U.S. Citizenship and Immigration Services

OVERVIEW OF ONGOING AUTHORIZATION (OA)

ISSO Training – Information Systems Security Officer

Information Security Division

12/7/2022

AGENDA

U.S. Citizenship and Immigration Services

- Differences between Security Authorization Process (SAP) and Ongoing Authorization (OA)
- Overview of the OA Process, including key components and tools
- Requirements of the OA Program
- Types of Independent Assessments

OBJECTIVES

U.S. Citizenship and Immigration Services

- Understand the key differences between SAP and OA
- Understand the requirements of the OA Program
- Understand how to record results of control testing in the Control Allocation Table (CAT)
- Understand when and how to record triggers in the TRigger Accountability Log (TRAL)
- Understand the requirements of the monthly Risk Management Board (RMB) meetings
- Understand the types of independent assessments and the outputs

U.S. Citizenship and Immigration Services

DIFFERENCES BETWEEN SECURITY AUTHORIZATION PROCESS (SAP)

AND

ONGOING AUTHORIZATION (OA)

SAP vs OA

U.S. Citizenship and Immigration Services

New Method:

Ongoing Authorization

- Enables risk-based decisions
- Tracks and reports system security postures in near real-time
- Monitors volatile controls through:
  - Defined frequency and documented testing processes
  - Periodic and event-driven testing and assessments
  - Identification of trigger events and escalating as appropriate
- Leverages CDM technologies to support authorization and operational decisions

WHAT IS ONGOING AUTHORIZATION?

U.S. Citizenship and Immigration Services

- OA shifts the focus from compliance-based security to risk-based security.
  - Continuous evaluation of system risk and timely identification of vulnerabilities.
  - Increases frequency of risk evaluations and openness of communication with the AO and System Owners (SO).
  - Increases system security by placing more scrutiny on critical and frequently changing controls.
  - Allows for flexibility to react to new threats and vulnerabilities.
  - Streamlines security authorization testing and reporting processes.
  - Increases awareness of vulnerabilities.

NIST SP 800-37

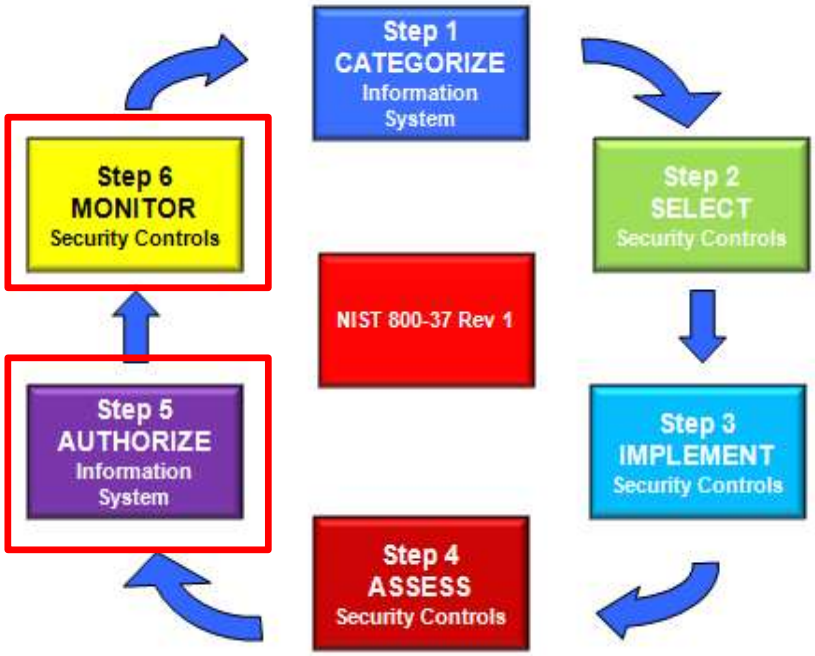
U.S. Citizenship and Immigration Services

- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, provides guidelines for applying the Risk Management Framework to federal information systems to:
  - Ensure that managing information system-related security risks is consistent with the organization's mission and business objectives and overall risk strategy established by senior leadership through the risk executive (function).
  - Ensure that information security requirements, including necessary security controls, are integrated into the organization's enterprise architecture and system development life cycle processes.
  - Support consistent, well-informed transparency of security and risk management-related information, and reciprocity.
  - Achieve more secure information and information systems within the federal government through the implementation of appropriate risk mitigation strategies.

NIST SP 800-37
WHERE DOES OA FIT?

U.S. Citizenship and Immigration Services

- Ongoing Authorization is part of Step 5, *Authorize*, and is dependent on the organization's continuous monitoring program which is implemented in Step 6, *Monitor*, of the Risk Management Framework as described in NIST SP 800-37.



NIST SUPPLEMENTAL GUIDANCE ON OA

U.S. Citizenship and Immigration Services

- The NIST SP 800-37 Supplemental Guidance on OA was published in June 2014 and includes the following summary points:
  - A robust Information Security Continuous Monitoring (ISCM) program is a key dependency of a successful transition to OA.
  - Automation is a consistent theme with respect to transparency and near real-time information transfer.
  - Implementing OA does not change the security authorization process as defined in NIST SP 800-37, it makes the process more efficient and produces more timely information to support risk-based decisions.
  - The 4 tasks in the Risk Management Framework (RMF) Step 5, Authorize, remain virtually unchanged as a result of ongoing authorization.
    - Task 5-1: Unchanged, weaknesses are identified in near real-time as a result of ISCM.
    - Task 5-2: Security posture reviews are conducted by the AO and informed by reports from ISCM automated activities. Greater transparency for the AO into the of risk posture of his/her portfolio.
    - Task 5-3: Unchanged, the AO still determines the organizational risk resulting from the operation of the information system.
    - Task 5-4: Unchanged, the AO remains accountable for understanding and accepting risk based on the organization's risk tolerance.

USCIS OA PROGRAM: BACKGROUND

- Department of Homeland Security (DHS) introduced the concept of OA in its DHS OA Methodology.
- US Citizenship and Immigration Services (USCIS) was an early adopter - participated as 1 of 3 Components in the OA Pilot Program.
- USCIS began transitioning from the traditional SAP to OA in September 2013.

USCIS OA PROGRAM: SUCCESS FACTORS

U.S. Citizenship and Immigration Services

- **Transparency**
  - Information System Security Officers (ISSOs) have access to scan data near real-time.
  - The Chief Information Security Officer (CISO) and/or AO is briefed monthly on security posture of systems, escalated risks (triggers), and weakness remediation plans.
  - All reports, documents, etc. are managed via the Enterprise Collaboration Network (ECN).
- **Accountability**
  - Governance drives accountability by way of meetings with the AO as well as monthly OA RMB meetings.
  - ISSOs are required to attend training annually.
- **Escalation**
  - POA&Ms and triggers are reviewed monthly during the RMB.
  - The OA Manager is an ongoing escalation point for the ISSOs in resolving issues. If issues persist, they are escalated to the CISO and AO.

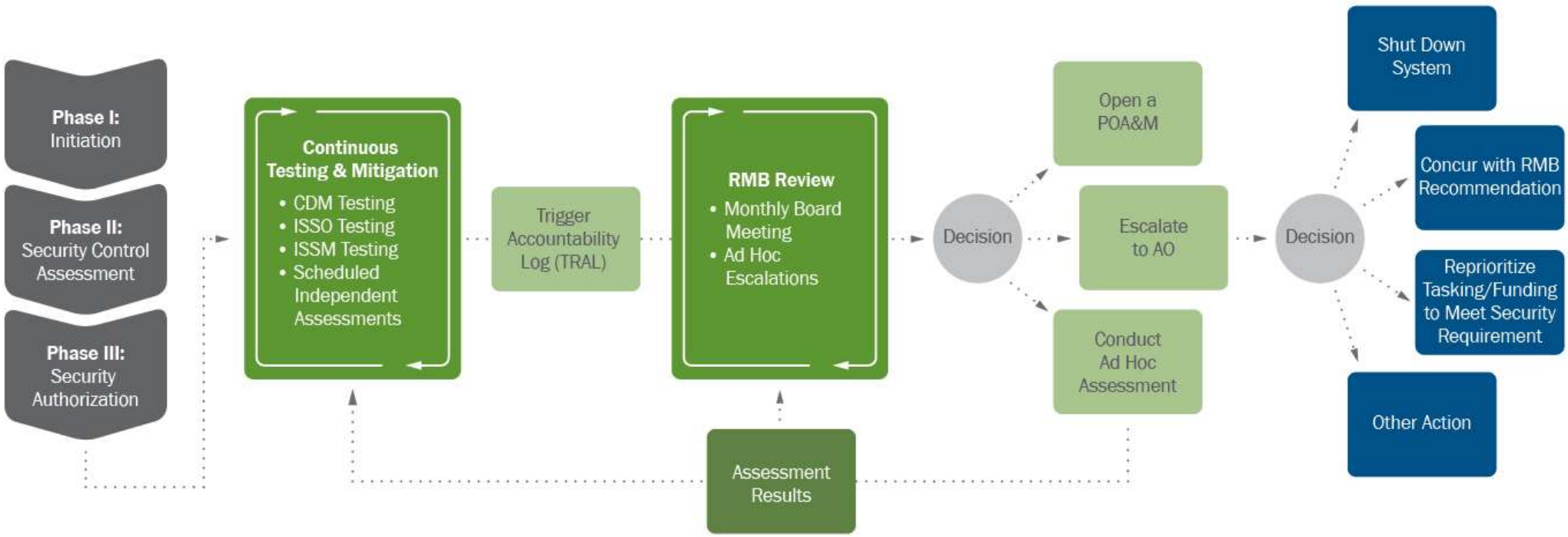
U.S. Citizenship and Immigration Services

OVERVIEW OF THE ONGOING AUTHORIZATION (OA) PROCESS

USCIS OA PROCESS

U.S. Citizenship and Immigration Services

- Traditional SAP (Phases I, II, and III) is a prerequisite to OA



REQUIREMENTS OF THE OA PROGRAM

U.S. Citizenship and Immigration Services

- ISSOs are responsible for the following actions in support of the OA Program:
  - Test controls and maintain the CAT.
  - Maintain the TRAL, including escalating Severity Level 1 and 2 triggers to OA Manager upon identification.
  - Participate in monthly RMB Meetings, including providing a status on action items, overdue POA&Ms, web and database scan findings, and providing justification for negative trends in Anti-virus, Hardening, and Critical/ High/Medium Vulnerabilities.
  - Conduct ISSO-related activities including audit log reviews, POA&M monitoring, account management reviews, etc.
- The Information System Security Manager (ISSM) and OA Manager are responsible for ensuring compliance with all security policy, including OA requirements.

