OFFICE OF INSPECTOR GENERAL

Audit Report

Fiscal Year 2016 Audit of Information Security at the Railroad Retirement Board

This abstract summarizes the results of the subject audit. The full report includes information protected from disclosure and has been designated for limited distribution pursuant to 5 U.S.C. § 552

Report No. 17-06
June 16, 2017

RAILROAD RETIREMENT BOARD

REPORT ABSTRACT
Fiscal Year 2016 Audit of Information Security At the Railroad Retirement Board

The Office of Inspector General (OIG) for the Railroad Retirement Board (RRB) conducted an audit of information security at the RRB for fiscal year 2016, as mandated by the Federal Information Security Modernization Act of 2014 (FISMA). FISMA requires an assessment of effectiveness of the agency's information security policies, procedures, and practices using a five level maturity model with the National Institute of Standards and Technology cybersecurity framework. An assessment of effectiveness considers internal control integration and whether the organization is achieving its intended objective.

Objectives

The objectives of our audit included:

- testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems;
- an assessment of the effectiveness of RRB's information security policies, procedures, and practices; and
- preparing a report on selected elements of the agency's information security program in compliance with the fiscal year 2016 FISMA reporting instructions.

Results of Audit

Our audit determined that RRB continues to make progress in implementing an information security program that meets the requirements of FISMA; yet a fully effective security program, and related information security policies, procedures, and practices, has not been achieved.

The overall information security program has weaknesses that impact more than one area of the cybersecurity framework. These overarching program weaknesses involve the need for new or updated policy and procedures, improper placement of the Chief Security Officer within the organization, resource constraints, and the lack of performance metrics. Our review of RRB's information security program also identified deficiencies in the areas of risk management, contractor systems, configuration management, identity and access management, security and privacy training, continuous monitoring management, incident response and reporting, and contingency planning. Each of these OIG FISMA metric domains and the corresponding cybersecurity framework functions have been assessed as 'Not Effective' when evaluated using the five level maturity model. The OIG submitted its online CyberScope report on the adequacy of RRB's information security controls for each of the eight OIG FISMA metric domains and the effectiveness of the five corresponding cybersecurity framework functions on November 9, 2016.

Recommendations

In total, we made 36 detailed recommendations to RRB management related to assorted policies, procedures, and plans; access control; training; resource management; performance management; updating agency records; exploring and using new automated technologies; and implementing stronger controls. Thirty-five of the recommendations were made in our independent auditor's report and one recommendation was made in Priority Audit Memorandum - Legal Opinion Digitization Contract (RRB13C003), October 4, 2016.

Management's Responses

Agency management either concurred or generally concurred with 32 of our 35 recommendations, partially concurred with 1 recommendation, and did not concur with 2 recommendations.[1] Agency management also advised that all personally identifiable information has been deleted from their contractor's system in response to our recommendation in the priority audit memorandum, but they are awaiting the final contractor's certification of this action.

The Bureau of Information Services (BIS) generally concurred with our recommendation concerning the improper placement of the Chief Security Officer within the organization and advised that the Chief Information Security Officer was approved to consult with the Chief Information Officer directly on any information security matters; is expected to meet with the Chief Information Officer on a weekly basis; and is expected to report directly to the Chief Information Officer on any cybersecurity issue that poses a threat to the agency. These actions meet the intent of our audit recommendation.

BIS did not concur with one recommendation and a portion of another recommendation, dealing with privacy training. BIS did not concur because although two positions met the minimum required timeframe in fiscal year 2016 for working on privacy related functions that directly support the agency's privacy program (at least half their time), those two positions are currently vacant in fiscal year 2017. We believe the two recommendations related to the Chief Privacy Officer still have merit and we will continue to track for future implementation through our semiannual update on corrective actions of audit recommendations.

The Bureau of Fiscal Operations (BFO) did not concur with our recommendation to evaluate and assess the skills of individuals in BFO with significant security and privacy responsibilities and provide that information to the Chief Security Officer or Chief Privacy Officer. BFO stated such responsibility does not fall under their purview. We disagree. Agency supervisors and managers are in the best position to evaluate and assess the skills of their employees, including those employees who have significant

[1] For the two recommendations in which the Bureau of Information Services did not concur, one recommendation dealt wholly with privacy training, while the other recommendation dealt partially with privacy training and partially with security training. The Bureau of Information Services concurred with the portion of the recommendation that dealt with security training.

security or privacy responsibilities. Effective training programs include developing individual development plans that consider an employee's skills, and ensuring that the training plan addresses identified skill gaps. Additionally, the RRB's security awareness and training procedures require supervisors to assign role based training annually to their employees designated as having information security responsibilities. The determination of what role based training to assign should consider the employee's individual development plan and skills. Therefore, we will continue to track the recommendation for implementation through our semiannual update on corrective actions of audit recommendations.