

**TECHNOLOGY AND INNOVATION  
SECURITY OFFICE  
VULNERABILITY ASSESSMENTS  
AUDIT 15-16  
JANUARY 28, 2016**



# CITY OF TAMPA

Bob Buckhorn, Mayor

Internal Audit Department

Christine Glover, Internal Audit Director

January 28, 2016

Honorable Bob Buckhorn  
Mayor, City of Tampa  
1 City Hall Plaza  
Tampa, Florida

RE: Vulnerability Assessments, Audit 15-16

Dear Mayor Buckhorn:

Attached is the Internal Audit Department's report on 15-16 Vulnerability Assessments.

We thank the management and staff of the Technology and Innovation Security Office for their cooperation and assistance during this audit.

Sincerely,

/s/ Christine Glover

Christine Glover  
Internal Audit Director

cc: Dennis Rogero, Chief of Staff  
Sonya Little, Chief Financial Officer  
Russell Harper, Director of Technology and Innovation  
Martin Zinaich, Information Security Officer

**TECHNOLOGY AND INNOVATION  
SECURITY OFFICE  
VULNERABILITY ASSESSMENTS  
AUDIT 15-16  
JANUARY 28, 2016**

/s/ Melinda Jenzarli

---

Melinda Jenzarli, Auditor

/s/ Christine Glover

---

Christine Glover, Audit Director

**TECHNOLOGY AND INNOVATION  
SECURITY OFFICE  
VULNERABILITY ASSESSMENTS  
AUDIT 15-16**

**BACKGROUND**

The City of Tampa Technology and Innovation Security Office (TISO) is committed to ensure the continuation of network and security services to the City of Tampa, its staff and citizens. In order to manage and reduce risk to the City network infrastructure, the Security Office utilizes Vulnerability Management tools to:

- Identify newly discovered assets on the network.
- Prioritize assets with the most critical and/or highest number of vulnerabilities.
- Proactively identify high risk assets and remediate vulnerabilities by working with system owners.<sup>1</sup>

TISO's primary focus is to address vulnerabilities that are identified on external or internet facing internet protocol (IP) addresses, as these pose the greatest risk. The internet facing IP addresses are also required to be scanned by an independent Approved Scanning Vendor (ASV) to meet the Payment Card Industry (PCI) Data Security Standard (DSS). Compliance with this standard is required by *entities involved in payment card processing, and that store, process or transmit cardholder data*. Specifically, 11.2 require these entities to *run internal and external network vulnerability scans, at least, quarterly, and after any significant change in the network*. Internal scans can be performed by a qualified staff of the organization. External scans must be performed by an independent ASV. Rescans should be performed until the passing scan is achieved. Rapid7, Inc. is currently the City of Tampa independent ASV for PCI compliance.

When a vulnerability is identified on the internal network that presents a high business risk, TISO creates a remediation plan, and works it with the system owner (this is generally the administrator for the system, which could be a Technology and Innovation team or a vendor). TISO is instrumental in facilitating this corrective process, and validating that the vulnerabilities creating the highest risk to the business are remediated.

**STATEMENT OF OBJECTIVES**

This audit was conducted in accordance with the Internal Audit Department's FY2015 Audit Agenda. The objective of this audit was to ensure the process by which TISO logs and remediates vulnerabilities, identified by the ASV, is adequate.

**STATEMENT OF SCOPE**

We have conducted an audit of vulnerability assessments performed by TISO. The audit included a review of the October 7, 2015, scan report conducted by Rapid7, Inc.

---

<sup>1</sup> Network Vulnerability Management Policy # PL-10.9.1

### **STATEMENT OF METHODOLOGY**

The scan report conducted by Rapid7, Inc. on October 7, 2015, was reviewed, and IP addresses that received a fail for PCI compliance were documented. Tests were performed to verify that TISO logged the failed IP addresses for remediation. The scan report conducted by Rapid7, Inc. on November 30, 2015, was reviewed to verify that the failed IP addresses had been remediated, or were in the process of being remediated.

### **STATEMENT OF AUDITING STANDARDS**

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

### **AUDIT CONCLUSIONS**

Based upon the test work performed, we conclude that the process by which TISO logs and remediates vulnerabilities, identified by the ASV, is adequate.