

THOMAS P. DINAPOLI
STATE COMPTROLLER



110 STATE STREET
ALBANY, NEW YORK 12236

STATE OF NEW YORK
OFFICE OF THE STATE COMPTROLLER

January 19, 2021

Sister Denise A. Roche
Chair
Niagara Frontier Transportation Authority
181 Ellicott Street
Buffalo, NY 14203

Re: Use of Vendor-Supported Technology
Report 2020-F-28

Dear Sister Denise:

Pursuant to the State Comptroller's authority as set forth in Article X, Section 5 of the State Constitution and Section 2803 of the Public Authorities Law, we have followed up on the actions taken by officials of the Niagara Frontier Transportation Authority to implement the recommendations contained in our audit report, *Use of Vendor-Supported Technology* (Report [2019-S-40](#)) issued December 12, 2019.

Background, Scope, and Objective

Niagara Frontier Transportation Authority (NFTA) is a New York State public benefit corporation responsible for the oversight of public transportation in Erie and Niagara counties, including the NFTA Metro Bus and Rail System, the Buffalo-Niagara International Airport, and Niagara Falls International Airport. NFTA has approximately 1,500 employees, including an information technology (IT) department that operates out of its main office. To help support its mission, NFTA owns IT resources, including approximately 546 desktops/workstations and 250 servers that support 30 databases.

As a public benefit corporation, NFTA must adhere to the New York State Information Technology Security Policy (Policy) established by the New York State Office of Information Technology Services. The Policy defines the minimum information security requirements that all state agencies (including all public benefit corporations) must follow to secure and protect the confidentiality, integrity, and availability of information. This includes requirements for ensuring systems are up to date and maintained at vendor-supported levels (i.e., systems continue to be updated by the system's vendor).

Our initial audit report, covering the period June 24, 2019 through August 29, 2019, examined whether NFTA was complying with requirements to maintain its systems at vendor-supported levels. We evaluated selected systems and determined that, generally, NFTA maintained its systems at vendor-supported levels. However, we identified unsupported systems used by NFTA on 66 devices. We found that NFTA officials did not develop policies and procedures to ensure that their systems were regularly reviewed and kept up to date, nor did they maintain a single clear inventory of IT assets to aid in tracking their systems. NFTA officials

indicated they were in the process of or had plans to upgrade certain systems identified as no longer supported by the vendors. We recommended NFTA officials ensure those actions and plans were completed and find solutions for systems that remained unaddressed. Generally, NFTA officials agreed with our recommendations and indicated they would take actions to implement them.

The objective of our follow-up was to assess the extent of implementation, as of October 15, 2020, of the two recommendations included in our initial audit report.

Summary Conclusions and Status of Audit Recommendations

NFTA officials have made significant progress in addressing the problems we identified in the initial audit. Both recommendations have been implemented.

Follow-Up Observations

Recommendation 1

Take steps to ensure that systems are maintained at vendor-supported levels such as developing policies and procedures related to software updates and vulnerability analysis.

Status – Implemented

Agency Action – NFTA officials have developed policies and procedures to help ensure systems are maintained at vendor-supported levels. NFTA developed a policy for the patch management of all NFTA- and Metro Bus and Rail System-owned systems, including all third-party entities that house, store, or process NFTA data. The policy dictates that, effective June 15, 2020, the patch updates be prioritized based on the severity of the vulnerability that the patch addresses. When patches cannot be completed within the timeline outlined in the policy, compensating controls must be put in place. Further, NFTA developed a policy mandating that, in order to be connected to a NFTA network, all software and hardware must be maintained at a vendor-supported level. Upgrades must be completed at least annually to ensure systems are kept current and support all current operating systems and hardware patches. Software and hardware that is approaching end of life must have a transition plan for its replacement or decommissioning at least one year before the end of life. Software and hardware that has reached end of life must be removed in a timely manner. If this software and/or hardware is needed for business operations, then the potential security threats must be evaluated and proper controls must be put in place.

Recommendation 2

Implement the remaining recommendations detailed in the preliminary report.

Status – Implemented

Agency Action – During our initial audit, we issued a preliminary report detailing the status of the unsupported systems and other controls in place. NFTA officials have taken steps to address the recommendations detailed in the preliminary report.

Major contributors to this report were Jessica Kirk, Christopher Bott, Melissa Davie, Molly Kramm, and Brendan Reilly.

We thank the management and staff of the Niagara Frontier Transportation Authority for the courtesies and cooperation extended to our auditors during this review.

Very truly yours,

Cynthia Herubin, CIA, CGAP
Audit Manager

cc: Patrick Dalton, Director of Internal Audit and Corporate Compliance