Results in Brief

OIG 18-08
June 20, 2018

Audit of WMATA's IT Incident Response Process

Why We Did This Review

Organizations rely on information technology (IT) to support business operations. The dependency on IT exposes organizations to compromises from fraudulent and malicious IT activities. These activities could negatively impact business operations, business continuity, financial operations and reputation. These IT related risks and exposures are commonly referred to as "computer security or IT related incidents."

Attacks on IT resources have become commonplace and increasingly sophisticated. For example, on November 25, 2016, the San Francisco Transportation Agency incurred a cyberattack that disabled critical rider systems and may have exposed thousands of employees' and customers' personal information. The cyber bandits demanded approximately $73,000.

To avoid or mitigate the damage and interruption to business services, the federal government, regulatory agencies, and IT industry leaders either require or encourage organizations to adopt and implement a formal IT incident response capability.

The audit objective was to determine the effectiveness of WMATA's IT incident response process.

What We Found

Although the Washington Metropolitan Area Transit Authority (WMATA) has taken steps toward implementing an "IT Incident" response program, the program has opportunities for improvement. These opportunities enhance WMATA's ability to detect, resolve and report IT incidents; enhance WMATA's ability to effectively apply incident escalation processes; and reduce the likelihood that IT incidents could impair WMATA's operations.

Management's Response

WMATA management agreed to the findings and recommendations made in this report and has initiated corrective actions.

NOTE: THIS REPORT CONTAINS SECURITY-RELATED INFORMATION AND IS NOT PUBLICALLY AVAILABLE.