Thomas P. DiNapoli
State Comptroller

110 State Street
Albany, New York 12236

STATE OF NEW YORK
OFFICE OF THE STATE COMPTROLLER

October 9, 2024

Dru Rai
Chief Information Officer
Office of Information Technology Services
Empire State Plaza
P.O. Box 2062
Albany, NY 12220

Re: Windows Domain Administration and Management
Report 2024-F-12

Dear Mr. Rai:

Pursuant to the State Comptroller's authority as set forth in Article V, Section 1 of the State Constitution and Article II, Section 8 of the State Finance Law, we have followed up on the actions taken by officials of the Office of Information Technology Services (ITS) to implement the recommendations contained in our initial audit report, *Windows Domain Administration and Management* (Report 2022-S-19).

Background, Scope, and Objective

ITS provides statewide IT strategic direction, directs IT policy, and delivers centralized IT products and services that support the mission of the State. ITS operates data centers 24 hours a day, 365 days a year to support statewide mission-critical applications for 53 agencies, encompassing over 16 million public accounts, 130,000 employee accounts, 63,000 VoIP phones and 37,000 mobile phones, 100,000 workstations/laptops/tablets, 16,000 virtual and real servers, 33 petabytes of storage, and 35,000 Virtual Desktop remote connections. ITS provides State agencies secure networking and desktop support for more than 38,000 workstations on 1,600 miles of fiber.

As part of its services, ITS is responsible for maintaining Active Directory domains on behalf of the State's Executive agencies. A domain is a group of interconnected devices, such as computers and servers, as well as users, groups, and systems. An Active Directory domain provides the methods for storing directory data and making this data available to network users and administrators. Each Active Directory uses servers, referred to as domain controllers, to manage the access and authentication of stored user credentials determining who can access file servers and other network resources. Since Active Directory and associated domain controllers ultimately control access and authorization in a Microsoft Windows environment, it is vital to ensure that appropriate controls are in place and that policies and standards are being adhered to.

ITS' Information Security Policy NYS-P03-002 (Security Policy) defines the mandatory minimum information security requirements for all State entities. The Security Policy defines a framework that will ensure appropriate measures are in place to protect the confidentiality, integrity, and availability of information assets, and ensure staff and all other affiliates understand their role and responsibilities; have adequate knowledge of security policies, procedures, and practices; and know how to protect State entity information. The Security Policy encompasses all systems, automated and manual, for which New York State has administrative responsibility. It addresses all information regardless of the form or format that is created or used to support the business activities of State entities. The Security Policy acts as an umbrella document to all other ITS security policies and associated standards.

The objective of our audit, issued May 31, 2023, was to determine whether ITS had security controls in place to ensure appropriate management and monitoring of its Active Directory environment. The audit covered the period from January 2021 through March 2023. Generally, we determined ITS did not have certain security controls in place, according to several ITS policies and standards, to ensure appropriate management and monitoring of its Active Directory environment.

Due to the confidential nature of our audit findings, our public report contained one recommendation: to implement the six recommendations included in a confidential draft report provided to ITS officials. ITS officials generally agreed with our findings and recommendations communicated in the confidential report, and, in several instances, indicated they were planning actions to address them. The objective of our follow-up was to assess the extent of implementation, as of September 2024, of the recommendation included in our initial audit report.

Summary Conclusions and Status of Audit Recommendation

ITS officials made progress in addressing the problems we identified in the initial audit report. The initial report's recommendation has been partially implemented.

Follow-Up Observations

Recommendation 1

Implement the six recommendations included in our confidential draft report.

Status – Partially Implemented

Agency Action – Since our initial audit, ITS officials have made progress toward implementing the six recommendations in our confidential report. Of the confidential report's six audit recommendations, three were implemented, two were partially implemented, and one was not implemented.

Major contributors to this report were Justin Dasenbrock, Christopher Bott, Misty Baldeo, and Stephen Kurtis.

ITS officials are requested, but not required, to provide information about any actions planned to address the unresolved issues discussed in this follow-up within 30 days of the report's issuance. We thank the management and staff of ITS for the courtesies and cooperation extended to our auditors during this follow-up.

Very truly yours,

Amanda Eveleth
Audit Manager

cc: Michelle Jones, Office of Information Technology Services