



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

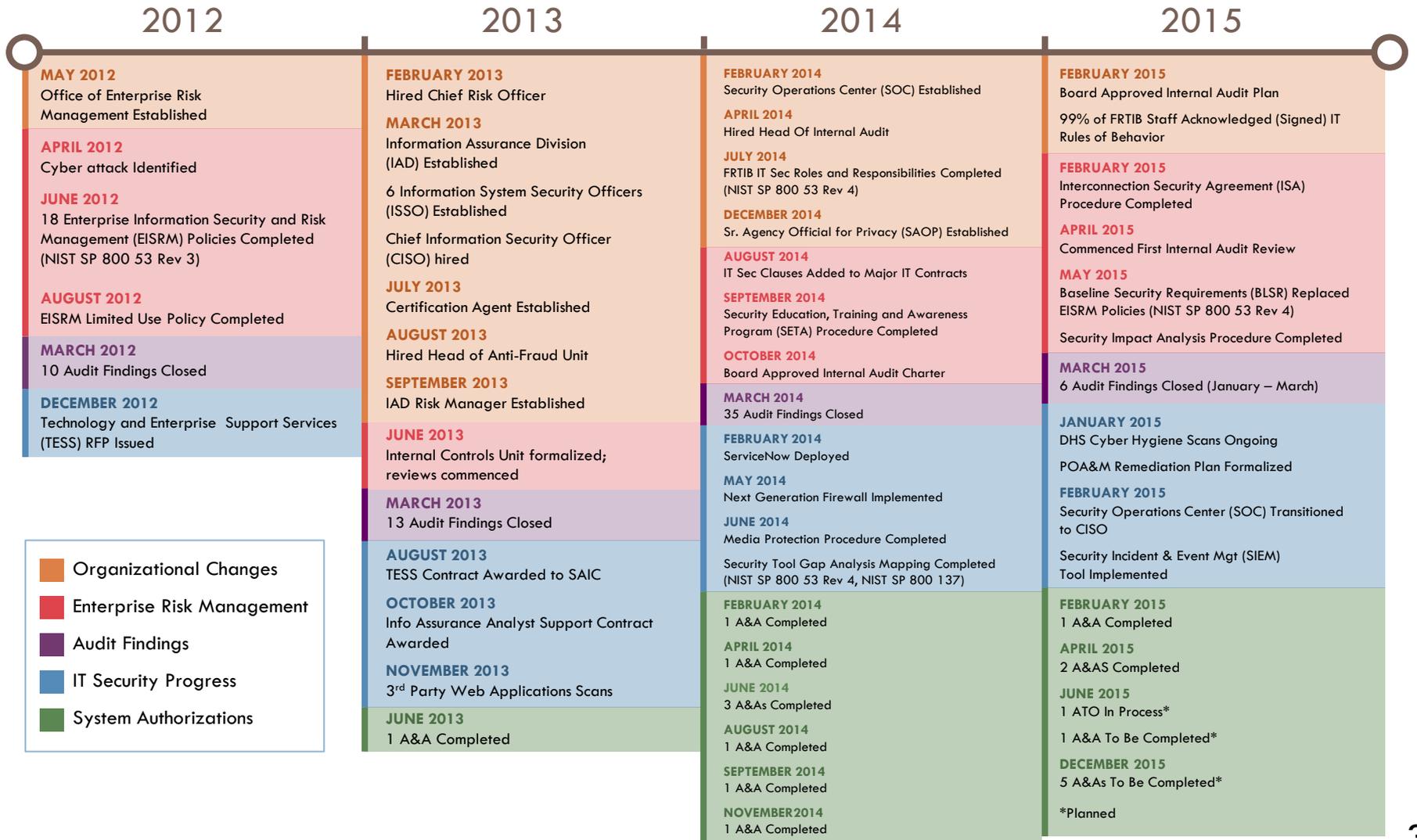
“...I’ll just say that as progress forward, it’s been really impressive to see...So, you know, great job from both the Board making it a priority and then obviously management for addressing those. So I did want to at least point that out, significant progress.”

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.”

