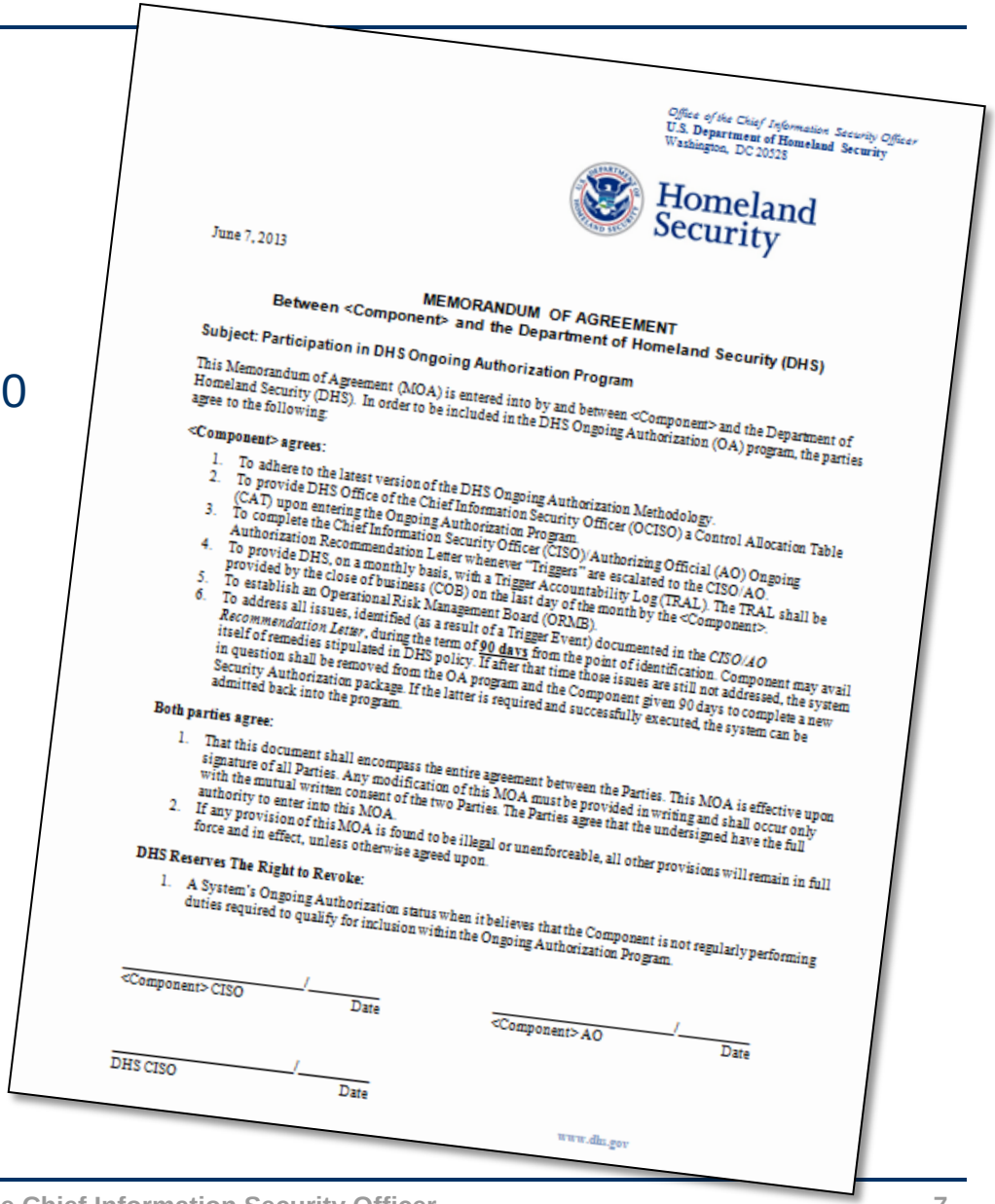
Audit Trails: TRigger Accountability Log (TRAL)

- 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**

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

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



Office of the Chief Information Security Officer
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

June 7, 2013

MEMORANDUM OF AGREEMENT
Between <Component> and the Department of Homeland Security (DHS)

Subject: Participation in DHS Ongoing Authorization Program

This Memorandum of Agreement (MOA) is entered into by and between <Component> and the Department of Homeland Security (DHS). In order to be included in the DHS Ongoing Authorization (OA) program, the parties agree to the following:

<Component> agrees:

1. To adhere to the latest version of the DHS Ongoing Authorization Methodology.
2. To provide DHS Office of the Chief Information Security Officer (OCISO) a Control Allocation Table (CAT) upon entering the Ongoing Authorization Program.
3. To complete the Chief Information Security Officer (CISO)/Authorizing Official (AO) Ongoing Authorization Recommendation Letter whenever "Triggers" are escalated to the CISO/AO.
4. To provide DHS, on a monthly basis, with a Trigger Accountability Log (TRAL). The TRAL shall be provided by the close of business (COB) on the last day of the month by the <Component>.
5. To establish an Operational Risk Management Board (ORMB).
6. To address all issues, identified (as a result of a Trigger Event) documented in the *CISO/AO Recommendation Letter*, during the term of **90 days** from the point of identification. Component may avail itself of remedies stipulated in DHS policy. If after that time those issues are still not addressed, the system in question shall be removed from the OA program and the Component given 90 days to complete a new Security Authorization package. If the latter is required and successfully executed, the system can be admitted back into the program.

