Federal Retirement Thrift Investment Board (FRTIB)

Board Meeting

Fiscal Year (FY) 2016 Federal Information Security Modernization Act (FISMA) Performance Audit

February 27, 2017

Building a better working world

Agenda

- Introductions and Opening Remarks
- FISMA Performance Audit Objective
- Scope and Methodology
- FY 2016 IG FISMA Metrics – Summary Results
- Questions and Closing Remarks

Introductions & Opening Remarks

- Federal Retirement Thrift Investment Board (FRTIB)
- Ernst & Young (EY)
  - Werner Lippuner – Principal
  - Angel Contreras – Senior Manager

FISMA Performance Audit Objectives

- EY was engaged by the FRTIB's Office of Enterprise Risk Management (OERM) Internal Audit Division to conduct the annual independent and objective evaluation of the information security program in accordance with the FISMA Inspector General (IG) metrics.
- EY assessed program elements at the enterprise-level and for 4 in-scope systems supporting the Thrift Savings Plan (TSP) to determine compliance with Federal standards measured by the Department of Homeland Security (DHS) Office of Cybersecurity and Communications (CS&C) reporting metrics from the Fiscal Year (FY) 2016 FISMA IG metrics.
- EY conducted a Performance Audit for FRTIB in accordance with Generally Accepted Government Auditing Standards (GAGAS).
- The objective of the Performance Audit was to provide results for the FY 2016 FISMA IG metrics based on an evaluation of sufficient and appropriate evidence.

FISMA Audit Scope & Methodology

- FISMA evaluations was performed for the following 4 FRTIB in-scope systems:
  - Core Record Keeping Services (CRS), Financial and Reconciliation Services (FRS), Participant Interaction Services (PIS), and TSP Distributed System (TDS).
- Assessed the FY 2016 FISMA IG metrics – which included the following areas:
  - Risk Management, Contractor Systems, Configuration Management, Identity and Access Management, Security and Privacy Training, Information Security Continuous Monitoring, Incident Response, and Contingency Planning.
- Assessed the extent to which FRTIB has documented and implemented IT security requirements for the four in-scope systems during FY 2016.

FRTIB Information Security Program Progress

- FRTIB conducted its first ever FISMA Inspector General audit in FY 2016.
- FRTIB has made progress in the security posture (e.g., completing 13 System Authorizations throughout 2015).
- FRTIB continues to strengthen its information security controls by initiating programs such as the implementation of Personal Identification Verification (PIV) program.
- Based on the FISMA audit results – corrective actions have begun which include the review and update of policies and procedures, the establishment of various groups such as the ISSO Management Branch (IMB) and the SOC Management Branch (SMB) within the Information Assurance Division (IAD).

EY

FY 2016 FISMA Audit – Summary Results

- **Risk Management** – FRTIB has not fully implemented a Risk Management strategy and has not established appropriate assessment procedures to continuously assess the security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome.

  Additionally, FRTIB has not established procedures to validate FRTIB's system inventory accuracy and has not developed Interconnection Security Agreements for systems within scope of the audit.

FY 2016 FISMA Audit – Summary Results

- **Contractor Systems** – FRTIB has not established and fully implemented a program to oversee systems operated on its behalf by contractors. In particular, Management has not established a formal process to consistently validate how information security performance is measured, reported, and monitored for contractor managed or operated information systems.
- **Configuration Management** – FRTIB's inventory of assets is not fully accurate and incomplete, security baselines required strengthening, a process that validates a list of changes from the production environment has not been established, and known vulnerabilities have not been completely remediated.

EY

FY 2016 FISMA Audit – Summary Results

- **Identity and Access Management** – FRTIB has not fully implemented an Identity and Access Management program, which should include (but is not limited to), granting user access based on the least privilege principle, annual review of privileged users, establishment of a Personal Identification Verification (PIV) program for logical and physical access, controls that govern shared accounts, segregation of duties matrices, and enhancements regarding remote access configurations.

FY 2016 FISMA Audit – Summary Results

- **Security and Privacy Training** – FRTIB has not provided a specialized security awareness and privacy training to its Executives, Information Technology (IT) Administrators and Managers having significant security responsibilities. Additionally, although Management has a process in place for tracking access related to the standard privacy training for contractors, Management has not implemented a control that validates the actual completion of privacy training.
- **Information Security Continuous Monitoring** – FRTIB's ISCM program has not been fully developed and related policy and procedures have not been finalized. Furthermore, ISCM training has not been developed for key ISCM personnel.

FY 2016 FISMA Audit – Summary Results

- **Incident Response** – Current policy does not include elements of an Incident Response program, such as training, designation of responsibilities for the Security Operations Center (SOC), collaboration procedures with DHS to respond to incidents to include utilization of DHS' Einstein program, and integration of IR requirements into FRTIB's other key business areas.
- **Contingency Planning** – An overarching Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) have not been fully developed and implemented for the organization. Additionally, associated contingency planning tests have not been performed.

Questions & Closing Remarks