KEY COMPONENTS

U.S. Citizenship and Immigration Services

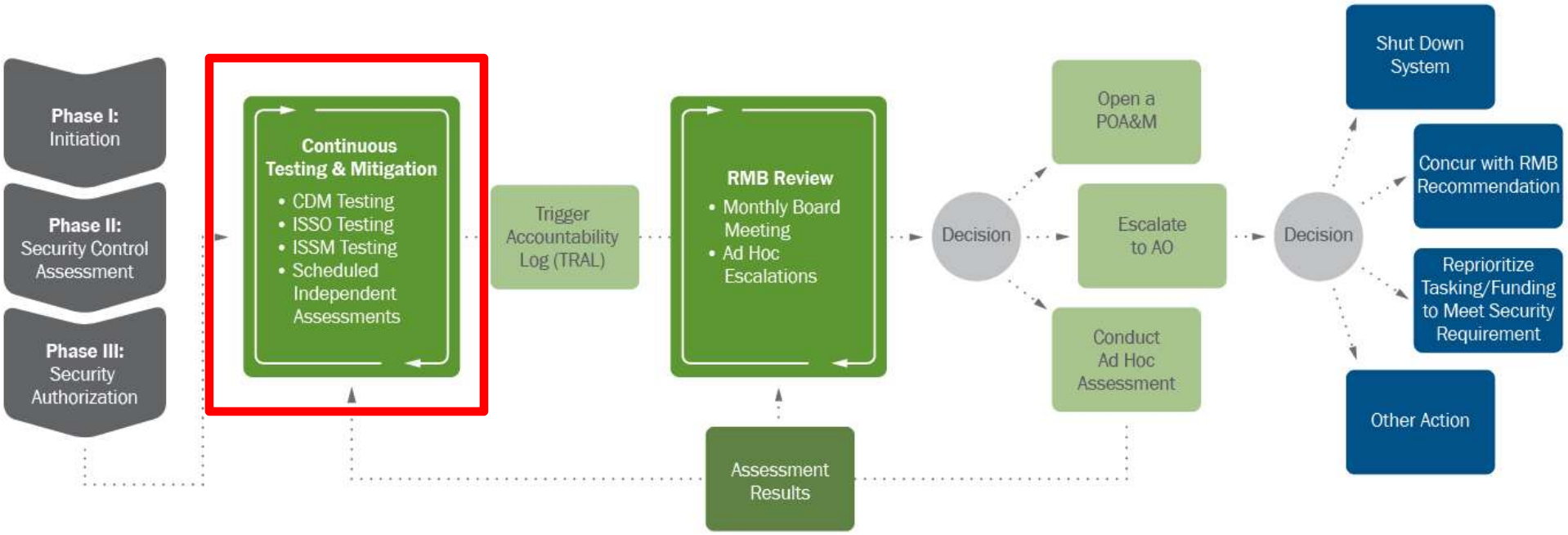
- OA Manager (A federal employee)
- OA Team (Contractor Team)
- OA RMB Meetings
- TRAL Reviews
- CAT Reviews
- Audit Log Reviews
- Account Management
- OA Dashboard
- Assessments are conducted in accordance with the frequencies defined in the CAT
- At least Quarterly Reviews with the AO and/or CISO
- Annually re-occurring ISSO and OA Training
- OA Data Trending Slides

KEY TOOLS

U.S. Citizenship and Immigration Services

- IACS
- Security Center 5 (Nessus)
- SPLUNK
- WebInspect
- DbProtect
- CAT
- TRAL
- Audit Log Review Tracker
- Account Management Tracker
- SharePoint

USCIS OA PROGRAM: TESTING



- Control Testing: In addition to leveraging CDM, the CAT provides a schedule for control testing, by ISSOs and the Security Control Assessment (SCA) Team, at pre-defined frequencies (1 Month, 1 Year, 18 Month, 2 Year, 3 Year, 4 Year, and 5 Year).

CONTROL ALLOCATION TABLE OVERVIEW

U.S. Citizenship and Immigration Services

- The CAT provides the controls to be tested and the frequency for testing.
- The latest version (CAT 3.0) focuses on the role of the SCA Team as the independent assessor, separating testing requirements and frequencies for SCA and the ISSO.
- ISSOs are responsible for testing the controls designated as ISSO-required for their system(s) in accordance with the frequencies outlined in the CAT.
- The SCA team is responsible for testing the controls designated as SCA-required for all systems in accordance with the frequencies outlined in the CAT.
- In addition, CAT 3.0 includes controls unique to FedRAMP-based systems for systems declared as such in IACS.
- Prior to entry into the OA program, the OA Team will build a new CAT based on the results of the last traditional SCA conducted on the system.

GENERATING THE CAT

- Generating the CAT
  - Step 1: Access the *Generate System-Specific CAT* Tab of the CAT

  - Step 2: Complete the system-specific information

<SYSTEM NAME>
SYSTEM OWNER: <System Owner Name>
ISSO: <ISSO Name>
Date: <Date of Completion>

GENERATING THE CAT

U.S. Citizenship and Immigration Services

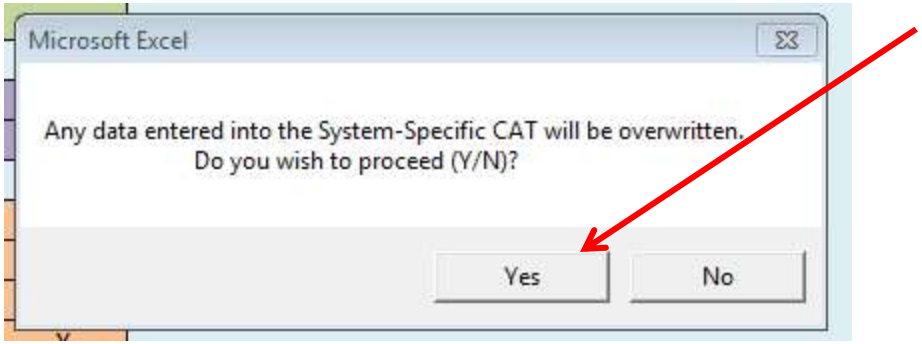
- Generating the CAT
  - Step 3: Complete the system-specific questions using the drop down options

What is the Security Categorization of the System?	
Confidentiality:	M
Integrity:	M
Availability:	M
Is the system following FedRAMP?	N
Is the system a Privacy-Sensitive System?	Y
Is the system a CFO-Designated System?	N
Inherits from DHS & USCIS CISO Programs?	Y
Inherits from DC1 Level 1?	Y
Inherits from DC1 Level 2?	N
Inherits from DC2 Level 1?	Y
Inherits from DC2 Level 2?	N
Inherits from EHS1?	Y
Inherits from EHS2?	N
Inherits from NIOC?	Y
Inherits from ESS?	Y
Inherits from CISNet?	Y
Inherits from OCONUS?	N
Inherits from AWS?	N

GENERATING THE CAT

- Generating the CAT
  - Step 4: Click the Build Table button to generate the system-specific CAT

  - Step 5: Select “Yes” to proceed. Note, this will overwrite any data previously entered within the System-Specific CAT Table



UPDATING THE CAT

U.S. Citizenship and Immigration Services

- Updating the CAT
  - Step 1: Access the *System-Specific CAT Table* Tab of the CAT

  - Step 2: Review the *Control Applicability* column for all controls. Mark any control that is not applicable to the system as Not Applicable (N/A). Provide a justification in the next column *If change made to Control Applicability, denote why*.

#	Control Name	Control Ref #	Control Requirement	Inherited Controls		Privacy System	Control Applicability	If change made to Control Applicability, denote why	CDM	Only applies to Partially Inherited and System-Specific		Last ISSO Test Date	Next ISSO Test Date
				DHS/CIS CISO Progra	OC1 Level 1					ISSO Tested?	ISSO Frequency		
10	Information Flow Enforcement	AC-4	The information system enforces approved authorizations for controlling the flow of information within the system and		PI	N/A	Partially Inherited		N/A	No	N/A	N/A	N/A
11	Separation Of Duties	AC-5	The organization: a. Separates [ASSIGNMENT: ORGANIZATION-DEFINED DUTIES OF INDIVIDUALS]; b. Documents separation of duties of individuals; and			N/A	System-Specific		N/A	No	N/A	N/A	N/A
12	Least Privilege	AC-6	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on			N/A	System-Specific		N/A	No	N/A	N/A	N/A
32	Wireless Access	AC-18	The organization: a. Establishes usage restrictions, configuration/connection requirements, and implementation guidance			N/A	N/A	There is no wireless access within t	N/A	No	N/A	N/A	N/A

UPDATING THE CAT

U.S. Citizenship and Immigration Services

- Step 3: Using the Microsoft (MS) Excel Filtering feature, filter the *Control Applicability* column for Fully Inherited and N/A Controls.
- Step 4: Mark the *Last ISSO Test Date* column as N/A for all controls that are Fully Inherited and N/A.

#	Control Name	Control Ref #	Control Requirement	Inherited Controls		Privacy System	Control Applicability	If change made to Control Applicability, denote why	CDM	Only applies to Partially Inherited and System-Specific controls		Last ISSO Test Date	Next ISSO Test Date
2	Sharing Of Personal Passwords	AC-1 (5.1.1.c)	DHS users shall not share personal passwords.	FI		N/A	Fully Inherited		N/A	No	N/A	N/A	N/A
32	Wireless Access	AC-18	The organization: a. Establishes usage restrictions, configuration/connection requirements, and implementation guidance			N/A	N/A	There is no wireless access within th	N/A	No	N/A	N/A	N/A
41	Security Awareness And Training Policy And Procedures	AT-1	The organization: a. Develops, documents, and disseminates to [PERSONNEL AND ROLES AS DEFINED IN DHS 4300A POLICY]: 1. A security awareness and	FI		N/A	Fully Inherited		N/A	No	N/A	N/A	N/A
42	Security Awareness Training	AT-2	The organization provides basic security awareness training to information system users (including managers, senior executives	FI		N/A	Fully Inherited		N/A	Yes	1 year	N/A	N/A
43	Security Awareness | Insider Threat	AT-2 (2)	The organization includes security awareness training on recognizing and reporting potential indicators of insider threat.	FI		N/A	Fully Inherited		N/A	Yes	1 year	N/A	N/A

UPDATING THE CAT

U.S. Citizenship and Immigration Services

- Step 5: Clear all filters.
- Step 6: Filter on the *ISSO Tested* Column to identify the controls for which the ISSO is responsible for testing. Review the *Next Test Date* column for any controls overdue or coming due. *Next Test Date* is auto-populated based on the *ISSO Frequency*.

#	Control Name	Control Ref #	Control Requirement	Inherited Controls		Privacy System	Control Applicability	If change made to Control Applicability, denote why	CDM	Only applies to Partially Inherited and System-Specific		Last ISSO Test Date	Next ISSO Test Date
				DHS/CIS CISO Progra	DC1 Level 1					ISSO Tested?	ISSO Frequency		
4	Account Management | Automated System Account Management	AC-2 (1)	The organization employs automated mechanisms to support the management of information system accounts.			N/A	System-Specific		X	Yes	1 month	11/6/2017	12/6/2017
5	Account Management | Removal Of Temporary / Emergency	AC-2 (2)	The information system automatically [SELECTION: REMOVES; DISABLES] temporary and emergency accounts after [ASSIGNMENT:			N/A	System-Specific		X	Yes	1 month	11/6/2017	12/6/2017
6	Account Management | Disable Inactive	AC-2 (3)	The information system automatically disables inactive accounts after [90 DAYS FOR LOW-			N/A	System-Specific		X	Yes	1 month	11/6/2017	12/6/2017
18	Unsuccessful Logon Attempts	AC-7	The information system: a. Enforces a limit of [THREE (3)] consecutive invalid logon attempts by a user during a [ASSIGNMENT: ORGANIZATION-DEFINED TIME PERIOD]; and	PI		N/A	Partially Inherited		X	Yes	1 month	11/6/2017	12/6/2017

UPDATING THE CAT

U.S. Citizenship and Immigration Services

- Step 7: Test the controls in accordance with NIST SP 800-53A and record the results by following Steps 8– 9.
  - For ISSO's reference, assessment procedures and evidence guidance is listed for each control.

#	Control Name	Control Ref #	Control Requirement	Inherited Controls		Privacy System	Control Applicability	Only applies to Partially Inherited and System-Specific controls			Last ISSO Test Date	Assessment Procedure	Assessment Evidence
				DHS/CIS CISO Program	DC1 Level 1			ISSO Tested?	ISSO Frequency	Frequency Justification			
3	Account Management	AC-2	The organization: a. Identifies and selects the following types of information system accounts to support			N/A	System-Specific	Yes	1 month	While unlikely to change once established, this control	11/6/2017	Interview the SO/ISSO/SA; identify the system accounts employed (e.g., individual, shared, group, system, guest/anonymous, emergency	Upload certification statement and screenshots to IACS.
4	Account Management | Automated System Account Management	AC-2 (1)	The organization employs automated mechanisms to support the management of information system accounts.			N/A	System-Specific	Yes	1 month	While unlikely to change once established, this control merits	11/6/2017	Interview the SO/ISSO/SA; identify the automated mechanisms (e.g., using email or text messaging to automatically notify account managers when users are	Upload certification statement and screenshot(s) to IACS.
5	Account Management | Removal Of Temporary / Emergency Accounts	AC-2 (2)	The information system automatically [SELECTION: REMOVES; DISABLES] temporary and emergency accounts after [ASSIGNMENT:			N/A	System-Specific	Yes	1 month	While unlikely to change once established, this control merits	11/6/2017	Interview the SO/ISSO/SA; determine whether temporary/emergency accounts are removed or disabled when no longer needed, and after what period	Upload certification statement and screenshot(s) to IACS.
6	Account Management | Disable Inactive Accounts	AC-2 (3)	The information system automatically disables inactive accounts after [90 DAYS FOR LOW-CONFIDENTIALITY SYSTEMS, 45 DAYS FOR MODERATE			N/A	System-Specific	Yes	1 month	While unlikely to change once established, this control merits	11/6/2017	For each system component (e.g. O/S, web, database), generate screenshot depicting how the system automatically disables accounts after 90 days of inactivity (for Low-	Upload screenshot(s) to IACS.

