

FEDERAL RETIREMENT THRIFT INVESTMENT BOARD 77K Street, NE Washington, DC 20002

FOR IMMEDIATE RELEASE May 18, 2015

EXECUTIVE DIRECTOR PROVIDES BRIEFING ON INFORMATION SECURITY PROGRAM AND RESPONDS TO LETTER FROM SENATORS JOHNSON AND CARPER

Washington, D.C. – Greg Long, the Executive Director of the Federal Retirement Thrift Investment Board (FRTIB), today provided a briefing to Agency Board members and members of the Employee Thrift Advisory Council (ETAC) regarding the Agency's robust information security program. Mr. Long shared with the Members of the Board and ETAC an overview of the initiatives and activities that the FRTIB has undertaken over the last three years. This overview is attached.

Mr. Long said, "We administer a very large defined contribution plan that exists solely to allow our participants to retire with dignity. We owe it to our 4.7 million participants to implement and maintain strong but ever-evolving information security and risk management practices. I can assure you we take this responsibility very seriously."

In 2012, the FRTIB established the Office of Enterprise Risk Management (OERM), which consists of the internal controls group, the anti-fraud group, the risk management group, and the internal audit group. Also in 2012, within the Office of the Chief Technology Officer, the FRTIB established a separate Information Assurance Division, led by a Chief Information Security Officer. In addition, the FRTIB has deployed a Security Operations Center (SOC) and a Network Operations Center (NOC) to monitor and assess IT security risks to the organization.

In furtherance of the Agency's activities under FISMA, an Enterprise Information Security & Risk Management (EISRM) program and 19 associated information security policies were implemented. In accordance with these new EIRSM policies, the Agency reviewed and updated system boundary delineations, which led to the designation of 19 separate systems. The FRTIB initiated assessment and authorization (A&A) activities of each system and, as of today, 14 of these 19 A&As are completed. The remaining A&A work will be concluded by December 2015.

All of these initiatives have been undertaken to continually improve the security posture of the Agency and the participant information it maintains. In addition to these benefits, this focus on people, process and technology over the past three years has allowed the

Agency to make steady progress in closing audit findings. Mr. Long committed to the Board and ETAC that this focus will continue as a part of the Agency's standard business practice and focus.

The FRTIB response to the letter from Senators Johnson and Carper can be found at www.frtib.gov/ReadingRoom/PressRel/PR-2015-05-18-ResponsetoSen.pdf

The TSP is a retirement savings plan for Federal employees; it is similar to the 401(k) plans offered by many private employers. As of April 2015, TSP assets totaled approximately \$454.0 billion, and retirement savings accounts were being maintained for more than 4.7 million TSP participants. Participants include Federal civilian employees in all branches of Government, employees of the U.S. Postal Service, and members of the uniformed services. Additional information can be found at www.tsp.gov.

MEDIA CONTACT:

Kim Weaver 202-942-1641

(end)

IT SECURITY & THE TSP

MAY 18, 2015

Fact-Based Review



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

JUNE 2012

18 Enterprise Information Security and Risk Management (EISRM) Policies Completed (NIST SP 800 53 Rev 3)

AUGUST 2012

EISRM Limited Use Policy Completed

SEPTEMBER 2014

Security Education, Training and Awareness Program (SETA) Procedure Completed

OCTOBER 2014

Board Approved Internal Audit Charter

Procedure Completed

APRIL 2015

Commenced First Internal **Audit Review**

MAY 2015

Baseline Security Requirements (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

2012	2013	2014	2015
	JUNE 2013 1 A&A Completed	FEBRUARY 2014 1 A&A Completed APRIL 2014 1 A&A Completed JUNE 2014 3 A&As Completed AUGUST 2014 1 A&A Completed SEPTEMBER 2014 1 A&A Completed NOVEMBER 2014 1 A&A Completed	FEBRUARY 2015 1 A&A Completed APRIL 2015 2 A&AS Completed JUNE 2015 1 ATO In Process 1 A&A To Be Completed DECEMBER 2015 5 A&As To Be Completed* *Planned

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