Thomas P. DiNapoli
State Comptroller

110 State Street
Albany, New York 12236

STATE OF NEW YORK
OFFICE OF THE STATE COMPTROLLER

August 27, 2025

Andrew Davis
Chief Operating Officer
Erie County Medical Center Corporation
462 Grider Street
Buffalo, NY 14215

Re: Security Over Critical Systems
Report 2023-S-48

Dear Mr. Davis:

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 Erie County Medical Center Corporation to determine whether the security over its critical systems is sufficient to minimize the various risks associated with unauthorized access to systems and data.

Background

Erie County Medical Center Corporation (ECMCC) is a leading health care provider and academic medical center in Western New York, with 573 inpatient beds. It specializes in various services, including oncology, transplantation, behavioral health, primary care, and more than 30 outpatient specialty services. ECMCC is recognized as a verified Level 1 Adult Trauma Center and serves as a regional hub for burn care and rehabilitation. As a teaching facility affiliated with the University at Buffalo, it plays a vital role in medical research. A core value of the organization is privacy, which involves respecting everyone's right to confidentiality.

ECMCC is governed by a board of directors. The Chief Information Officer (CIO) oversees technical services and information systems. The IT Security Committee at ECMCC includes the CIO, Chief Operating Officer (COO), Chief Financial Officer, Risk Officer, and Compliance Officer. The Healthcare Information Security Officer (HISO) oversees the daily management of the Information Security Program and is responsible for developing and implementing its long-term strategy. The authority of the HISO, which is derived from both the COO and the CIO, includes conducting necessary activities to protect ECMCC's electronic information assets, information systems, and services.

HISO conducts a Business Impact Analysis to evaluate the importance of its applications and data. In 2024, HISO identified eight critical systems and 24 essential applications that are vital for its core operations. These critical systems include MEDITECH Client Server, PACS, Dentrix, and Active Directory. The key applications consist of electronic medical records for both primary and outpatient care, employee location tracking, imaging systems, medication, and dosage platforms as well as various databases and laboratory services.

ECMCC's IT Security Architecture emphasizes key principles such as the least privilege, data classification, and separation of duties. Additionally, the IT security framework covers essential aspects like physical security, wireless network protection, and contingency planning. Contingency planning involves crucial elements, such as data backups, emergency operations, disaster recovery, and business continuity, to ensure a robust response to potential incidents. To protect against unauthorized access to systems and data, ECMCC adheres to important laws and guidelines, including Health Insurance Portability and Accountability Act (HIPAA), Federal Information System Controls Audit Manual (FISCAM), National Institute of Standards and Technology (NIST) standards, and its internal policies.

Results of Audit

We identified areas where ECMCC could improve certain security controls in place to minimize the various risks associated with unauthorized access to its systems and data. Due to the confidential nature of our audit findings, we communicated the details of these findings with eight recommendations in a separate, confidential report to ECMCC officials for their review and comment. ECMCC officials generally agreed with our findings and recommendations and in several instances indicated they were planning actions to address them.

Recommendation

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

Audit Scope, Objective, and Methodology

The objective of our audit was to determine whether the security over ECMCC's critical systems is sufficient to minimize the various risks associated with unauthorized access to systems and data. The audit period covered the period from December 2023 to December 2024.

To accomplish our objective and assess related internal controls, we interviewed ECMCC officials and subject matter experts in the relevant areas of the Human Resources department to understand the responsibilities and controls they have in place for on-boarding, transferring, and off-boarding employees; the CyberArk management team to identify how ECMCC manages privileged user accounts and daily user accounts; and the Information Security Resiliency team to comprehend backup-recovery, business impact analysis, and disaster recovery exercises and know roles and responsibilities, standards, and guidelines applied for recovery from IT disruptions. The audit team used certain tools on site to document any weak or unsecured networks and confirm whether ECMCC's internal networks are secure. We visited the data center to ensure physical and environmental controls were in place. Further, we utilized our IT testing lab to analyze firewall rules. The audit team analyzed ECMCC's written internal policies and procedures in identity and access management, disaster recovery and business continuity planning, vulnerability remediation procedures, physical access controls to data centers, and firewall rules. We compared ECMCC's internal policies with HIPAA and NIST guidelines to identify gaps between internal policies and best practices. Additionally, we examined reports generated by third parties for ECMCC on risk assessment, vulnerability identification, and penetration testing.

We used a non-statistical sampling approach to provide conclusions on our audit objective and to test internal controls and compliance. We selected various judgmental samples to test whether ECMCC was taking appropriate steps to prevent unauthorized access,

including providing appropriate levels of access to systems, terminating access timely, patching applications to address security vulnerabilities, and properly configuring systems. We provided details about the specific samples selected and the results of our work to ECMCC.

We obtained an Employee Listing from UKG (ECMCC's payroll/HR system) and assessed the reliability of that data by reviewing existing information, interviewing officials knowledgeable about the system, and tracing to and from source data. We were not able to assess the completeness of UKG data and so could not determine its reliability. However, it is the only data available to us for certain audit tests and was used for those tests.

Additionally, we relied on data about user accounts obtained from the Active Directory, which is recognized as an appropriate source, and used this data for widely accepted purposes. Therefore, this data is sufficiently reliable for the purposes of this report without requiring additional testing.

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. 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 audit of ECMCC's oversight and administration of security over critical systems.

Reporting Requirements

A draft copy of the report was provided to ECMCC officials for their review and comment. Their comments were considered in preparing this final report and are attached in their entirety at the end of it. In their response, ECMCC officials generally agreed with our recommendations and indicated actions they would take to implement 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 Erie County Medical Center Corporation 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 Amanda Eveleth, Justin Dasenbrock, Christopher Bott, Monal Patel, Cosmos Houndonougbo, Madison Adams, and Rachel Moore.

We wish to thank the management and staff of the Erie County Medical Center Corporation for the courtesies and cooperation extended to our auditors during this audit.

Very truly yours,

Nadine Morrell, CIA, CISM
Audit Director

cc: John Cumbo, Erie County Medical Center Corporation

Agency Comments

ECMC 462 GRIDER STREET | BUFFALO, NEW YORK 14215 ECMC.EDU
(716) 898-3000 | (716) 898-5178 FAX

July 22, 2025

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

Re: ECMCC Response- Public Letter
2023-s-48
Erie County Medical Center Corporation
Security Over Critical Systems Closing
Conference: 07/08/2025

Re: Acknowledgement of Public Draft

Dear Ms. Morrell:

In response to report 2023-S-048, Security over Critical Systems, ECMCC acknowledges the public draft containing the results of audit, notating several recommendations in the confidential report. During this review, discussions regarding statements within several paragraphs in the public report were acknowledged and agreed to be rephrased based on overall relation to this audit. ECMCC is grateful for the observations notated by the team which will help ECMCC improve its security posture by developing stronger procedures in the future.

Lastly, ECMCC would like to thank all the Office of the State Comptroller auditors for their cooperation in the matter listed above during this audit. Direct feedback and professionalism with clear communication demonstrated by all team members was much appreciated.

Sincerely,

Andrew Davis
President and Chief Operating Officer
Erie County Medical Center Corporation