UPDATING THE CAT

U.S. Citizenship and Immigration Services

- Step 8: Update the *Last ISSO Test Date* column for all controls tested as part of the ISSO's typical monthly duties, such as Audit Log Reviews (AU-3, AU-6), Account Management Reviews (AC-2) as well as controls covered by weekly and monthly CDM activities (CA-7, SI-2).
- Step 9: Designate whether the control passed or failed the last test in the *Pass/Fail/Compensated* column.

#	Control Name	Control Ref #	Control Requirement	Inherited Controls		Privacy System	Control Applicability	If change made to Control Applicability, denote	CDM	Only applies to Partially Inherited and System-Specific controls			Last ISSO Test Date	Pass / Fail / Compensated	If Control Failed, associated POA&M	If Control Failed, what is Impact (H/M/L)	Next ISSO Test Date
				DHS/CIS CISO Prog	DC1 Level					ISSO Tested?	ISSO Frequency	Frequency Justification					
3	Account Management	AC-2	The organization: a. Identifies and selects the following types of information system			N/A	System-Specific		X	Yes	1 month	While unlikely to change once established	11/3/2017	Pass		High	12/3/2017
49	Content Of Audit Records	AU-3	The information system generates audit records containing information that establishes what type of event occurred.			N/A	System-Specific		X	Yes	1 month	While unlikely to change once established this control	11/6/2017	Pass		High	12/6/2017
50	Content Of Audit Records | Additional Audit	AU-3 (1)	The information system generates audit records containing the following additional information:			N/A	System-Specific		X	Yes	1 month	While unlikely to change once established	11/6/2017	Pass		High	12/6/2017
53	Audit Review, Analysis, And Reporting	AU-6	The organization: a. Reviews and analyzes information system audit records [AS DEFINED IN THE SECURITY PLAN] for indications of			N/A	System-Specific		X	Yes	1 month	While unlikely to change once established this control merits increased	11/6/2017	Pass		High	12/6/2017
372	Flaw Remediation	SI-2	The organization: a. Identifies, reports, and corrects information system flaws; b. Tests software and firmware updates			N/A	System-Specific		X	Yes	1 month	Flaws are frequently identified in all categories of system components	11/8/2017	Fail		High	12/8/2017

UPDATING THE CAT

U.S. Citizenship and Immigration Services

- Step 10: Clear all filters.
- Step 11: Update the *Last SCA Test Date* column for all controls tested as part of the last SCA. Designate whether the control passed or failed the last test in the *Pass/Fail/Compensated* column.

#	Control Name	Control Ref #	Inherited Controls		Control Applicability	CDM	Only applies to Partially Inherited and System-Specific controls				Last ISSO Test Date	Last SCA Test Date	Pass / Fail / Compen sated	If Control Failed, associated POA&M	If Control Failed, what is Impact (H/M/L)	POA&M Scheduled Completion Date	If Risk Accepted, associated WEAR artifact #	Next ISSO Test Date	Next SCA Test Date
			DHS/CIS CIS	DCJ Level			ISSO Tested	SCA Tested	ISSO Frequen	SCA Frequen									
3	Account Management	AC-2			System-Specific	X	Yes	Yes	1 month	1 year	11/3/2017	10/3/2017	Pass		High			12/3/2017	10/3/2018
49	Content Of Audit Records	AU-3			System-Specific	X	Yes	Yes	1 month	1 year	11/6/2017	10/3/2017	Pass		High			12/6/2017	10/3/2018
50	Content Of Audit Records | Additional Audit Information	AU-3 (1)			System-Specific	X	Yes	Yes	1 month	1 year	11/6/2017	10/3/2017	Pass		High			12/6/2017	10/3/2018
53	Audit Review, Analysis, And Reporting	AU-6			System-Specific	X	Yes	Yes	1 month	1 year	11/6/2017	10/3/2017	Pass		High			12/6/2017	10/3/2018
372	Flaw Remediation	SI-2			System-Specific	X	Yes	Yes	1 month	1 year	11/8/2017	10/9/2017	Fail	74	High	4/28/2018	CIS-2017-W-001	12/8/2017	10/9/2018

UPDATING THE CAT

U.S. Citizenship and Immigration Services

- Step 12: For failed controls, if there is an associated POA&M, add the POA&M number in the *If Control Failed, associated POA&M #* column and the POA&M's Scheduled Completion Date in the *POA&M Scheduled Completion Date* column.
- Step 13: If there is an approved Waiver or Accepted Risk (WEAR) signed by the USCIS AO, include the WEAR tracking number in the *If Risk Accepted, associated WEAR artifact #* column. Add the DHS tracking number once it is available.

#	Control Name	Control Ref #	Inherited Controls		Control Applicability	CDM	Only applies to Partially Inherited and System-Specific controls				Last ISSO Test Date	Last SCA Test Date	Pass / Fail / Compensated	If Control Failed, associated POA&M #	If Control Failed, what is Impact (H/M/L)?	POA&M Scheduled Completion Date	If Risk Accepted, associated WEAR artifact #	Next ISSO Test Date	Next SCA Test Date
			DHS/CIS CIS	DC1 Level			ISSO Tested	SCA Tested	ISSO Frequency	SCA Frequency									
3	Account Management	AC-2			System-Specific	X	Yes	Yes	1 month	1 year	11/3/2017	10/3/2017	Pass		High			12/3/2017	10/3/2018
49	Content Of Audit Records	AU-3			System-Specific	X	Yes	Yes	1 month	1 year	11/6/2017	10/3/2017	Pass		High			12/6/2017	10/3/2018
50	Content Of Audit Records | Additional Audit Information	AU-3 (1)			System-Specific	X	Yes	Yes	1 month	1 year	11/6/2017	10/3/2017	Pass		High			12/6/2017	10/3/2018
53	Audit Review, Analysis, And Reporting	AU-6			System-Specific	X	Yes	Yes	1 month	1 year	11/6/2017	10/3/2017	Pass		High			12/6/2017	10/3/2018
372	Flaw Remediation	SI-2			System-Specific	X	Yes	Yes	1 month	1 year	11/8/2017	10/9/2017	Fail	74	High	4/28/2018	CIS-2017-W-001	12/8/2017	10/9/2018

UPDATING THE CAT
NEW POA&Ms

U.S. Citizenship and Immigration Services

DSD(6

- Step 14: Reference IACS, and add any new POA&Ms that were not previously included in the CAT.
  - Scenario: POA&M 93 was created in IACS on 10/28/2017 for updating the Security Plan to include a newly added minor application. The POA&M has a Scheduled Completion Date in IACS of 10/28/2018.
    - Update *Last Test Date* to the POA&M Creation Date, 10/28/2017.
    - Update *Pass/Fail* field to Fail.
    - Enter 93 in the *If Control Failed, Associated POA&M Number* field.
    - Enter 10/28/2018 in the *POA&M Scheduled Completion Date* field.

#	Control Name	Control Ref #	Control Applicability	Only applies to Partially Inherited and System-		Last SCA Test Date	Assessment Procedure	Pass / Fail / Compensated	If Control Failed, associated POA&M #	If Control Failed, what is Impact (H/M/L)?	POA&M Scheduled Completion Date	If Risk Accepted, associated WEAR artifact #	Next SCA Test Date
				SCA Tested?	SCA Frequency								
258	Sensitive PII	PL-1 (3.14.5.c)	System-Specific	Yes	4 years	10/28/2017	Interview the SO/ISSO; determine if routine CREs are performed for the system.	Pass		Low			10/28/2021
260	System Security Plan	PL-2	System-Specific	Yes	1 year	10/28/2017	Interview the CISO/SO/ISSO; determine if the SP includes the noted items; identify who is responsible for	Fail	93	High	10/28/2018		10/28/2018
261	System Security Plan | Plan / Coordinate With Other Organizational	PL-2 (3)	System-Specific	Yes	1 year	10/28/2017	Interview the SO/ISSO; determine how security-related activities (e.g., security assessments,	Fail	93	High	10/28/2018		10/28/2018

Slide 29

DSD(6 Have OA Team review this slide
Dodson, Shari D (CTR), 3/14/2018

UPDATING THE CAT
COMPLETED POA&M

U.S. Citizenship and Immigration Services

DSD(5

- Scenario: POA&M 96 was marked completed in IACS on 11/09/2017.
  - Update *Last Test Date* with the POA&M Completion Date, 11/09/2017. The *Next Test Date* column automatically adjusts to reflect the assigned frequency of testing for the control.
  - Update *Pass/ Fail* field to Pass.
  - Remove reference to POA&M number and POA&M Scheduled Completion Date.

Before

#	Control Name	Control Ref #	Inherited Controls		Control Applicability	CDM	Only applies to Partially Inherited and System-Specific controls				Last SCA Test Date	Assessment Procedure	Pass / Fail / Compensated	If Control Failed, associated POA&M #	If Control Failed, what is Impact (H/M/L)?	POA&M Scheduled Completion Date	If Risk Accepted, associated WEAR artifact #	Next SCA Test Date
			DHS/CIS CISO Program	DC1 Level 1			ISSO Tested?	SCA Tested?	ISSO Frequency	SCA Frequency								
8	Access Enforcement	AC-3			System-Specific	N/A	No	Yes	N/A	3 years	6/5/2017	For each system layer (e.g. O/S, web database	Fail	96	Moderate	11/13/2017		6/5/2020
12	Least Privilege	AC-6			System-Specific	N/A	No	Yes	N/A	18 months	6/5/2017	Interview the SO/ISSO/SA; identify each user group and the	Fail	96	Moderate	11/13/2017		12/5/2018

After

#	Control Name	Control Ref #	Inherited Controls		Control Applicability	CDM	Only applies to Partially Inherited and System-Specific controls				Last SCA Test Date	Assessment Procedure	Pass / Fail / Compensated	If Control Failed, associated POA&M #	If Control Failed, what is Impact (H/M/L)?	POA&M Scheduled Completion Date	If Risk Accepted associated WEA artifact #	Next SCA Test Date
			DHS/CIS CISO Program	DC1 Level 1			ISSO Tested?	SCA Tested?	ISSO Frequency	SCA Frequency								
8	Access Enforcement	AC-3			System-Specific	N/A	No	Yes	N/A	3 years	11/9/2017	For each system layer (e.g. O/S, web database	Pass		Moderate			11/9/2020
12	Least Privilege	AC-6			System-Specific	N/A	No	Yes	N/A	18 months	11/9/2017	Interview the SO/ISSO/SA; identify each user group and the	Pass		Moderate			5/9/2019

Slide 30

DSD(5 Have OA Review this slide deck.
Dodson, Shari D (CTR), 3/14/2018

UPDATING THE CAT

APPROVED WEAR

U.S. Citizenship and Immigration Services

DSD(7

- Step 15: Add any approved WEAR not previously included on the CAT.
  - Scenario: Overdue POA&M 73 now has a USCIS-approved waiver.
    - Update *If Risk Accepted, associated WEAR artifacts with WEAR number* field to include the tracking number for the waiver, CIS-2017-W-056.
    - Update the CAT with the DHS tracking number once it is received. This can be included in the notes column along with the WEAR expiration date.

#	Control Name	Control Ref #	Control Applicability	Only applies to Partially SCA Frequency	Last SCA Test Date	Assessment Procedure	Pass / Fail / Compensated	If Control Failed, associated POA&M #	If Control Failed, what is Impact (H/M/L)?	POA&M Scheduled Completion Date	If Risk Accepted, associated WEAR artifact #	Notes	Next SCA Test Date
24	Permitted Actions Without Identification Or Authentication	AC-14	System-Specific	5 years	10/28/2017	Interview the SO/ISSO/AO; determine what actions can be performed without I&A. Examine the SP; validate that a rationale is	Fail	73	Low	5/28/2018	CIS-2017-W-056	USCIS Approved - Exp: 09/28/2018	10/28/2022
25	Remote Access	AC-17	System-Specific	18 months	11/6/2017	Interview the SO/ISSO/SA; identify the different remote access methods. Examine (for each remote access method)			Moderate				5/6/2019

Slide 31

DSD(7 Have OA Team review this slide.
Dodson, Shari D (CTR), 3/14/2018

UPDATING THE CAT
PRIVACY CONTROLS

U.S. Citizenship and Immigration Services

- The DHS Privacy Office is responsible for testing privacy controls. Record N/A in the Pass/Fail column of the CAT for the privacy controls until the results are received.

