

Addressing IT Network Vulnerabilities

Scope Statement – August 1, 2018

Background

Cyberattacks, service disruptions, and hacked confidential information are frequently reported in the news. All organizations are vulnerable to attacks. Experts warn it is not “if” an organization will be attacked, but “when” it will be attacked. Successful cyberattacks cause real economic damage to organizations, damage that can take months or years to resolve. According to respondents to the Cisco 2018 Security Capabilities Benchmark Study, more than half of all attacks resulted in financial damage of \$500,000 to over \$5,000,000. The recent ransomware attack on the city of Atlanta shut down city systems and computers and severely limited Atlanta government’s ability to function. It cost over \$5 million to restore files and rebuild systems, and an additional \$9.5 million was requested to pay for recovery costs in the next fiscal year’s budget.

The Information Technology Division (ITD) of the General Services Department is responsible for providing secure technology infrastructure. The division uses multiple methods to protect the city’s information technology systems, including the identification and repair of network vulnerabilities.

Why audit how ITD addresses network vulnerabilities?

Information technology systems are critical city infrastructure. The city is obligated to protect the system from cybersecurity risks which can cause service disruption, damage to the city’s reputation, and loss of public trust, in addition to financial cost. Identifying and addressing vulnerabilities in the IT network are important components of safeguarding the city’s IT infrastructure from cyberattacks.

Audit objective

Our objective is to answer the following question:

- Is the Information Technology Division addressing identified network vulnerabilities appropriately?

Audit methods

We will review recommended practices, city policy and procedures for detecting and addressing network vulnerabilities, related department reports, and professional literature. We will also interview city staff.

Anticipated release date

We plan to issue the audit report in October 2018.