IT SECURITY & THE TSP

MAY 18, 2015

Agenda

- □ Tale of Two Auditors
- Timeline
 - Organizational Changes
 - Enterprise Risk Management
 - Audit Findings
 - IT Security Progress
 - System Authorizations
- What's Next

Tale of Two Auditors

CliftonLarsonAllen

"...I'll just say that as progress forward, it's been really impressive to see...So, you know, great job from both the Board making it a priority and then obviously management for addressing those. So I did want to at least point that out, significant progress."

EBSA

Without updates, FRTIB "will not be able to prevent...unauthorized disclosure of the systems and data," Dingwall said.

There are significant holes in the agency's mainframe and access management, he added, "collectively opening the agency to unnecessary risk."

TIMELINE

2012 2013 2014 2015 **MAY 2012 FEBRUARY 2013** FEBRUARY 2014 FEBRUARY 2015 Security Operations Center (SOC) Established Board Approved Internal Audit Plan Office of Enterprise Risk Hired Chief Risk Officer Management Established **APRIL 2014** 99% of FRTIB Staff Acknowledged (Signed) IT **MARCH 2013** Hired Head Of Internal Audit Rules of Behavior Information Assurance Division **APRIL 2012** (IAD) Established Cyber attack Identified FEBRUARY 2015 FRTIB IT Sec Roles and Responsibilities Completed Interconnection Security Agreement (ISA) (NIST SP 800 53 Rev 4) 6 Information System Security Officers **JUNE 2012** Procedure Completed (ISSO) Established **DECEMBER 2014** 18 Enterprise Information Security and Risk **APRIL 2015** Sr. Agency Official for Privacy (SAOP) Established Management (EISRM) Policies Completed Chief Information Security Officer Commenced First Internal Audit Review (NIST SP 800 53 Rev 3) **AUGUST 2014** (CISO) hired IT Sec Clauses Added to Major IT Contracts **JULY 2013** Baseline Security Requirements (BLSR) Replaced **AUGUST 2012** SEPTEMBER 2014 Certification Agent Established EISRM Policies (NIST SP 800 53 Rev 4) Security Education, Training and Awareness EISRM Limited Use Policy Completed Program (SETA) Procedure Completed **AUGUST 2013** Security Impact Analysis Procedure Completed **MARCH 2012** Hired Head of Anti-Fraud Unit OCTOBER 2014 10 Audit Findings Closed Board Approved Internal Audit Charter SEPTEMBER 2013 6 Audit Findings Closed (January – March) **MARCH 2014 DECEMBER 2012** IAD Risk Manager Established 35 Audit Findings Closed Technology and Enterprise Support Services **JANUARY 2015 JUNE 2013 FEBRUARY 2014** DHS Cyber Hygiene Scans Ongoing (TESS) RFP Issued Internal Controls Unit formalized; ServiceNow Deployed POA&M Remediation Plan Formalized reviews commenced MAY 2014 **FEBRUARY 2015** Next Generation Firewall Implemented **MARCH 2013** Security Operations Center (SOC) Transitioned 13 Audit Findings Closed **JUNE 2014** to CISO Media Protection Procedure Completed **AUGUST 2013** Security Incident & Event Mgt (SIEM) Security Tool Gap Analysis Mapping Completed Organizational Changes TESS Contract Awarded to SAIC Tool Implemented (NIST SP 800 53 Rev 4, NIST SP 800 137) OCTOBER 2013 FEBRUARY 2014 FEBRUARY 2015 Enterprise Risk Management Info Assurance Analyst Support Contract 1 A&A Completed 1 A&A Completed **Audit Findings** Awarded **APRIL 2014 APRIL 2015** 1 A&A Completed **NOVEMBER 2013** 2 A&AS Completed **IT Security Progress JUNE 2014** 3rd Party Web Applications Scans **JUNE 2015** 3 A&As Completed 1 ATO In Process* System Authorizations **JUNE 2013** AUGUST 2014 1 A&A Completed 1 A&A To Be Completed* 1 A&A Completed **DECEMBER 2015** SEPTEMBER 2014 5 A&As To Be Completed* 1 A&A Completed