#	Control Name	Control Ref #	Control Requirement	Inherited Controls		Privacy System	Control Applicability	Only applies to Partially Inherited and System-Specific controls		Last SCA Test Date	Assessment Procedure	Pass / Fail / Compensated	Next SCA Test Date
				DHS/CIS CISO Program	DC1 Level 1			SCA Frequency	Frequency Justification				
413	Purpose Specification	AP-2	The organization describes the purpose(s) for which personally identifiable information (PII) is collected, used, maintained, and shared in its privacy notices.			X	Privacy Office	N/A	While unlikely to change once established, this control merits increased scrutiny.		Examine the privacy notice; validate the purpose for which PII is collected, used, maintained, and shared is included. Generate screenshot of	N/A	N/A
414	Governance And Privacy Program	AR-1	The organization: a. Appoints a Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) accountable for developing, implementing, and maintaining an organization-wide			X	Privacy Office	N/A	Unlikely to change once established		Interview the CPO; validate an organization wide governance program has been developed/implemented/maintained. s/he	N/A	N/A
416	DHS Privacy Impact Assessment	AR-2 (3.14.2.a)	A PTA shall be conducted as part of new information system development or whenever an existing system is significantly modified. PTA artifacts expire after three years and a new PTA must be			N/A	Privacy Office	N/A	PIA should be reviewed and updated, if necessary, annually		Examine the PTA; validate the PTA is current, and generate screenshot.	N/A	N/A
417	DHS Privacy Impact Assessment	AR-2 (3.14.2.b)	A PTA shall be conducted whenever an information system undergoes security authorization.			N/A	Privacy Office	N/A	PIA should be reviewed and updated, if necessary, annually		Examine the PTA; validate the PTA was conducted in conjunction with the SA&A effort, and generate screenshot.	N/A	N/A

UPDATING THE CAT
PRIVACY CONTROLS

U.S. Citizenship and Immigration Services

- Once the DHS Privacy Office has tested the controls, if all controls passed, they will set the *Privacy Assessment (Task 2)* in IACS to *Complete* and notify the USCIS Privacy Office.
- The USCIS Privacy Office will notify Information Security Division (ISD), and ISD will notify the ISSO.
- If any of the privacy controls fail, DHS will notify the USCIS Privacy Office and USCIS Privacy will coordinate further with ISD and the ISSO to complete the necessary actions.

UPDATING THE CAT
PRIVACY CONTROLS

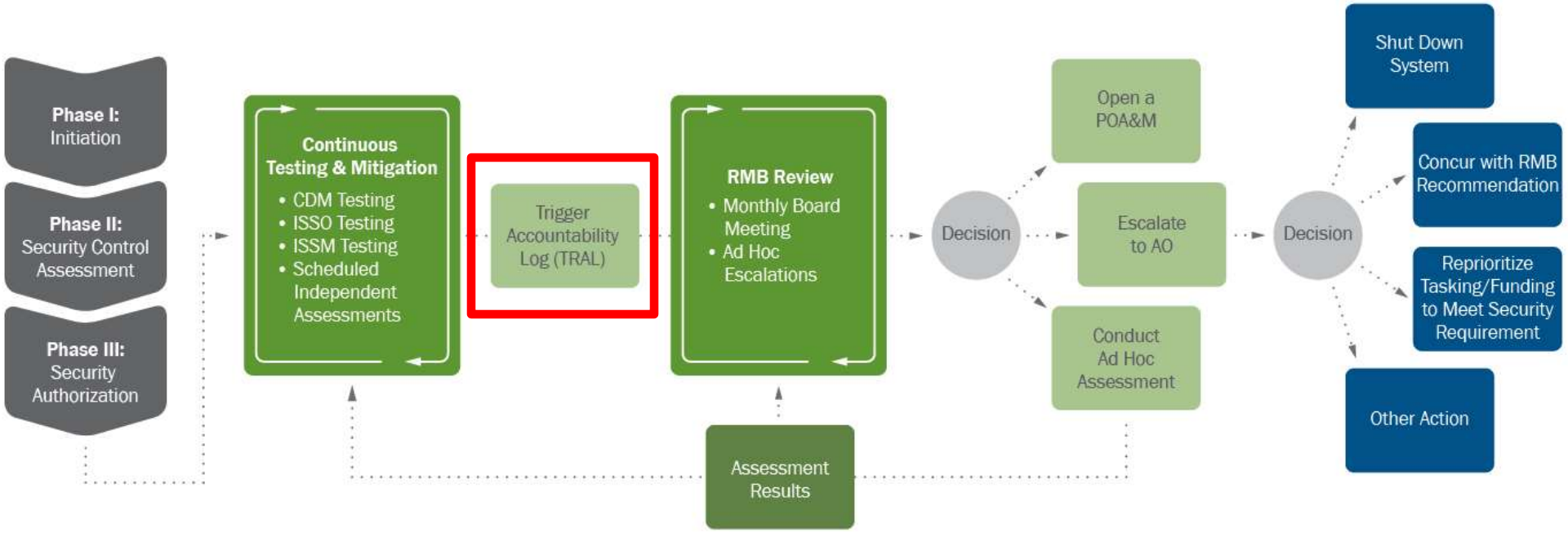
U.S. Citizenship and Immigration Services

- Once the ISSO receives notification from ISD that all privacy controls have passed, the ISSO shall update the Last SCA Test Date column and Pass/Fail column accordingly.

#	Control Name	Control Ref #	Privacy System	Control Applicability	Only applies to Partially Inherited and System-Specific controls		Last SCA Test Date	Assessment Procedure	Pass / Fail / Compensated	If Control Failed, associated POA&M #	If Control Failed, what is Impact (H/M/L)?	POA&M Scheduled Completion Date	If Risk Accepted, associated WEAR artifact #	Next SCA Test Date
					SCA Frequency	Frequency Justification								
413	Purpose Specification	AP-2	X	Privacy Office	N/A	While unlikely to change once established, this control merits increased scrutiny.	11/8/2017	Examine the privacy notice; validate the purpose for which PII is collected, used, maintained, and shared is included. Generate screenshot of applicable	Pass		Moderate			N/A
414	Governance And Privacy Program	AR-1	X	Privacy Office	N/A	Unlikely to change once established	11/8/2017	Interview the CPO; validate an organization-wide governance program has been developed/implemented/ maintained. s/he	Pass		Low			N/A
416	DHS Privacy Impact Assessment	AR-2 (3.14.2.a)	N/A	Privacy Office	N/A	PIA should be reviewed and updated, if necessary, annually	11/8/2017	Examine the PTA; validate the PTA is current, and generate screenshot.	Pass		High			N/A
417	DHS Privacy Impact Assessment	AR-2 (3.14.2.b)	N/A	Privacy Office	N/A	PIA should be reviewed and updated, if necessary, annually	11/8/2017	Examine the PTA; validate the PTA was conducted in conjunction with the SA&A effort, and generate screenshot.	Pass		High			N/A

USCIS OA PROGRAM:
RISK MONITORING

U.S. Citizenship and Immigration Services



- TRAL: Ensures all risk-related activities are recorded and managed.
  - USCIS tracks risk proactively via the TRAL.
  - High severity triggers (risk events) are escalated to the OA Manager as they occur.

WHAT IS A TRIGGER?

U.S. Citizenship and Immigration Services

- A Trigger is defined as an unidentified event or significant change to the system or its controls, which may change the security posture of the system.
- Triggers are:
  - Detected through ISSO assessments, CDM activities, independent assessments, ISSM assessments, and/or manual monitoring.
  - Recorded in the TRAL and monitored by the ISSO.
  - Escalated within the TRAL to the OA Manager for initial review and then to the RMB for risk-based recommendations.

TRIGGER ATTRIBUTES

U.S. Citizenship and Immigration Services

- Triggers are categorized into 4 groups: People, Processes, Technology, and Discretionary Frequency
- Triggers can be either routine or non-routine
  - Routine: triggers that are normal or scheduled occurrences
  - Non-routine: triggers that are out-of-cycle, anomalies, or of unknown origin or activity
- Discretionary Frequency Triggers
  - Triggers that fall outside of the Routine/Non-routine category (e.g., Management decides that an assessment is needed due to an excessive number of triggers)

DATA FIELDS ON THE TRAL

USCIS TRigger Accountability Log				
Trigger ID	Date Recorded	Observed Date	Estimated Completion Date	Resolution Date

- Trigger ID: Derived from the FISMA ID, followed by a sequential number. This number is manually input.
  - Example: CIS-03516-00001
- Date Recorded: Date trigger was recorded on the TRAL. May not be the same as the Observed Date. Recognizes a lag time between events and tracking.
- Date Observed: Date the trigger occurred or was observed.
- Estimated Completion Date: Date the trigger is expected to be resolved.
- Resolution Date: This field is only completed for triggers once they have been closed/ resolved.

DATA FIELDS ON THE TRAL

U.S. Citizenship and Immigration Services

USCIS TRigger Accountability Log								
FISMA ID	System Name	Trigger Type	Description	Category	Severity	Impacted Controls	Tested Controls	Test Results

FISMA ID: Drop down selections - FISMA ID of the system.

System Name: Drop down selections - Displayed as an acronym.

Trigger Type: Drop down selections - Indicates what category the trigger is related to; Database, General, Informational, O/S, POA&M, or Vulnerability.

Description: Clear, concise description of the trigger event.

Category: Drop down selections - People, Processes, Technology.

Severity: Drop down selections - 1=Severe mission and operations impact, 2=Mission and operations impact, 3=Non-Routine requiring immediate attention, 4=Routine Support

Impacted Controls: NIST/ DHS control(s) impacted by the trigger event.

Tested Controls: This field is only completed for triggers once they have been closed/ resolved and should reflect the NIST/DHS controls tested to validate resolution.

Test Results: Drop down selections - This field is only completed for triggers once they have been closed/ resolved and should depict the results of the test(s).

DATA FIELDS ON THE TRAL

U.S. Citizenship and Immigration Services

USCIS TRigger Accountability Log			
Escalation Path	Recommendation	Action/Resolution	General Comments

- Escalation Path: Drop down selections - No Escalation Needed, Escalated to Ongoing Authorization Risk Management Board (ORMB), Escalated to ORMB/Chief Information Security Officer (CISO), Escalated to ORMB/CISO/AO.
  - Use the Trigger Severity Matrix as a guide to determine the recommended Escalation Path, the OA Manager will adjust as needed (see slide 43).
- Recommendation: This field is used by the ISSO/OA Team to recommend a course of action to the RMB.
- Action/ Resolution: This field is used by the ISSO/OA Team to record the RMB's decision on the course of action. For resolved triggers, this field includes a brief description of how the trigger was resolved.
- General Comments: This field is to be used by the ISSO to provide a general status and additional information concerning the trigger event. Include the date of the update as well.