Both parties agree:

1. That this document shall encompass the entire agreement between the Parties. This MOA is effective upon signature of all Parties. Any modification of this MOA must be provided in writing and shall occur only with the mutual written consent of the two Parties. The Parties agree that the undersigned have the full authority to enter into this MOA.
2. If any provision of this MOA is found to be illegal or unenforceable, all other provisions will remain in full force and in effect, unless otherwise agreed upon.

DHS Reserves The Right to Revoke:

1. A System's Ongoing Authorization status when it believes that the Component is not regularly performing duties required to qualify for inclusion within the Ongoing Authorization Program.

<Component> CISO _____/_____ Date

<Component> AO _____/_____ Date

DHS CISO _____/_____ Date

www.dhs.gov

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

Saved	Title	Location/Subject ▲	Calc Risk	Adj Risk
No	Access Control for Mobile Devices [NIST 800-53 w/ DHS 4300A AC-19]	DC1	High	High
No	Alternate Processing Site [NIST 800-53 w/ DHS 4300A CP-7[1]]	DC1	High	High

Example of Auto-Created Risk Element

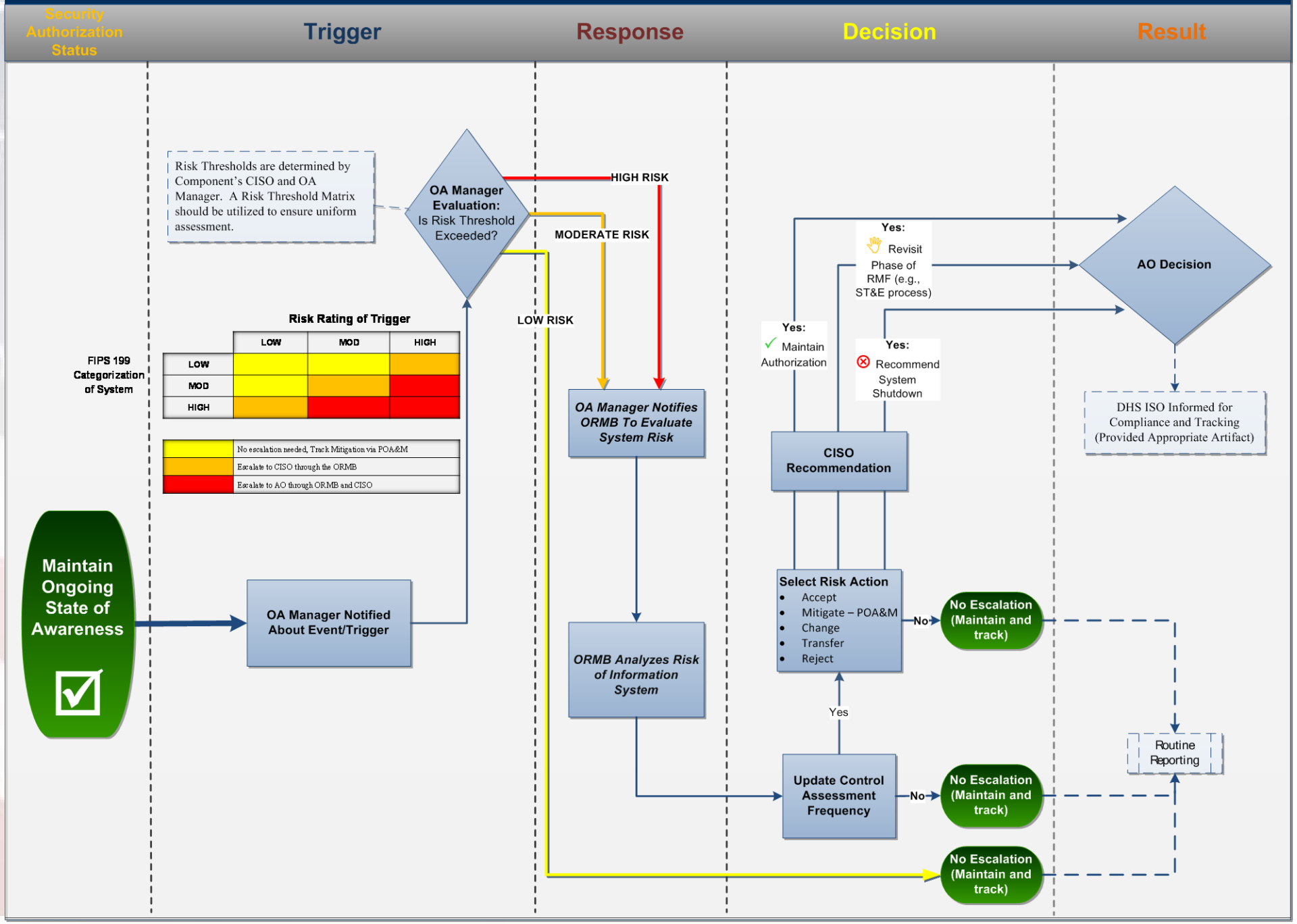
Results: Pilot Trigger Events

- **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)

Component	High	Moderate	Low	Total
DHS HQ	0	3	0	**3**
TSA	0	6	7	**13**
ICE	2	0	3	**5**
TOTALS	**2** (9.5%)	**9** (42.9%)	**10** (47.6%)	**21**

BACKUP SLIDES

Ongoing Authorization - Component Level Risk Evaluation Process



Homeland Security