U.S. Environmental Protection Agency
Office of Inspector General

16-P-0035
November 5, 2015

At a Glance

CSB Needs Better Security Controls to Protect Critical Data Stored on Its Regional Servers

Why We Did This Review

We sought to assess the U.S. Chemical Safety and Hazard Investigation Board's (CSB's) implementation of physical and environmental controls at its Western Regional Office of Investigations (WRO), and actions taken to correct prior year information security control weaknesses. The WRO is in Denver, Colorado. Implementing physical and environmental protection controls are important because they are the common controls needed to protect all information technology (IT) assets. These controls serve as the foundation for granting access to the server room and protecting the IT assets and data from harm due to unauthorized access, ineffective fire suppression and humidity control management.

This report addresses the following CSB goal:

- *Preserve the public trust by maintaining and improving organizational excellence.*

Send all inquiries to our public affairs office at (202) 566-2391 or visit www.epa.gov/oig.

Listing of OIG reports.

What We Found

CSB should strengthen physical and environmental protection controls for the WRO server room. CSB also should take steps to implement the remaining four recommendations from the prior year report to resolve security deficiencies cited.

Ineffective physical and environmental protection controls place CSB's investigative data at risk of theft, loss or damage.

Weak physical and environmental controls existed because CSB had not established and disseminated policy and procedures to WRO personnel to inform them of management's requirements for protecting the server room. CSB also had not taken steps associated with the WRO server room to establish access control rosters and physical access logs to control and monitor access. Further, CSB had not (1) implemented procedures to escort visitors, (2) secured the server room keys, (3) installed automatic fire suppression capability, and (4) monitored humidity levels.

As a result of the weaknesses noted, critical CSB network equipment and investigative data may be susceptible to theft, loss or damage.

Recommendations and Planned Agency Corrective Actions

We recommend that CSB establish and disseminate written physical and environmental protection policy and procedures, develop an authorized access roster and physical access log, periodically review and update the roster and the logs to restrict access to the server room, develop escort procedures for server room visitors, secure the server room keys and limit key access to authorized users, and equip the server room with automatic fire suppression capability to protect investigative data critical to CSB's mission.

CSB concurred with our audit recommendations and provided planned corrective actions and completion dates. Based on the CSB's response, OIG considered Recommendation 5 closed and revised Recommendation 7. We agreed with the CSB's plan of corrective actions and estimated completion dates, and consider Recommendations 1, 2, 3, 4, 6 and 7 open with corrective actions pending.

Noteworthy Achievements

In response to prior OIG audit recommendations and this year's audit, CSB took the following actions at its headquarters and WRO server rooms:
(1) implemented processes to monitor temperature levels, (2) revised the server room visitor access logs, and (3) installed software to enable automatic orderly shutdown of servers in the event of a power outage.