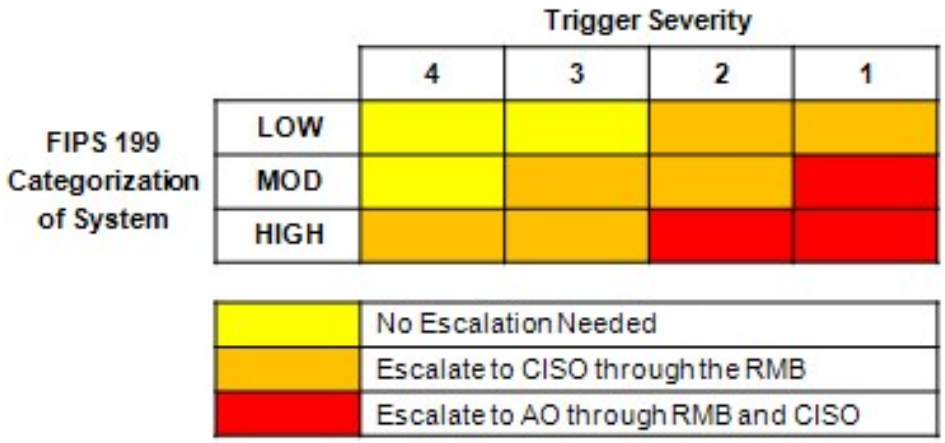
ITEMS TO RECORD ON THE TRAL

U.S. Citizenship and Immigration Services

- All incidents
- All POA&Ms are triggers, but all triggers are not POA&Ms
- All Information Security Vulnerability Management (ISVM) Alert notices affecting the system
- Change Requests (CRs) that have been determined could have a security impact
- Change in hardware/software
- Changes in personnel/ support teams/contracts
- Any controls that failed when tested in accordance with the CAT
- Sudden changes in Continuous Monitoring scan results for Anti-Virus, Critical/High/Medium Vulnerabilities, or Hardening

TRIGGER SEVERITY MATRIX: RISK THRESHOLD

- The risk threshold is a function of the system's FIPS 199 categorization and the trigger severity.



Severity Indicators:
1 = Severe mission and operations impact
2 = Mission and operations Impact
3 = Non-routine requiring immediate attention
4 = Routine support

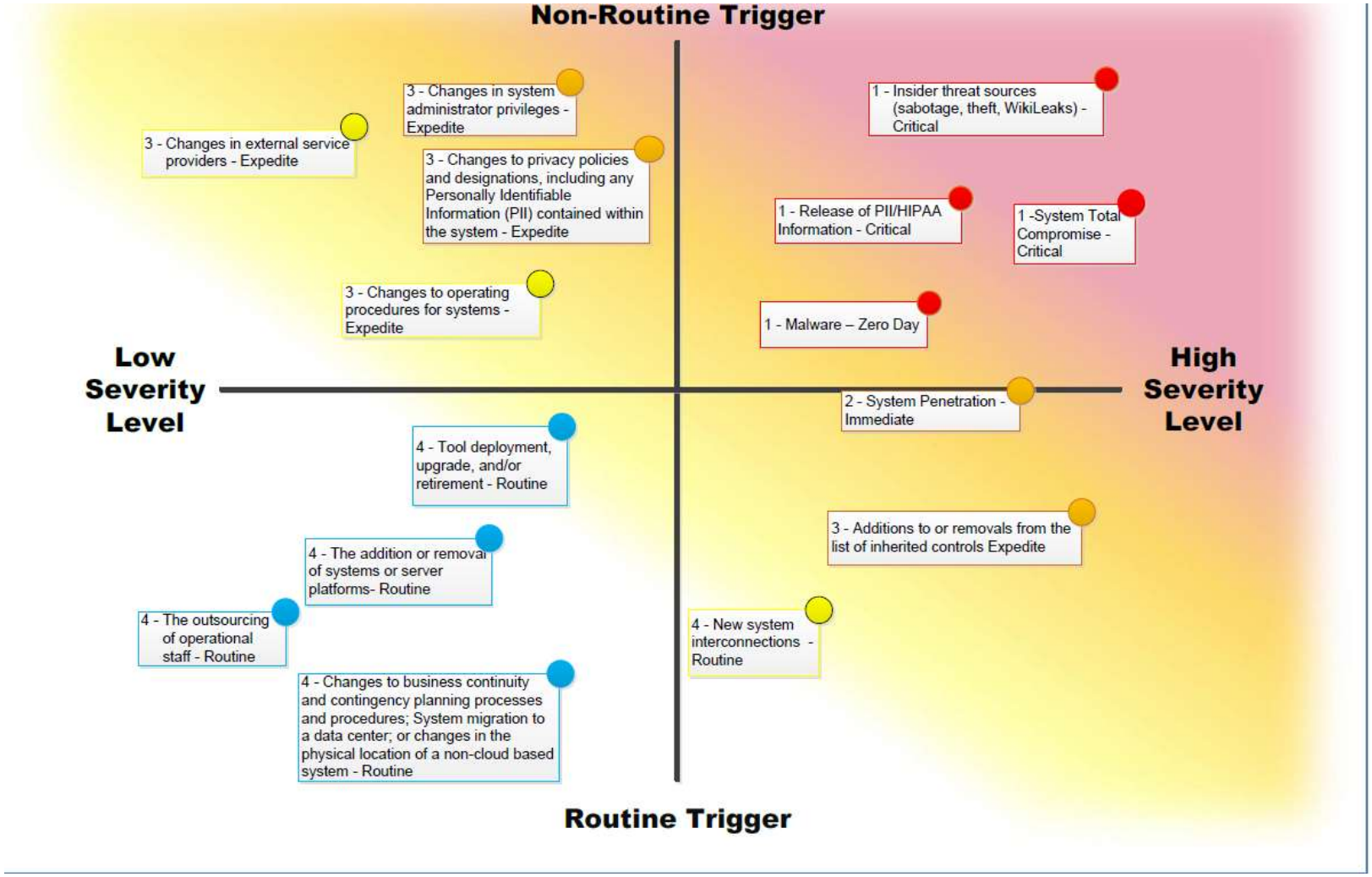
TRIGGER SEVERITY MATRIX:
TRIGGER SEVERITY INDEX

U.S. Citizenship and Immigration Services

- DHS OA Methodology, Appendix G: Trigger Severity Index provides examples of triggers identified by grouping of people, processes, and technology. The table does not list all possible triggers, but is a representative sampling of the most common and prevalent types.

Severity	Description	Response
	People	
1	Insider threat sources (e.g. sabotage, theft)	Critical
1	Release of PII/HIPAA Information	Critical
3	Changes in external service providers	Expedite
3	Changes in system administrator privileges	Expedite
4	The outsourcing of operational staff	Routine

TRIGGER SEVERITY EXAMPLES



TRAL CONDITIONAL FORMATTING

U.S. Citizenship and Immigration Services

- System-Level TRALs include conditional formatting to increase visibility to the following triggers:
  - Open triggers that are older than 90 days – Highlighted Red
  - Triggers with Estimated Completion Date (ECD) in the Past – Highlighted Yellow

Trigger ID	Date Recorded	Observed Date	Estimated Completion Date	Resolution Date	FISMA ID	System Name	Trigger Type	Description
CIS-00829-00945	10/5/2017	10/01/2017	3/28/2018		CIS-00822-MAJ-00079	ACME	Informational	Asset Management ACME inventory Inventory changing between 118 and 160 assets.
CIS-00829-00946	12/27/2017	12/27/2017	2/28/2018		CIS-00822-MAJ-00079	ACME	Vulnerability	**New High vulnerabilities** identified on Splunk Dashboard . Plugin Vulnerability
CIS-00829-00947	1/9/2018	1/9/2018	4/1/2018		CIS-00822-MAJ-00079	ACME	Vulnerability	**High vulnerabilities** identified on Splunk Dashboard Jan 9, 2018. **Plugin Vulnerability Number**

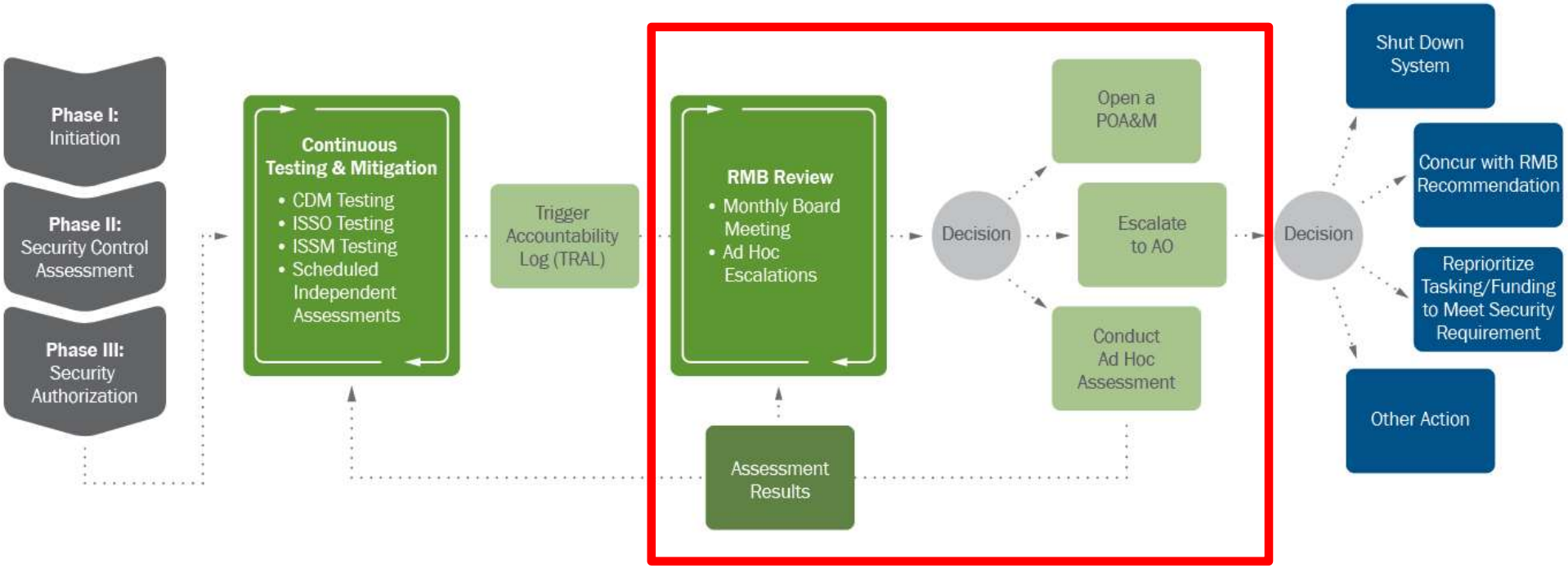
TRAL QUICK REFERENCE GUIDE

U.S. Citizenship and Immigration Services

- The USCIS OA TRAL Quick Reference Guide is located within the OA Policy, Training and Documentation Library.
- This document is intended to provide guidance on how to complete each column of the system-level TRAL and identify areas of focus for ISSOs and TRAL reviewers.

TRAL Column Title	Review Criteria
Description	• This column should include a brief description of the issue and the potential risk. A clear, concise description should address these questions: what, where, who, when, and how. • If a trigger is related to a POA&M, ensure the description matches the POA&M weakness description in IACS and identifies the POA&M number in bold. • Ensure that no IP addresses or host names are included in the description. • The trigger description should not be modified after initial entry. All new updates should be added under the General Comments column.

USCIS OA PROGRAM: RMB



- RMB Meetings: Participate in monthly collaborative meetings where Board members review and monitor system security posture.
- RMB decides course of action in managing risk.

MONTHLY OA RMB MEETINGS

U.S. Citizenship and Immigration Services

- RMB meetings are conducted monthly where members review the security posture of each system participating in the OA Program.
- Reporting elements have evolved considerably since the inception of the Program.
- Action items are tracked to closure and status is reported monthly.
- Escalated triggers are reviewed to determine course of action.

ACME: OA Trending Data

C-I-A: M-M-L
Start Secure. Stay Secure.

ISSO: Wile E. Coyote ITPM: Yosemite Sam	Weakness: 100%	HW Assets: 98%	SW Assets: 86%	Vuln Mgmt: 100%	Config Mgmt: 66%	Anti-Phish/Malware: 33%

	OS Trending					POA&M Trending					Web Scan Trending				Database Scan Trending					Code Scan Trending	
											WebInspect				DbProtect			ARCAT		Fortify	
	Hardening	Antivirus	Critical	High	Medium	Open	Overdue	Due in 30 Days	Due in 60 Days	Due in 90 Days	Critical	High	Mod	Low	High	Mod	Low	Pass	Fail	Pass	Fail
Feb	77%	0%	26	96	686	0	0	0	0	0	-	-	-	-	-	-	-	167	22	N/A	N/A
Jan	77%	55%	17	250	788	0	0	0	0	0	0	4	2	18	-	-	-	324	54	N/A	N/A
Dec	82%	62%	25	302	773	0	0	0	0	0	0	3	22	54	1	13	11	165	27	N/A	N/A
Nov	80%	59%	0	189	858	0	0	0	0	0	1	3	4	62	2	12	10	156	5	N/A	N/A
Oct	80%	85%	27	433	1177	0	0	0	0	0	0	3	4	15	2	12	10	156	5	N/A	N/A
Sep	95%	92%	32	170	-	0	0	0	0	0	162	4	69	105	3	7	4	156	5	N/A	N/A

#Assets: 102

Auth Scans: 92

CredCoverage: 97%

System Notes:
17 total ISVMs; 1 CIO ISVM. 23% of hosts are not affected by an ISVM
DbProtect is currently offline.

