OFFICE OF INSPECTOR GENERAL

Audit Report

Review of the Railroad Retirement Board's Security Patch Management Process

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. 11-08
July 7, 2011

RAILROAD RETIREMENT BOARD

REPORT ABSTRACT
Review of the Railroad Retirement Board's Security Patch Management Process

The Office of Inspector General of the Railroad Retirement Board (RRB) conducted an audit to determine whether the RRB's patch management policies, procedures and practices are in compliance with the Federal Information Security Management Act of 2002 (FISMA) requirements and if the security controls over patch management are in place and operating as intended.

FISMA requires agencies to establish and maintain a security management program that includes timely and secure installation of software patches. Patch management is a security practice designed to prevent the exploitation of information technology (IT) vulnerabilities that exist within an organization. Patches are additional pieces of code developed to address security flaws and problems in software. Timely installation of security patches is generally recognized as critical to maintaining the operational availability, confidentiality, and integrity of IT systems.

In a separately issued Restricted Distribution report, we communicated that the RRB's security patch management policies, procedures and practices comply with FISMA requirements. However, while security controls over patch management are in place, they are not fully effective or operating as intended. We made 13 detailed recommendations to RRB management for improvement in:

- procedures for the remediation of identified vulnerabilities;
- standards for timely resolution of remediation requests;
- vulnerability scanning procedures for PCs and servers;
- third-party software security updates;
- monthly server patching process;
- security patch management process performance reports;
- notification of mainframe computer updates; and
- information security policies and procedures.

Agency Management has agreed to take corrective actions for all recommendations.