

THOMAS P. DiNAPOLI  
STATE COMPTROLLER



110 STATE STREET  
ALBANY, NEW YORK 12236

STATE OF NEW YORK  
OFFICE OF THE STATE COMPTROLLER

February 25, 2026

Jayne Lahut  
Chairman  
Capital District Transportation Authority  
110 Watervliet Avenue  
Albany, NY 12206

Re: Access Controls and Vulnerability  
Management  
Report 2025-S-3

Dear Mr. Lahut:

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 conducted an audit of the Capital District Transportation Authority (CDTA) to determine whether its access controls and vulnerability management over critical systems are sufficient to minimize the various risks associated with unauthorized access to systems and data.

**Background**

CDTA was created by the New York State Legislature in 1970 to provide transportation services to the Capital Region and is the primary transportation provider in the area, providing multiple bus services, shuttle systems, and paratransit services (for riders with disabilities) across Albany, Montgomery, Rensselaer, Saratoga, Schenectady, and Warren counties. Additionally, CDTA subsidiaries own and operate the Rensselaer Rail and Saratoga Springs train stations and the Northway Xpress (NX) commuter service between Saratoga County and downtown Albany. CDTA also operates the regional bike-share program, CDPHP Cycle, and a carshare program, DRIVE. CDTA had an approximate workforce of 806 employees in 2025.

CDTA's mission is to provide mobility solutions that connect the region's communities by increasing transit ridership and revenue, improving the transportation network, retaining a high-quality workforce, and identifying appropriate funding sources. Its vision is to be a growing and vibrant company that seeks to continually increase ridership and the use of its facilities by providing services that people want and need.

CDTA is governed by a board of directors. The Chief Operating Officer oversees technical services and information systems, including activities to protect CDTA's electronic information assets, information systems, and services. To safeguard against unauthorized access, CDTA adheres to key requirements and guidelines, including Payment Card Industry Data Security Standards (PCI-DSS), National Institute of Standards and Technology (NIST) standards, and its internal policies and standards.

## **Results of Audit**

We identified areas where CDTA could improve certain security controls to minimize the various risks associated with unauthorized access to its systems and data. Due to the confidential nature of our findings, we communicated the details of these findings along with the recommendation in a separate, confidential report to CDTA officials for their review and comment. CDTA officials generally agreed with our findings and indicated actions to implement our recommendation.

## **Recommendation**

1. Implement the recommendation included in our confidential preliminary report.

## **Audit Objective, Scope, and Methodology**

The objective of the audit was to determine whether CDTA's access controls and vulnerability management over critical systems are sufficient to minimize the various risks associated with unauthorized access to systems and data. The audit covered the period from January 2024 through November 2025.

To accomplish our objective and assess related internal controls, we conducted interviews with CDTA officials to gain insight into their roles and responsibilities, as well as the measures they have implemented for identity and access management and vulnerability management concerning critical systems. We used a non-statistical sampling approach to provide conclusions on our audit objective and to test internal controls and compliance. We obtained and analyzed an application inventory of CDTA's IT systems and selected a judgmental sample based on the criticality of the business function. However, because we used a non-statistical sampling approach for our tests, we cannot project the results to the respective populations. Additionally, we examined the security features of these critical systems and reviewed information to identify any vulnerabilities related to security, processing integrity, confidentiality, and privacy.

We obtained user and vulnerability data from CDTA, which we used to perform user access testing and vulnerability remediation, and provide background information. We observed the user listings generated from the in-scope applications, as well as from Active Directory without any omitting parameters or filters. We also observed the vulnerability data within CDTA's vulnerability management tool, confirming that we obtained the full population from our audit period. Data we used was obtained from the best available source. We have determined that the data obtained is reliable for the purposes of this report.

## **Statutory Requirements**

### ***Authority***

The audit was performed 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 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, including some duties on behalf of public authorities. For CDTA, these include reporting CDTA as a discrete component unit in the State's financial statements and approving selected contracts. These duties could be considered management functions for the purposes of evaluating organizational independence under generally accepted government auditing standards. In our professional judgment, these duties do not affect our ability to conduct this independent performance audit of CDTA's oversight and administration of security over critical systems.

### ***Reporting Requirements***

We provided a draft copy of this report to CDTA officials for their review and formal comment. We considered their comments in preparing this final report and have included their response in its entirety at the end of it. In their response, CDTA officials agreed with our audit conclusions and recommendation.

Within 180 days after final release of this report, as required by Section 170 of the Executive Law, the Chairman of the Capital District Transportation Authority shall report to the Governor, the State Comptroller, and the leaders of the Legislature and fiscal committees, advising what steps were taken to implement the recommendations contained herein, and where recommendations were not implemented, the reasons why.

Major contributors to this report were Amanda Eveleth, Justin Dasenbrock, Christopher Bott, Logan Frese, and Cosmos Houndonougbo.

We wish to thank the management and staff of the Capital District Transportation Authority for the courtesy and cooperation extended to our auditors during this audit.

Very truly yours,

Nadine Morrell, CIA, CISM  
Audit Director

cc: Chris Desany, Capital District Transportation Authority  
Thomas Guggisberg, Capital District Transportation Authority  
Rich Fantozzi, Capital District Transportation Authority  
Sarah Matrose, Capital District Transportation Authority

# Agency Comments and State Comptroller's Comment



January 20, 2026

Nadine Morrell, CIA, CISM  
Audit Director  
Office of the State Comptroller  
State Government Accountability  
110 State Street  
Albany, NY 12236

**Christopher G. Desany**  
Chief Operating Officer  
O: 518.437.8320  
C: 518.479-1060  
chrisd@cdta.org

Dear Nadine Morrell:

On behalf of the Capital District Transportation Authority (CDTA), thank you for the opportunity to review and respond to the draft audit report concerning access controls and vulnerability management over our critical systems. We appreciate the work and professionalism of your audit team, as well as the collaborative approach taken throughout this review.

We are pleased that the audit recognized our commitment to safeguarding CDTA's electronic information assets and our adherence to industry standards and internal policies. We acknowledge the areas identified for improvement and appreciate the clear recommendations provided in the confidential preliminary report.

Overall, CDTA concurs with the findings and recommendations and has already begun taking steps to implement the two recommendations outlined in the confidential report. We remain committed to strengthening our security posture and ensuring that our systems and data are protected against unauthorized access.

**State Comptroller's Comment** – The two recommendations contained in the confidential report were summarized to just one recommendation.

We would also like to express our sincere appreciation for the courtesy, cooperation, and open communication extended by your audit staff during the course of this review. Their constructive and collaborative approach greatly supported our shared goal of continuous improvement.

We have provided this formal written response within the 30-day timeframe requested.

Thank you again for your guidance and partnership.

Sincerely,

Christopher Desany  
Chief Operating Officer

Cc: Sarah Matrose, CDTA Internal Auditor  
Thomas Guggisberg, CDTA Director of Information Technology  
Rich Fantozzi, CDTA Software Architect

**Jayne B. Lahut**  
Chairman  
Schenectady County

**Michael J. Criscione**  
Vice Chairman  
Albany County

**Denise A. Figueroa**  
Treasurer  
Albany County

**Georgeanna M. Nugent**  
Secretary  
Saratoga County

**David M. Stackrow**  
Rensselaer County

**Jackie McDonough**  
Rensselaer County

**Jaclyn Falotico**  
Schenectady County

**Peter D. Wohl**  
Saratoga County

**Patrick M. Lance**  
Labor Representative

**Frank Annicaro**  
Chief Executive Officer