Compliance Notes:
Compliance Due Date- **Jan 12th – Feb 9th**
Account Management- Account Management missing a month review

OA Compliance							
CPT 6/21/18	PTA 8/26/19	SP 4/30/18	FIPS 1/22/19	CMP -	BACKUP SITE	ACCT MGMT 1/7/18	CAT 2/8/18
CP 7/25/18	PIA USCIS	SORN USCIS	eAUTH 1/29/19	ISA 0-0-0	MOU/MOA -	AUDIT LOG 2/6/18	TRAL 2/9/18

Next Assessment: 09/02/18	Last Assessment: 10/05/14	Decommission:	OA Entry: 08/22/12	Location(s): DC1, AWS

MONTHLY OA RMB MEETINGS

U.S. Citizenship and Immigration Services

- Each system is scheduled for monthly RMB meetings to review the previous six (6) months of data and current POA&M status.
- The meetings are presented using Adobe Connect. The meeting invitation includes links to the meeting site and the meeting materials.
- Due dates associated with the RMB meeting are posted within the OA Calendar on the OA ECN Site.
  - OA Compliance items include: CAT updates, TRAL updates, Account Management, and Audit Log Review Trackers

COLLABORATE WITH THE OA TEAM

U.S. Citizenship and Immigration Services

- Approximately two days prior to an RMB meeting, the OA Team will coordinate with the ISSOs to gather the status on action items assigned at previous RMB meetings.
- The OA Team reviews the TRALs for triggers that require escalation to the RMB and possibly for further escalation to the AO. The OA Team will collaborate with the ISSOs if there are any questions during the reviews.
- The POA&M Management Team also coordinates with ISSOs to gather statuses on POA&Ms and WEAR, and ensure the TRAL is updated prior to the RMB meeting.
- The system TRALs are reviewed by the OA Manager during the monthly RMB meetings.

RESEARCH DOWNWARD TRENDS

- Approximately two days prior to the monthly RMB meeting, the OA Team develops a data trending slide for each system.
- Data trending slides are posted in each system's library on the OA ECN site.
- ISSOs are to research any changed trends from the Nessus scan results, and/or relating to overdue POA&Ms or POA&Ms coming due within 90 days. ISSOs should come to the RMB meetings prepared to discuss these items.

ACME: OA Trending Data

C-I-A: M-M-L
Start Secure. Stay Secure.

ISSO: Wile E. Coyote
ITPM: Yosemite Sam

Weakness: 100%	HW Assets: 98%	SW Assets: 86%	Vuln Mgmt: 100%	Config Mgmt: 66%	Anti-Phish/Malware: 33%

	OS Trending					POA&M Trending					Web Scan Trending				Database Scan Trending					Code Scan Trending	
											WebInspect				DbProtect			ARCAT		Fortify	
	Hardening	Antivirus	Critical	High	Medium	Open	Overdue	Due in 30 Days	Due in 60 Days	Due in 90 Days	Critical	High	Mod	Low	High	Mod	Low	Pass	Fail	Pass	Fail
Feb	77%	0%	26	96	686	0	0	0	0	0	-	-	-	-	-	-	-	167	22	N/A	N/A
Jan	77%	55%	17	250	788	0	0	0	0	0	0	4	2	18	-	-	-	324	54	N/A	N/A
Dec	82%	62%	25	302	773	0	0	0	0	0	0	3	22	54	1	13	11	165	27	N/A	N/A
Nov	80%	59%	0	189	858	0	0	0	0	0	1	3	4	62	2	12	10	156	5	N/A	N/A
Oct	80%	85%	27	433	1177	0	0	0	0	0	0	3	4	15	2	12	10	156	5	N/A	N/A
Sep	95%	92%	32	170	-	0	0	0	0	0	162	4	69	105	3	7	4	156	5	N/A	N/A

#Assets: 102
Auth Scans: 92
CredCoverage: 97%

System Notes:
17 total ISVMs; 1 CIO ISVM. 23% of hosts are not affected by an ISVM
DbProtect is currently offline.

Compliance Notes:
Compliance Due Date- **Jan 12th – Feb 9th**
Account Management- Account Management missing a month review

OA Compliance								
CPT 6/21/18	PTA 8/26/19	SP 4/30/18	FIPS 1/22/19	CMP -	BACKUP SITE	ACCT MGMT 1/7/18	CAT 2/8/18
CP 7/25/18	PIA USCIS	SORN USCIS	eAUTH 1/29/19	ISA 0-0-0	MOU/MOA -	AUDIT LOG 2/6/18	TRAL 2/9/18

Next Assessment: 09/02/18 | Last Assessment: 10/05/14 | Decommission: | OA Entry: 08/22/12 | Location(s): DC1, AWS

REPORT PROGRESS ON WEB & DB ISSUES

U.S. Citizenship and Immigration Services

- Data on recent Web and Database scans will also be presented at the monthly RMB meeting. ISSOs should come prepared to discuss progress in addressing critical and high findings. The scans are posted on the system's library on the SCA ECN.
- Code scan results will also be reviewed (if applicable).

ACME: OA Trending Data

C–I–A: M–M–L
Start Secure. Stay Secure.

ISSO: Wile E. Coyote ITPM: Yosemite Sam	Weakness: 100%	HW Assets: 98%	SW Assets: 86%	Vuln Mgmt: 100%	Config Mgmt: 66%	Anti-Phish/Malware: 33%

	OS Trending					POA&M Trending					Web Scan Trending				Database Scan Trending					Code Scan Trending	
											WebInspect				DbProtect			ARCAT		Fortify	
	Hardening	Antivirus	Critical	High	Medium	Open	Overdue	Due in 30 Days	Due in 60 Days	Due in 90 Days	Critical	High	Mod	Low	High	Mod	Low	Pass	Fail	Pass	Fail
Feb	77%	0%	26	96	686	0	0	0	0	0	-	-	-	-	-	-	-	167	22	N/A	N/A
Jan	77%	55%	17	250	788	0	0	0	0	0	0	4	2	18	-	-	-	324	54	N/A	N/A
Dec	82%	62%	25	302	773	0	0	0	0	0	0	3	22	54	1	13	11	165	27	N/A	N/A
Nov	80%	59%	0	189	858	0	0	0	0	0	1	3	4	62	2	12	10	156	5	N/A	N/A
Oct	80%	85%	27	433	1177	0	0	0	0	0	0	3	4	15	2	12	10	156	5	N/A	N/A
Sep	95%	92%	32	170	-	0	0	0	0	0	162	4	69	105	3	7	4	156	5	N/A	N/A

#Assets: 102

Auth Scans: 92

CredCoverage: 97%

System Notes:
17 total ISVMs; 1 CIO ISVM. 23% of hosts are not affected by an ISVM
DbProtect is currently offline.

Compliance Notes:
Compliance Due Date- **Jan 12th – Feb 9th**
Account Management- Account Management missing a month review

OA Compliance								
	CPT 6/21/18	PTA 8/26/19	SP 4/30/18	FIPS 1/22/19	CMP -	BACKUP SITE	ACCT MGMT 1/7/18	CAT 2/8/18
	CP 7/25/18	PIA USCIS	SORN USCIS	eAUTH 1/29/19	ISA 0-0-0	MOU/MOA -	AUDIT LOG 2/6/18	TRAL 2/9/18

Next Assessment: 09/02/18	Last Assessment: 10/05/14	Decommission:	OA Entry: 08/22/12	Location(s): DC1, AWS

REPORT PROGRESS ON SYSTEM STATUS

U.S. Citizenship and Immigration Services

- Progress on completion of Security Authorization documentation and OA Compliance is reported to the RMB.
- High level system or compliance notes are highlighted on the data trending slide.
- Upcoming and recent assessment activities are also included.

ACME: OA Trending Data

C – I – A: M – M – L
Start Secure. Stay Secure.

ISSO: Wile E. Coyote ITPM: Yosemite Sam	Weakness: 100%	HW Assets: 98%	SW Assets: 86%	Vuln Mgmt: 100%	Config Mgmt: 66%	Anti-Phish/Malware: 33%

	OS Trending					POA&M Trending					Web Scan Trending				Database Scan Trending					Code Scan Trending	
											WebInspect				DbProtect			ARCAT		Fortify	
	Hardening	Antivirus	Critical	High	Medium	Open	Overdue	Due in 30 Days	Due in 60 Days	Due in 90 Days	Critical	High	Mod	Low	High	Mod	Low	Pass	Fail	Pass	Fail
Feb	77%	0%	26	96	686	0	0	0	0	0	-	-	-	-	-	-	-	167	22	N/A	N/A
Jan	77%	55%	17	250	788	0	0	0	0	0	0	4	2	18	-	-	-	324	54	N/A	N/A
Dec	82%	62%	25	302	773	0	0	0	0	0	0	3	22	54	1	13	11	165	27	N/A	N/A
Nov	80%	59%	0	189	858	0	0	0	0	0	1	3	4	62	2	12	10	156	5	N/A	N/A
Oct	80%	85%	27	433	1177	0	0	0	0	0	0	3	4	15	2	12	10	156	5	N/A	N/A
Sep	95%	92%	32	170	-	0	0	0	0	0	162	4	69	105	3	7	4	156	5	N/A	N/A

#Assets: 102

Auth Scans: 92

CredCoverage: 97%

System Notes:
17 total ISVMs; 1 CIO ISVM. 23% of hosts are not affected by an ISVM
DbProtect is currently offline.

Compliance Notes:
Compliance Due Date- **Jan 12th – Feb 9th**
Account Management- Account Management missing a month review

OA Compliance							
CPT 6/21/18	PTA 8/26/19	SP 4/30/18	FIPS 1/22/19	CMP -	BACKUP SITE	ACCT MGMT 1/7/18	CAT 2/8/18
CP 7/25/18	PIA USCIS	SORN USCIS	eAUTH 1/29/19	ISA 0-0-0	MOU/MOA -	AUDIT LOG 2/6/18	TRAL 2/9/18

Next Assessment: 09/02/18	Last Assessment: 10/05/14	Decommission:	OA Entry: 08/22/12	Location(s): DC1, AWS

DATA TRENDING SLIDE
A CLOSER LOOK

U.S. Citizenship and Immigration Services

ACME: OA Trending Data

C – I – A: M – M – L
Start Secure. Stay Secure.

ISSO: Wile E. Coyote ITPM: Yosemite Sam	Weakness: 100%	HW Assets: 98%	SW Assets: 86%	Vuln Mgmt: 100%	Config Mgmt: 66%	Anti-Phish/Malware: 33%

	OS Trending					POA&M Trending					Web Scan Trending				Database Scan Trending					Code Scan Trending	
											WebInspect				DbProtect			ARCAT		Fortify	
	Hardening	Antivirus	Critical	High	Medium	Open	Overdue	Due in 30 Days	Due in 60 Days	Due in 90 Days	Critical	High	Mod	Low	High	Mod	Low	Pass	Fail	Pass	Fail
Feb	77%	0%	26	96	686	0	0	0	0	0	-	-	-	-	-	-	-	167	22	N/A	N/A
Jan	77%	55%	17	250	788	0	0	0	0	0	0	4	2	18	-	-	-	324	54	N/A	N/A
Dec	82%	62%	25	302	773	0	0	0	0	0	0	3	22	54	1	13	11	165	27	N/A	N/A
Nov	80%	59%	0	189	858	0	0	0	0	0	1	3	4	62	2	12	10	156	5	N/A	N/A
Oct	80%	85%	27	433	1177	0	0	0	0	0	0	3	4	15	2	12	10	156	5	N/A	N/A
Sep	95%	92%	32	170	-	0	0	0	0	0	162	4	69	105	3	7	4	156	5	N/A	N/A

#Assets: 102

Auth Scans: 92

CredCoverage: 97%

System Notes:
17 total ISVMs; 1 CIO ISVM. 23% of hosts are not affected by an ISVM
DbProtect is currently offline.

