THOMAS P. DINAPOLI
STATE COMPTROLLER

110 STATE STREET
ALBANY, NEW YORK 12236

STATE OF NEW YORK
OFFICE OF THE STATE COMPTROLLER

May 31, 2023

Jennifer Lorenz
Acting 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 2022-S-19

Dear Ms. Lorenz:

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 conducted an audit of the Office of Information Technology Services (ITS) to determine whether the agency has security controls in place to ensure appropriate management and monitoring of its Active Directory environment. The audit covered the period of January 2021 through March 2023.

Background

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.

Results of Audit

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, we communicated the details of these findings with six recommendations in a separate, confidential report to ITS officials for their review and comment. ITS officials generally agreed with our findings and recommendations and in several instances indicated they were planning actions to address them.

Recommendation

1. Implement the six recommendations included in our confidential draft report.

Audit Scope, Objective, and Methodology

The objective of our audit was to determine whether ITS has security controls in place to ensure appropriate management and monitoring of its Active Directory environment. The audit covered the period of January 2021 through March 2023.

To accomplish our objective and assess related internal controls, we reviewed relevant ITS system security policies applicable to State agencies and industry standards issued by the National Institute of Standards and Technology related to the administration and monitoring of the Active Directory environment. We met with ITS personnel to gain an understanding of their processes for securing the Active Directory environment. We performed walk-throughs via WebEx to observe certain system controls and reviewed documentation, such as screenshots of system settings, to verify controls were in place. Further, we selected judgmental samples of certain records to assess ITS compliance with selected portions of ITS standards. Due to their confidential nature, we do not discuss those records and judgments in this public report. However, those record and judgments are documented in our working papers and are described in the private report to ITS officials. Our sample results only applied to the sampled items and we cannot project the results of our samples in our audit. We determined that the data used to pull our samples and perform our analysis was sufficiently reliable for accomplishing our audit objective.

Statutory Requirements

Authority

This audit was performed 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 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. These duties could be considered management functions for 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 ITS' oversight and administration of its Active Directory environment.

Reporting Requirements

We provided a draft copy of this report, along with a confidential report detailing our audit findings, to ITS officials for their review and formal comment. We considered their comments in preparing this final report and have included their response to our public report in its entirety at the end of it. In their response, ITS officials generally agreed with our audit conclusions and recommendations and indicated that actions have been and will be taken to address them.

Within 180 days after the final release of this report, as required by Section 170 of the Executive Law, the Chief Information Officer of the Office of Information Technology Services 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 the recommendations were not implemented, the reasons why.

Major contributors to this report were Cynthia Herubin, CIA, CGAP; Brian Krawiecki, CIA; Justin Dasenbrock, CISA, ITIL; Andrew Davis; and Jason Getman, CPA, CISA, CCSK.

We wish to thank the management and staff of the Office of Information Technology Services for the courtesies and cooperation extended to our auditors during this audit.

Very truly yours,

Nadine Morrell, CIA, CISM
Audit Director

cc: John Futia, Office of Information Technology Services

Agency Comments

NEW YORK STATE OF OPPORTUNITY. | Office of Information Technology Services

KATHY HOCHUL
Governor

JENNIFER LORENZ
Acting NYS Chief Information Officer

May 8th, 2023

Dear Ms. Morrell,

Please find enclosed the NYS Office of Information Technology Services response to the Office of State Comptroller's Draft Report on the Windows Domain Administration and Management Audit. Thank you.

Sincerely,

Jennifer Lorenz

Jennifer Lorenz

NEW YORK STATE OF OPPORTUNITY. | Office of Information Technology Services

KATHY HOCHUL
Governor

JENNIFER LORENZ
Acting NYS Chief Information Officer

To: Nadine Morrell, CIA, CISM, NYS Office of the State Comptroller
From: Jennifer Lorenz
Date: May 5, 2023
Subject: OSC AD Audit Draft Report Recommendations and ITS Reponses (Public Report)

OSC AD Audit Draft Report Recommendations and ITS Reponses (Public Report)

1. **ITS Response to the Draft Report Recommendation** –

   Where applicable, ITS has identified a plan to address the findings and separately communicated the response to OSC.

Jennifer Lorenz
Acting NYS Chief Information Officer