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
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

- Office of Enterprise Risk Management Established
- Cyber attack Identified
- 18 Enterprise Information Security and Risk Management (EISRM) Policies Completed (NIST SP 800 53 Rev 3)
- EISRM Limited Use Policy Completed
- 10 Audit Findings Closed
- Technology and Enterprise Support Services (TESS) RFP Issued

2013

- Hired Chief Risk Officer
- Information Assurance Division (IAD) Established
- 6 Information System Security Officers (ISSO) Established
- Chief Information Security Officer (CISO) hired
- Certification Agent Established
- Hired Head of Anti-Fraud Unit
- IAD Risk Manager Established
- Internal Controls Unit formalized; reviews commenced
- 13 Audit Findings Closed
- TESS Contract Awarded to SAIC
- Info Assurance Analyst Support Contract Awarded
- 3rd Party Web Applications Scans
- 1 A&A Completed

2014

- Security Operations Center (SOC) Established
- Hired Head Of Internal Audit
- FRTIB IT Sec Roles and Responsibilities Completed (NIST SP 800 53 Rev 4)
- Sr. Agency Official for Privacy (SAOP) Established
- IT Sec Clauses Added to Major IT Contracts
- Security Education, Training and Awareness Program (SETA) Procedure Completed
- Board Approved Internal Audit Charter
- 35 Audit Findings Closed
- ServiceNow Deployed
- Next Generation Firewall Implemented
- Media Protection Procedure Completed
- Security Tool Gap Analysis Mapping Completed (NIST SP 800 53 Rev 4, NIST SP 800 137)
- 1 A&A Completed
- 2 A&AS Completed
- 1 ATO In Process*
- 1 A&A To Be Completed*
- 5 A&As To Be Completed* (Planned)

2015

- Board Approved Internal Audit Plan
- 99% of FRTIB Staff Acknowledged (Signed) IT Rules of Behavior
- Interconnection Security Agreement (ISA) Procedure Completed
- Commenced First Internal Audit Review
- Baseline Security Requirements (BLSR) Replaced EISRM Policies (NIST SP 800 53 Rev 4)
- Security Impact Analysis Procedure Completed
- 6 Audit Findings Closed (January – March)
- DHS Cyber Hygiene Scans Ongoing
- POA&M Remediation Plan Formalized
- Security Operations Center (SOC) Transitioned to CISO
- Security Incident & Event Mgt (SIEM) Tool Implemented
- 1 A&A Completed
- 2 A&AS Completed
- 1 A&A To Be Completed*
- 1 A&A To Be Completed*
- 5 A&As To Be Completed*
TIMELINE – Organizational Changes

2012

MAY 2012
Office of Enterprise Risk Management Established

2013

FEBRUARY 2013
Hired Chief Risk Officer

MARCH 2013
Information Assurance Division (IAD) Established
6 Information System Security Officers (ISSO) Established
Chief Information Security Officer (CISO) hired

JULY 2013
Certification Agent Established

AUGUST 2013
Hired Head of Anti-Fraud Unit

SEPTEMBER 2013
IAD Risk Manager Established

2014

FEBRUARY 2014
Security Operations Center (SOC) Established

APRIL 2014
Hired Head Of Internal Audit

JULY 2014
FRTIB IT Sec Roles and Responsibilities Completed
(NIST SP 800 53 Rev 4)

DECEMBER 2014
Sr. Agency Official for Privacy (SAOP) Established

2015

FEBRUARY 2015
Board Approved Internal Audit Plan
99% of FRTIB Staff Acknowledged (Signed) IT Rules of Behavior
TIMELINE – Enterprise Risk Management

2012
APRIL 2012
Cyber attack Identified

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

2013
JUNE 2013
Internal Controls Unit formalized; reviews commenced

2014
AUGUST 2014
IT Sec Clauses Added to Major IT Contracts

SEPTEMBER 2014
Security Education, Training and Awareness Program (SETA) Procedure Completed

OCTOBER 2014
Board Approved Internal Audit Charter

2015
FEBRUARY 2015
Interconnection Security Agreement (ISA) 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

- **2012**
  - MARCH 2012
    - 10 Audit Findings Closed

- **2013**
  - MARCH 2013
    - 13 Audit Findings Closed

- **2014**
  - MARCH 2014
    - 35 Audit Findings Closed

- **2015**
  - MARCH 2015
    - 6 Audit Findings Closed (January – March)
TIMELINE – IT Security Progress

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

2012

JUNE 2013
1 A&A Completed

2013

FEBRUARY 2014
1 A&A Completed

APRIL 2014
1 A&A Completed

JUNE 2014
3 A&As Completed

2014

AUGUST 2014
1 A&A Completed

SEPTEMBER 2014
1 A&A Completed

2015

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