Compliance Notes:
Compliance Due Date- **Jan 12th – Feb 9th**
Account Management- Account Management missing a month review

OA Compliance								
	CPT 6/21/18	PTA 8/26/19	SP 4/30/18	FIPS 1/22/19	CMP -	BACKUP SITE	ACCT MGMT 1/7/18	CAT 2/8/18
	CP 7/25/18	PIA USCIS	SORN USCIS	eAUTH 1/29/19	ISA 0-0-0	MOU/MOA -	AUDIT LOG 2/6/18	TRAL 2/9/18

Next Assessment: 09/02/18	Last Assessment: 10/05/14	Decommission:	OA Entry: 08/22/12	Location(s): DC1, AWS

For reference, the OA RMB Data Trending Slide Criteria is posted on the OA ECN.

DATA TRENDING SLIDE
A CLOSER LOOK

U.S. Citizenship and Immigration Services

ACME: OA Trending Data						C – I – A: M – M – L Start Secure. Stay Secure.
ISSO: Wile E. Coyote ITPM: Yosemite Sam	Weakness: 100%	HW Assets: 98%	SW Assets: 86%	Vuln Mgmt: 100%	Config Mgmt: 66%	Anti-Phish/Malware: 33%

- **ISSO**: ISSO Name
- **ITPM**: ITPM Name
- **C-I-A**: System's Confidentiality, Integrity, Availability
- Data from the FISMA Scorecard:
  - **Weakness**: Weakness Remediation score - % of POA&Ms meeting timeliness and quality checks
  - **HW Assets:** Hardware assets score- %
  - **SW Assets:** Software assets score- %
  - **Vuln. Mgmt.**: Vulnerability Management score - % of assets meeting threshold of assigned risk value for critical and high Common Vulnerability Enumerations (CVEs)
  - **Config. Mgmt.:** Configuration Management score - % applicable assets meeting threshold of assigned risk value for configuration setting benchmark
  - **Anti-Phish/ Malware**: Antivirus/Anti-Phishing/Malware - % assets meeting endpoint security requirements

DATA TRENDING SLIDE
A CLOSER LOOK

U.S. Citizenship and Immigration Services

	OS Trending					POA&M Trending					Web Scan Trending				Database Scan Trending					Code Scan Trending	
											WebInspect				DbProtect			ARCAT		Fortify	
	Hardening	Antivirus	Critical	High	Medium	Open	Overdue	Due in 30 Days	Due in 60 Days	Due in 90 Days	Critical	High	Mod	Low	High	Mod	Low	Pass	Fail	Pass	Fail
Feb	77%	0%	26	96	686	0	0	0	0	0	-	-	-	-	-	-	-	167	22	N/A	N/A

- OS Trending data
  - **Hardening:** Hardening score from SC5, as reported on the Splunk OA Dashboard
  - **Anti-virus:** Anti-virus score from SC5, as reported on the Splunk OA Dashboard
  - **Critical:** Number of Critical severity vulnerabilities from SC5, as reported on Splunk OA Dashboard
  - **High:** Number of High severity vulnerabilities from SC5, as reported on Splunk OA Dashboard
  - **Medium:** Number of Medium severity vulnerabilities from SC5, as reported on Splunk OA Dashboard
- POA&M Trending data
  - **Open:** # POA&Ms in IACS in the following statues: In Progress, Waiver, Exception, Delayed
  - **Overdue:** # POA&Ms in IACS in Delayed status
  - **Due in 30 days:** # POA&Ms with a Scheduled Completion Date within 30 days
  - **Due in 60 days:** # POA&Ms with a Scheduled Completion Date within 60 days
  - **Due in 90 days:** # POA&Ms with a Scheduled Completion Date within 90 days

DATA TRENDING SLIDE
A CLOSER LOOK

U.S. Citizenship and Immigration Services

	OS Trending					POA&M Trending					Web Scan Trending				Database Scan Trending					Code Scan Trending	
											WebInspect				DbProtect			ARCAT		Fortify	
	Hardening	Antivirus	Critical	High	Medium	Open	Overdue	Due in 30 Days	Due in 60 Days	Due in 90 Days	Critical	High	Mod	Low	High	Mod	Low	Pass	Fail	Pass	Fail
Feb	77%	0%	26	96	686	0	0	0	0	0	-	-	-	-	-	-	-	167	22	N/A	N/A

- **WebInspect Findings**
  - # critical, high, moderate, and low findings averaged across # websites scanned
- **DbProtect Findings**
  - # high, moderate, and low findings averaged across # database instances scanned
- **ARCAT findings**
  - Total # of pass and fail findings scanned (cloud systems only)
- **Code scanning (Fortify) findings**
  - Total # of pass and fail findings scanned (cloud systems only)

DATA TRENDING SLIDE
A CLOSER LOOK

U.S. Citizenship and Immigration Services

OA Compliance								
	CPT 6/21/18	PTA 8/26/19	SP 4/30/18	FIPS 1/22/19	CMP -	BACKUP SITE	ACCT MGMT 1/7/18	CAT 2/8/18
	CP 7/25/18	PIA USCIS	SORN USCIS	eAUTH 1/29/19	ISA 0-0-0	MOU/MOA -	AUDIT LOG 2/6/18	TRAL 2/9/18
Next Assessment: 09/02/18		Last Assessment: 10/05/14		Decommission:		OA Entry: 08/22/12		Location(s): DC1, AWS

- **Contingency Plan Test (CPT) Compliance:** CPT expiration date
- **Contingency Plan (CP) Compliance:** CP expiration date
- **Privacy Threshold Analysis (PTA) Compliance:** PTA expiration date
- **Privacy Impact Assessment (PIA) Compliance:** PIA status (required and current, update required, or N/A)
- **Security Plan (SP) Compliance:** Annual SP due date
- **System of Records Notice (SORN):** SORN status (required and current, update required, or N/A)
- **FIPS Compliance:** Annual FIPS 199 review due date
- **eAUTH (eAuthentication) Compliance:** Annual eAuthentication review due date
- **Configuration Management Plan (CMP) Compliance:** CMP due date (not yet required)
- **Interconnection Security Analysis (ISA):** ISA status (Expired/ Upcoming/ Current)
- **Backup Site:** Hot, Warm, or Cold backup site as identified by the system's CP
- **Memorandum of Understanding (MOU)/ Memorandum of Agreement (MOA) Compliance:** MOU/MOA status (not yet required)

DATA TRENDING SLIDE
A CLOSER LOOK

U.S. Citizenship and Immigration Services

OA Compliance								
	CPT 6/21/18	PTA 8/26/19	SP 4/30/18	FIPS 1/22/19	CMP -	BACKUP SITE	ACCT MGMT 1/7/18	CAT 2/8/18
	CP 7/25/18	PIA USCIS	SORN USCIS	eAUTH 1/29/19	ISA 0-0-0	MOU/MOA -	AUDIT LOG 2/6/18	TRAL 2/9/18
Next Assessment: 09/02/18	Last Assessment: 10/05/14	Decommission:	OA Entry: 08/22/12	Location(s): DC1, AWS				

- **Account Management Reviews**
  - Account management reviews conducted and entered into the Account Management Tracker within 4 weeks of the RMB
- **Audit Log Reviews**
  - Audit log reviews conducted and entered into the Audit Log Tracker within 1 week of the RMB
- **CAT Compliance-** CAT updated and all *Next Test Dates* current (no overdue controls)
- **TRAL Compliance-** TRAL reviewed and updated within 4 weeks of the RMB

DATA TRENDING SLIDE
A CLOSER LOOK

U.S. Citizenship and Immigration Services

#Assets: 102 Auth Scans: 92 CredCoverage: 97%	**System Notes:** 17 total ISVMs; 1 CIO ISVM. 23% of hosts are not affected by an ISVM DbProtect is currently offline.	**Compliance Notes:** Compliance Due Date- **Jan 12th – Feb 9th** Account Management- Account Management missing a month review

- **#Assets and Auth Scans:** Number of assets in the system and number of authenticated scans reported on the Splunk OA Dashboard
- **Cred Coverage**: Identifies percentage of assets having received a compliance scan, or both
- **System Notes:** Notes requested by OA Manager or recommended by ISSO
- **Compliance Notes:** Notes provided by OA Team

Next Assessment: 09/02/18	Last Assessment: 10/05/14	Decommission:	OA Entry: 08/22/12	Location(s): DC1, AWS

- **Next Assessment:** Date of upcoming OA assessment
- **Last Assessment:** Date of last OA assessment
- **Decommission:** System's decommissioning date
- **OA Entry:** Date of system's entry to the OA Program
- **Location:** Physical location of the system's assets

POST RMB MEETING ACTIVITIES

U.S. Citizenship and Immigration Services

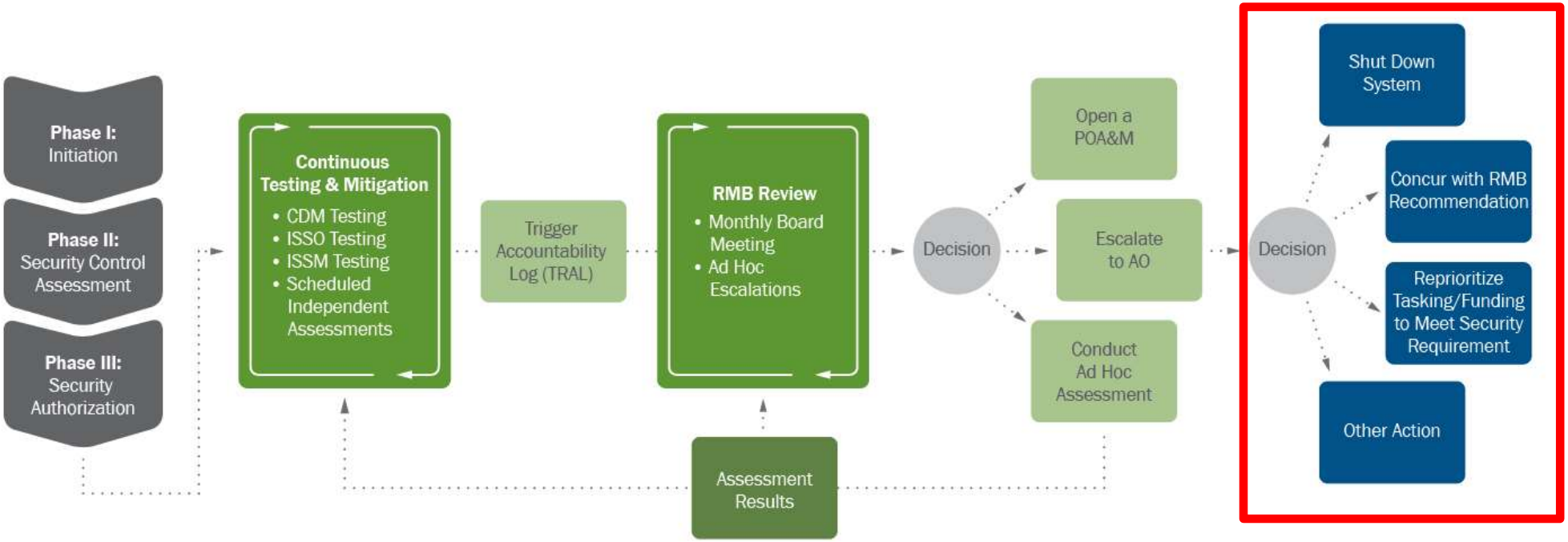
Action Number	Action Item Description	Date Originated	Completion Date	Status	Assigned To
System-5	Add a trigger regarding CPT. ISSO should schedule a CPT.	3/15/2017	3/16/2017	Complete	ISSO
System-6	Add a trigger for applicable ISVMs affecting the system	4/16/2017	4/28/2017	Complete	ISSO

TRAL | Action Items | Inventory

- After the RMB meeting, the OA Team updates the Action Items Tab of the system TRAL with any actions assigned.
- ISSOs are expected to update trigger events within the TRAL throughout the month to ensure adequate progress is made on addressing POA&Ms, assigned action items, and for escalating to the OA Team, OA Manager, and the RMB as needed.