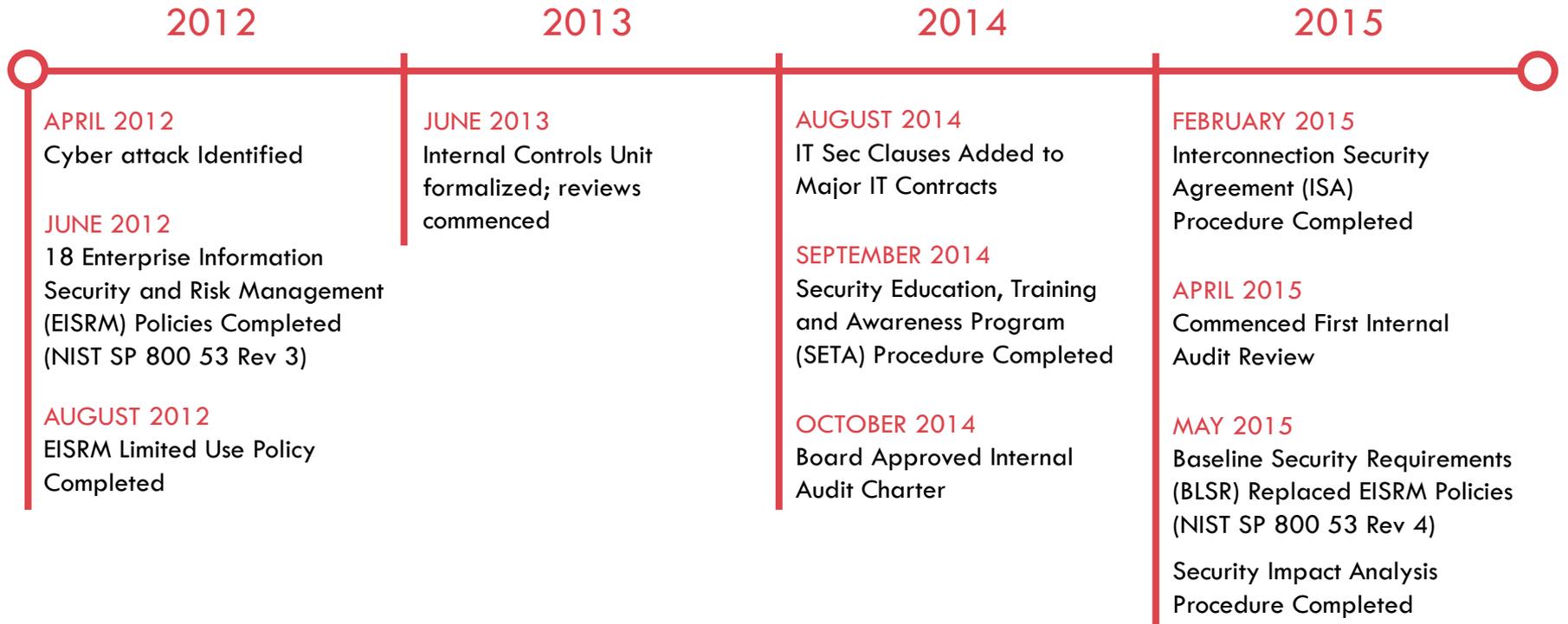
TIMELINE



TIMELINE – Organizational Changes



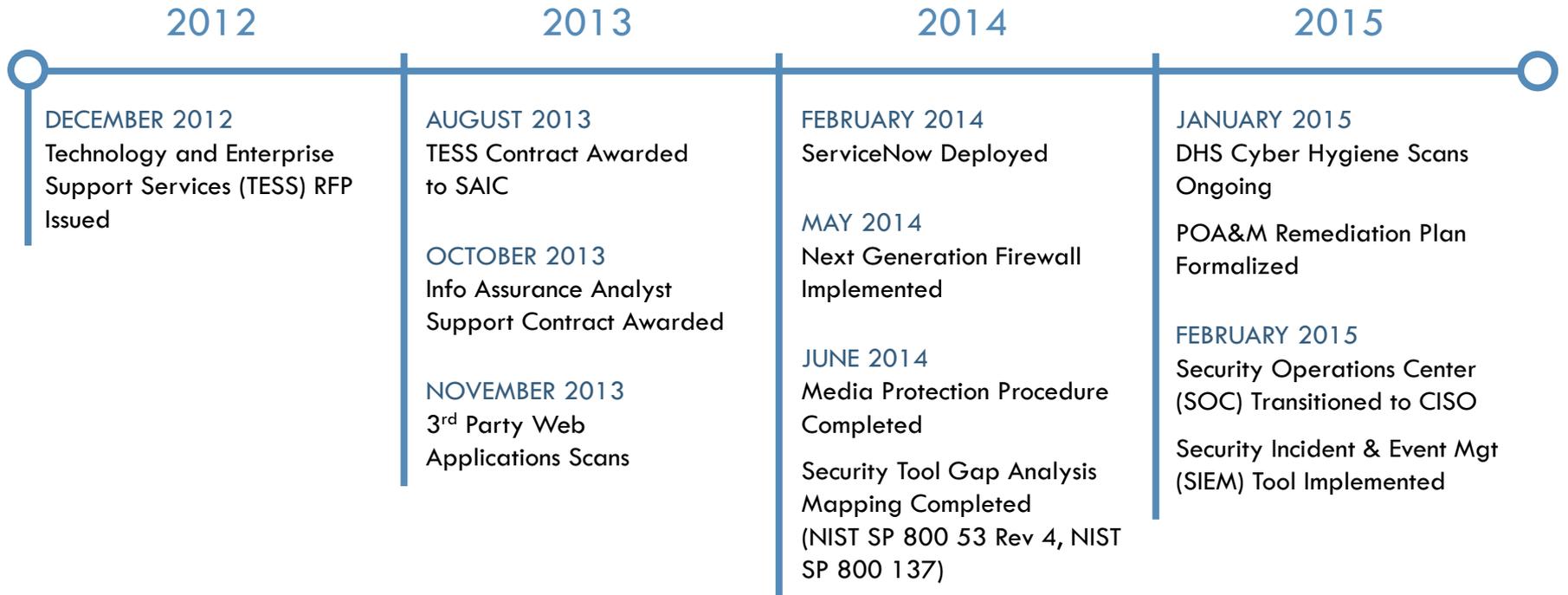
TIMELINE – Enterprise Risk Management



TIMELINE – Audit Findings



TIMELINE – IT Security Progress



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