Washington Metropolitan Area Transit Authority

Board Action/Information Summary

◉ Action ○ Information	MEAD Number: 202004	Resolution: ○ Yes ◉ No

TITLE:

Acceptance of OIG Report

PRESENTATION SUMMARY:

One OIG audit report submitted to the Business Oversight Committee for acceptance.

PURPOSE:

The Business Oversight Committee's acceptance of OIG's report entitled:

- Audit of WMATA's IT Incident Response Process

DESCRIPTION:

Key Highlights:

Situation: Attacks on IT resources have become commonplace and increasingly sophisticated.

Impact: Implementing the recommendations in this report will enhance WMATA's ability to detect,
resolve and report IT incidents that could impair WMATA's operations.

Management's Solution: To implement the recommendations.

Background and History:

Per the Bylaws of the WMATA Board of Directors, when the Business Oversight Committee determines there is no conflict remaining between the IG's findings and recommendations and management's response, it will accept the reports as final, and the reports and corrective action plans shall be deemed approved. Acceptance of the final reports constitute the Board's authorization to post the reports on the WMATA website provided the IG has conferred with the General Counsel and confirmed that any private or confidential information has been redacted in accordance with applicable law and WMATA policy.

Discussion:

The work highlighted in this report demonstrates OIG's commitment to promoting accountability, efficiency, and effectiveness in WMATA's programs and operations and keeping the Board of Directors fully and currently informed about deficiencies in WMATA's activities, as well as the necessity for and progress of corrective actions.

There were no conflicts between the IG's findings and recommendations listed in this report and management's response. The IG has conferred with the General Counsel and confirmed that any private or confidential information has been removed/redacted in accordance with applicable law and WMATA policy.

FUNDING IMPACT:

There is no impact on funding.

TIMELINE:

Anticipated action after presentation: Business Oversight Committee's acceptance of OIG's report.

RECOMMENDATION:

Business Oversight Committee accept OIG's report.

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 common place and have become 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.