NOVEMBER 2014

1 A&A Completed

*Planned

TIMELINE – Organizational Changes

2012 2013 2014 2015 MAY 2012 FEBRUARY 2013 FEBRUARY 2014 FEBRUARY 2015 Hired Chief Risk Officer Office of Enterprise Risk Security Operations Center **Board Approved Internal** Management Established (SOC) Established Audit Plan **MARCH 2013** 99% of FRTIB Staff Information Assurance Division **APRIL 2014** Acknowledged (Signed) IT (IAD) Established Hired Head Of Internal Audit Rules of Behavior 6 Information System Security JULY 2014 Officers (ISSO) Established FRTIB IT Sec Roles and **Chief Information Security** Responsibilities Completed Officer (CISO) hired (NIST SP 800 53 Rev 4) **JULY 2013** DECEMBER 2014 Certification Agent Sr. Agency Official for Established Privacy (SAOP) Established AUGUST 2013 Hired Head of Anti-Fraud Unit SEPTEMBER 2013 IAD Risk Manager Established

TIMELINE – Enterprise Risk Management

2014 2012 2013 2015 AUGUST 2014 **APRIL 2012 JUNE 2013** FEBRUARY 2015 IT Sec Clauses Added to Cyber attack Identified Internal Controls Unit Interconnection Security Major IT Contracts formalized; reviews Agreement (ISA) commenced Procedure Completed **JUNE 2012** 18 Enterprise Information SEPTEMBER 2014 Security Education, Training Security and Risk Management **APRIL 2015** (EISRM) Policies Completed and Awareness Program Commenced First Internal (NIST SP 800 53 Rev 3) (SETA) Procedure Completed **Audit Review** AUGUST 2012 OCTOBER 2014 MAY 2015 **EISRM Limited Use Policy Board Approved Internal Baseline Security Requirements** Completed **Audit Charter** (BLSR) Replaced EISRM Policies (NIST SP 800 53 Rev 4)

Security Impact Analysis Procedure Completed

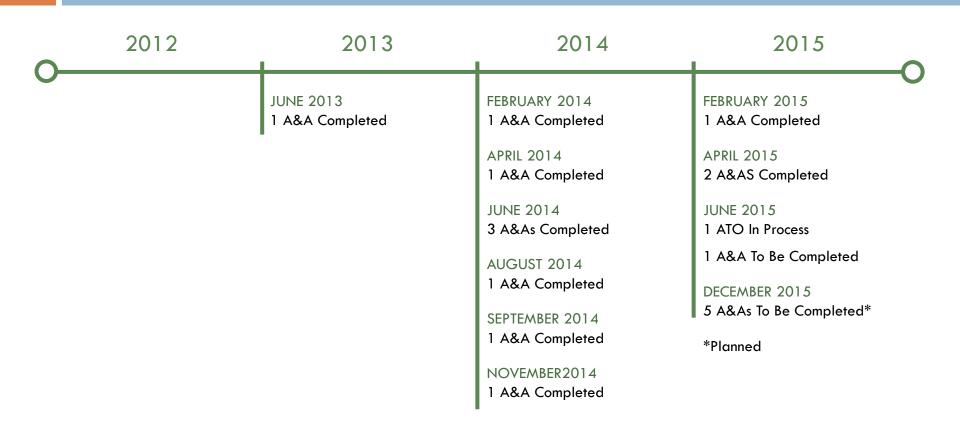
TIMELINE – Audit Findings



TIMELINE – IT Security Progress

2012 2013 2014 2015 DECEMBER 2012 AUGUST 2013 FEBRUARY 2014 JANUARY 2015 **TESS Contract Awarded** Technology and Enterprise ServiceNow Deployed DHS Cyber Hygiene Scans Support Services (TESS) RFP to SAIC Ongoing Issued MAY 2014 POA&M Remediation Plan OCTOBER 2013 **Next Generation Firewall Formalized** Info Assurance Analyst Implemented Support Contract Awarded FEBRUARY 2015 JUNE 2014 Security Operations Center NOVEMBER 2013 Media Protection Procedure (SOC) Transitioned to CISO 3rd Party Web Completed Security Incident & Event Mgt **Applications Scans** Security Tool Gap Analysis (SIEM) Tool Implemented Mapping Completed (NIST SP 800 53 Rev 4, NIST SP 800 137)

TIMELINE – System Authorizations



What's Next?

Continue strengthening and adding resilience to the Agency's Vulnerability Assessment Program

- Penetration Testing
- Remaining Assessments & Authorizations
- Governance, Risk, and Compliance (GRC)
 Management Information System
- Adaptive Authentication