Federal Retirement Thrift Investment Board – Thrift Savings Fund

Status of Prior Recommendations

November 17, 2014

CliftonLarsonAllen

cliftonlarsonallen.com

Marie Caputo, Principal

Status of Prior Recommendations

- As part of our review procedures, we updated our understanding of internal controls
  - We did not test operating effectiveness of the controls
  - We did not test any changes made to improve areas commented on in previous years

- We did update our understanding of status of prior recommendations (summarized in following table)

Summary – June 30, 2014 Interim Review
Status of Prior Recommendations (continued)

Prior Comment/ Recommendation	Status per Discussions with Agency Personnel
2013-1 System Authorizations	FRTIB identified 19 systems which require security authorizations. The authorization and accreditation (A&A) process has been initiated for 18 systems, 8 systems have received an Authorization To Operate (ATO), 13 systems are expected to receive their ATO by 12/31/14, and all systems are expected to be fully authorized to operate by 9/30/15. FRTIB tracks the current progress of A&A efforts on a dashboard spreadsheet. The previously identified 21 major applications and general support systems have been re-baselined into 18 systems with one new system added "Service Now", for a total of 19 systems. "ENS" already underwent a full assessment and authorization as of June 2013 and is currently undergoing its annual testing of security controls as part of continuous monitoring.

Summary – June 30, 2014 Interim Review
Status of Prior Recommendations (continued)

Prior Comment/ Recommendation	Status per Discussions with Agency Personnel
2013-2 Savantage Segregation of Duties	FRTIB expects to complete the development of a segregation of duties matrix by mid October 2014, with a review of user profiles by 10/31/14, with subsequent updates or creation of all profiles to be completed by 12/31/14.

Summary – June 30, 2014 Interim Review
Status of Prior Recommendations (continued)

Prior Comment/ Recommendation	Status per Discussions with Agency Personnel
2013-3 Service Level Agreements	Management hired SAIC to implement the Technology and Enterprise Support Services (TESS) contract to include 144 service level requirements (SLRs). FRTIB continues to work with SAIC to understand and fine tune SLR performance metrics and expected reporting deliverables. SAIC provides FRTIB with monthly service level reports which discuss the status of each SLR. Based upon subsequent SAIC and FRTIB discussions, reductions in the total number of SLRs were possible due to aggregation and consolidation efforts. Thus, the original 144 SLRs were reduced to a total of 76 SLRs however still map back to the original Statement of Work (SOW) SLRs identified as "critical" are of primary focus for metrics performance reporting, As part of a phased implementation approach, about 50% of the 76 SLRs are currently in pilot status, with migration into production status expected approximately 3 months later. The remaining SLRs (on Hold) are undergoing further definition of measurement processes, data gathering processes, and determination of data availability and ease of collection. FRTIB and SAIC also maintain a performance management matrix which tracks SLRs, and captures data such as completion status, criticality, timeframes and delivery requirements, priority levels, etc. FRTIB conducts ongoing reviews with SAIC to ensure SLR status is accurate.

Summary – June 30, 2014 Interim Review
Status of Prior Recommendations (continued)

Prior Comment/ Recommendation	Status per Discussions with Agency Personnel
2013-4 Logging and Monitoring of user system activity	Management is in the process of analyzing business roles described within the Trustwave Security Information and Event Management tool (SIEM) to see if it still meets FRTIB logging and monitoring needs since conversion to SAIC. Full implementation of the SIEM tool is anticipated by 6/30/15. The Platinum application is in the process of being replaced by the Sage application, with the migration expected to be completed by December 2014.
2013-6 Inactive mainframe accounts	Management is approximately 80% complete with their review of critical system mainframe accounts. This is part of a larger ongoing internal compliance review effort. A compliance review process kickoff letter was issued by the Chief Information Security Officer which describes the purpose, goals, methodology and responsibilities in order to conduct a 2014 compliance review of identification and authentication, access controls, and audit and accountability requirements across all FRTIB information systems. This review process includes a review of all accounts to include user accounts, service accounts and any authorized share accounts.

Summary – June 30, 2014 Interim Review
Status of Prior Recommendations (continued)

Prior Comment/ Recommendation	Status per Discussions with Agency Personnel
2013-7 Business Impact Analysis	Management awarded a contract to a vendor on 5/27/14 to perform Business Impact Analysis and Business Continuity services with an anticipated project completion date of 12/31/14.
2013-8 Incident Management	Management is in the process of presenting a task order to SAIC to build the infrastructure to implement an incident management module of the Governance Risk Compliance tool. This module is expected to be fully operational by 12/31/14 and should provide a central repository for all IT security incidents.

Questions?