Results in Brief

OIG 19-02
September 5, 2018

Why We Did This Review

Web applications have become indispensable to both public and commercial enterprises and a key strategic component in customer acquisition and service. Web applications allow an organization to publish information, interact with Internet users, and establish an e-commerce or e-government presence.

WMATA manages 17 publicly accessible web applications to share information with stakeholders and the public. WMATA's publicly accessible web applications include 24 web-based login portals and remote access systems. Two of the best-known web applications are the Metrobus Schedule and the SmarTrip.

Recent media reports highlight increases in velocity and cost of cyber-attacks and data breaches. For example, Equifax breach of 143 million consumers' sensitive information, and per Verizon, web applications represented 35 percent of breaches in 2014.

WMATA is a target of cyber-attacks. For example, WMATA had a breach in 2012 and identified other cyber-attacks, which were remediated.

The audit objective was to determine the effectiveness of WMATA's security controls over publicly accessible web applications.

Audit of WMATA's Security Over Publicly Accessible Web Applications

What We Found

WMATA has developed various security controls to protect highly sensitive information. However, opportunities exist to further strengthen security over publicly accessible web applications thereby reducing the likelihood of data breaches. Without strong security controls, WMATA's publicly accessible web applications are vulnerable to cyberattacks and data breaches which could have detrimental impact on WMATA's mission, operations, and critical infrastructure.

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 PUBLICLY AVAILABLE