THOMAS P. DiNAPOLI
COMPTROLLER

110 STATE STREET
ALBANY, NEW YORK 12236

STATE OF NEW YORK
OFFICE OF THE STATE COMPTROLLER

July 29, 2019

Mr. Geoffrey Astles
Chairman
Rochester-Genesee Regional Transportation Authority
1372 East Main Street
Rochester, NY 14609

Re: Compliance With Requirements to Maintain Systems at Vendor-Supported Levels
Report 2019-S-6

Dear Chairman Astles:

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 conducted an audit of Rochester-Genesee Regional Transportation Authority's (RGRTA) compliance with requirements to maintain its systems at vendor-supported levels.

Background

RGRTA is a regional transportation authority established by New York State to provide safe, reliable, and convenient public transportation to customers in eight counties (Monroe, Genesee, Livingston, Ontario, Orleans, Seneca, Wayne, and Wyoming). RGRTA has more than 900 employees, including an information technology (IT) department that operates out of its main office. RGRTA owns IT resources, including desktops/workstations, servers, and databases used to help carry out its mission.

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

Audit Results

According to the Policy, State entities, including public benefit corporations like RGRTA, are required to maintain systems at a vendor-supported level to ensure

the accuracy and integrity of information. The Policy defines systems as including, but not limited to, servers, platforms, networks, communications, databases, and software applications. We determined that, generally, RGRTA maintained its systems at vendor-supported levels. However, we did identify unsupported systems used by RGRTA on 14 devices. The systems on 6 of the 14 devices (43 percent) were the responsibility of third-party vendors. In these cases, we determined that RGRTA was not providing sufficient oversight of those vendors to ensure they were meeting their obligations to keep systems up to date. Instead, RGRTA generally relied on the vendors to fulfill requirements in maintenance plans or service agreements related to keeping systems up to date. In another circumstance, RGRTA officials stated a system could not be updated to the vendor-supported level in a cost-effective way without affecting the functionality of a particular application. We also found that RGRTA officials have not developed policies and procedures to ensure that its systems are regularly reviewed and kept up to date.

Due to their confidential nature, we communicated the details of the unsupported systems we identified to RGRTA officials in a separate report and do not address those details in this report. Generally, RGRTA officials agreed with our recommendations and indicated they will take actions to implement them.

Recommendations

1. Take steps to ensure that systems are maintained at vendor-supported levels, including:

    - Developing policies and procedures related to software updates and vulnerability analysis.
    - Monitoring vendors to ensure they are keeping the systems they are responsible for up to date.

2. Implement the remaining recommendation detailed in the preliminary report.

Audit Scope, Objective, and Methodology

Our audit determined whether RGRTA was complying with requirements to maintain its systems at vendor-supported levels. The audit covered the period January 1, 2019 through April 3, 2019.

To accomplish our objective and assess related internal controls, we reviewed applicable NYS ITS policies and met with RGRTA officials to understand their management of IT resources. We performed scans of the RGRTA network and compared the results with an inventory of systems provided by RGRTA. We compared the RGRTA systems identified with the last supported date for those systems and followed up with RGRTA officials to determine the reasons for the outdated systems and the actions planned to address those systems.

We conducted our 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

In addition to being the State Auditor, the Comptroller performs certain other constitutionally and statutorily mandated duties as the chief fiscal officer of New York State. These include operating the State's accounting system; preparing the State's financial statements; and approving State contracts, refunds, and other payments. In addition, the Comptroller appoints members to certain boards, commissions, and public authorities, some of whom have minority voting rights. These duties may be considered management functions for purposes of evaluating organizational independence under generally accepted government auditing standards. In our opinion, these functions do not affect our ability to conduct independent audits of program performance.

Reporting Requirements

We provided a draft copy of this report to RGRTA officials for their review and formal comment. We considered their comments in preparing this final report and have included them in their entirety at the end of it. In their response, RGRTA officials stated they found no material discrepancies with the report or its findings. In addition, they indicated they have started to take actions to address the recommendations contained in the report. Our response to RGRTA comments are included in the report's State Comptroller's Comment.

Major contributors to this report were Nadine Morrell, Brian Krawiecki, Holly Thornton, Renee Boel, and Christopher Bott.

We would like to thank RGRTA management and staff for the courtesies and cooperation extended to our auditors during this audit.

Sincerely,

Brian Reilly, CFE, CGFM
Audit Director

cc: Bill Carpenter, Chief Executive Officer
Scott Adair, Chief Financial Officer

Agency Comments

myRTS.com

July 17, 2019

Mr. Brian Reilly
Office of the State Comptroller
State Government Accountability
110 State Street
Albany, NY 12236

Re: Audit Report 2019-S-6

Dear Mr Reilly:

Thank you for providing Report 2019-S-6 on Compliance with requirements to maintain systems at Vendor-supported levels. Rochester Genesee Regional Transportation Authority (RGRTA) finds no material discrepancies contained within the report or its findings.

RGRTA does request that the final report contain a clarification on page 2 under the 'Audit Results' section as it pertains to the total number of systems. The statement does not reference the 815 systems and assets, which were reviewed. The statement as written today provides a picture that 43% of the devices are unsupported when in reality that number is less than 2% of RGRTA's systems. We believe that referencing the total systems provides appropriate magnitude to the issue that is being reported on.

* Comment 1

The recommendations included in your report and the Authority's responses are noted below:

1. *Develop policies and procedures related to software updates and vulnerability analysis.*

   RGRTA is working through this recommendation to ensure that the appropriate policies and procedures are implemented.

2. *Monitoring vendors to ensure they are keeping the systems they are responsible for up to date.*

   RGRTA has already begun to take action on this recommendation to provide resolution to adhere to New York State Information Security Policies.

Regional Transit Service 1372 East Main Street, Rochester, NY 14609 • P: 585-654-0200 • F: 585-654-0293

The Authority notes the efforts of the individual contributors to this report from the State Comptroller's Office. The Authority, as always, will continue to be a responsible financial steward in protection of our assets.

Sincerely,

Scott M. Adair, CPA
Chief Financial Officer

Cc:
Geoff Astles, *Board Chairman*
Mike Jankowski, *Audit Committee Chairman*
Bill Carpenter, *Chief Executive Officer*

State Comptroller's Comment

1. The Audit Results section is clear as written. The report does not claim 43 percent of RGRTA devices are unsupported. Rather, it states we identified 14 devices with unsupported systems. The 43 percent simply refers to the percentage of those 14 devices with unsupported systems that were the responsibility of third-party vendors.