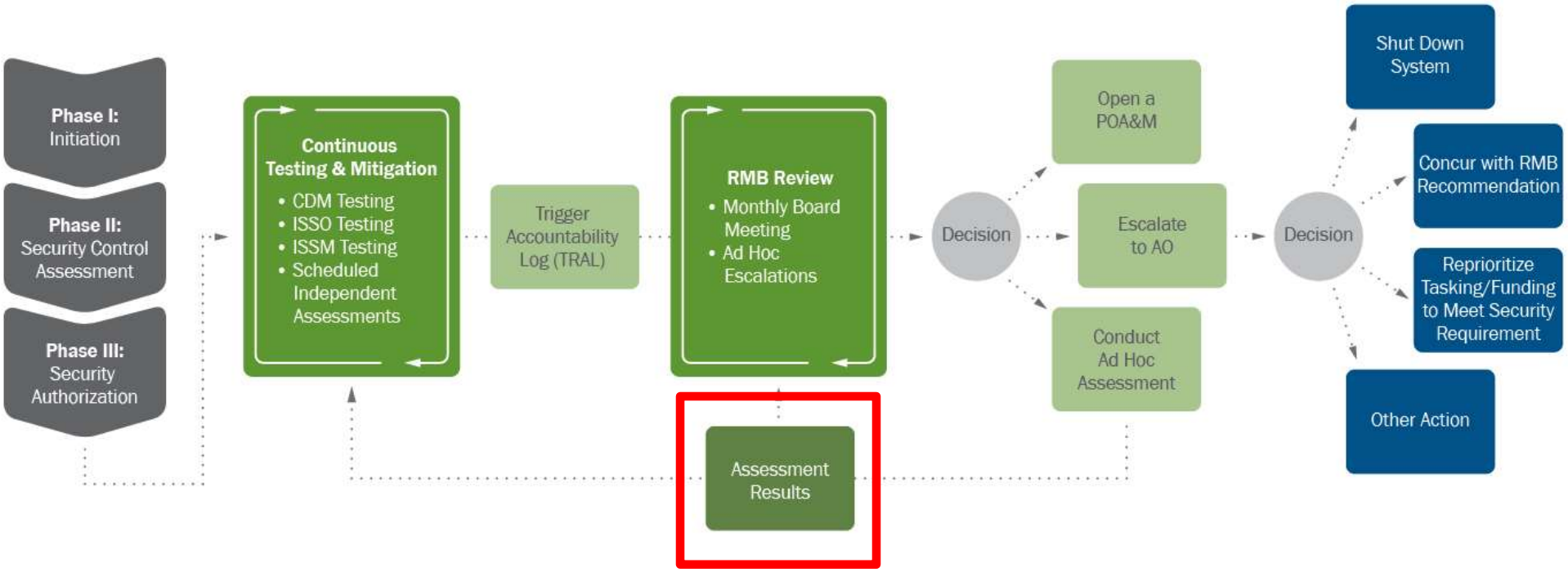
USCIS OA PROGRAM: AO ENGAGEMENT

U.S. Citizenship and Immigration Services



- Monthly meetings with CISO/AO to review security posture, POA&M status and remediation plans, and gain concurrence and/or new direction on risk-based decisions.
- Escalated triggers are also reviewed with the CISO/AO monthly.
  - The OA Team will collaborate with the ISSO to identify recommendations for remediation and next steps.

USCIS OA PROGRAM: INDEPENDENT ASSESSMENTS



- Periodic independent assessments occur according to the FIPS categorization of the system and/or at the discretion of the RMB and CISO/AO. Results from these assessments are further reviewed by the RMB.

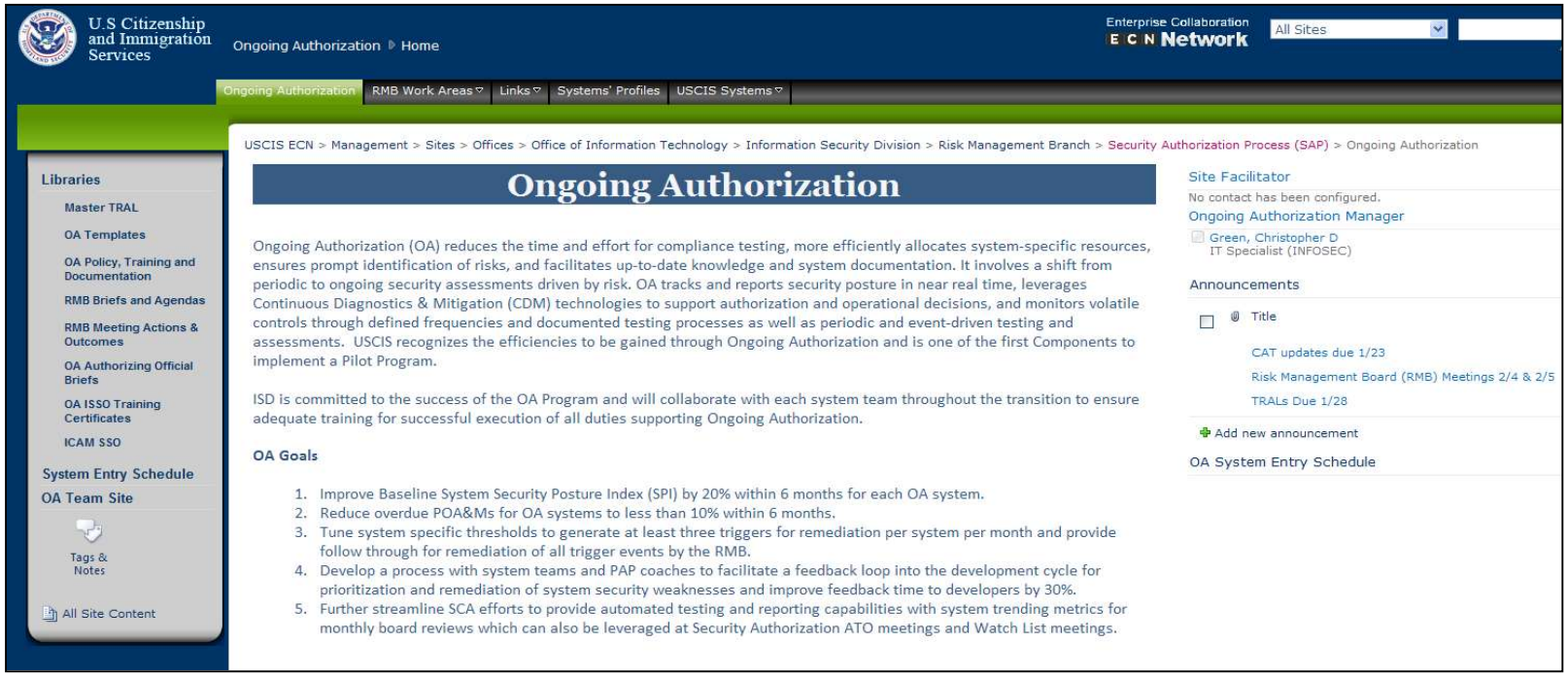
INDEPENDENT ASSESSMENTS

U.S. Citizenship and Immigration Services

- Limited: Includes controls that can be assessed through automated mechanisms.
- OA: The independent SCA Team tests controls in accordance with the CAT schedule to validate ISSO testing activities. However, the tested controls are a limited subset based on the OA methodology.
- Full: Similar to the SCA conducted as part of the traditional SAP process to obtain an initial ATO. Full assessments include all of the controls applicable to a system.
- Independent assessment results are documented in a Security Assessment Report (SAR) with any vulnerabilities identified further in a POA&M Table prior to entry into IACS.

ECN: OA DOCUMENTS

- All OA documents are stored and managed on ECN
  - System entry documentation, CAT, and TRAL
  - RMB meeting briefs, agendas, and actions
  - Templates, training, and other resources



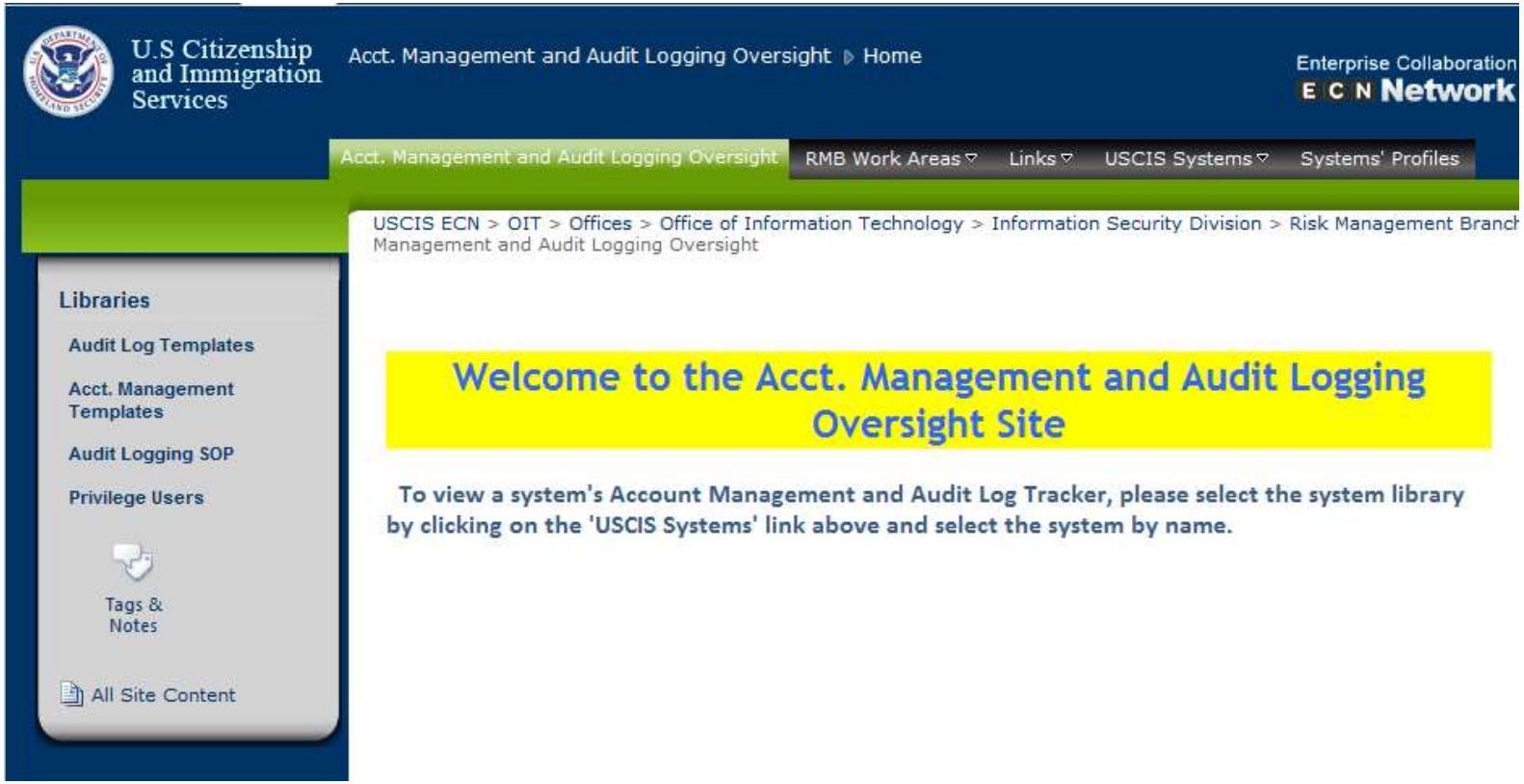
ECN: OA RMB CALENDAR

U.S. Citizenship and Immigration Services

- The OA RMB Calendar is populated with RMB meeting and OA compliance due dates and is available on the OA ECN.

ECN: OA ACCOUNT MANAGEMENT AND AUDIT LOGS

- Acct. Management and Audit Logging Oversight ECN
  - Account Management Review and Audit Log Review Trackers are stored and maintained within the system libraries



REFERENCES

U.S. Citizenship and Immigration Services

- NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations
- NIST SP 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations
- NIST SP 800-37, Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
- NIST Supplemental Guidance on Ongoing Authorization
- DHS Ongoing Authorization Methodology, version 1.7

U.S. Citizenship and Immigration Services

QUESTIONS?