THOMAS P. DINAPOLI
STATE COMPTROLLER

110 STATE STREET
ALBANY, NEW YORK 12236

STATE OF NEW YORK
OFFICE OF THE STATE COMPTROLLER

January 3, 2024

Mark M. Finkle
Chairman
Hudson River–Black River Regulating District
54 State Street, Suite 501
Albany, NY 12207

Re: Security Over Critical Systems
Report 2023-S-24

Dear Mr. Finkle:

Pursuant to the State Comptroller's authority as set forth in Article X, Section 5 of the State Constitution and Section 15-2129(9) of the Environmental Conservation Law, we have conducted an audit of the Hudson River–Black River Regulating District to determine if security over the District's critical systems is sufficient to minimize the various risks associated with unauthorized access to systems and data.

Background

The Hudson River–Black River Regulating District (District) is a New York State public benefit corporation whose mission is to construct, maintain, and operate reservoirs in the upper Hudson River and Black River watershed, including the Sacandaga, Indian, Black, Moose, and Beaver Rivers, for the purpose of regulating the flow of streams or rivers when required by public welfare, including public health and safety.

As a public benefit corporation, the District must adhere to the Office of Information Technology Services' (ITS) policies, including ITS' Information Security Policy and Acceptable Use Policy, for its IT assets. These policies define the minimum requirements all State entities (including public benefit corporations) must follow, including completing a data classification and applying the correct security controls for information used by the District, monitoring systems, and managing the risks of security exposure or compromise. Additionally, the District is responsible for adhering to provisions in the Department of Environmental Conservation or Federal Energy Regulatory Commission (FERC) regulations, which require security risk assessments for certain types of dams.

The District maintains a State-owned buffer zone around the Great Sacandaga Lake and provides access permits for exclusive use of this land to nearby landowners. The District accepts both in-person and online credit card payments for these permits. In general, all organizations that accept credit cards as a method of payment must comply with the Data Security Standards (DSS) established by the Payment Card Industry (PCI) Security Standards Council. The PCI DSS are comprehensive technical and operational requirements addressing security management, information security policies and procedures, and other critical protective measures associated with credit card data. These standards are intended to help an organization proactively protect customer credit card data stored, processed, or transmitted in

its network. As part of this, organizations must complete a self-assessment of their compliance with said standards.

Results of Audit

We evaluated the District's overall security posture for its dams and IT systems. This evaluation included assessments of the dams' physical security, processing of credit card payments for permits (both online through a web portal and in person), and policies and procedures for relevant IT assets and systems. Overall, the District has demonstrated effort and timeliness in addressing security issues as they arise. Due to the confidential nature of some of our evaluations, we communicated certain details to District officials and do not address those details in this report.

Prior to our audit, in May 2022, the District completed a risk assessment survey to evaluate its cybersecurity posture. The survey identified a few areas in which the District could enhance its cybersecurity posture, and we found the District took action in these areas. Additionally, on an annual basis, the District is required to complete or recertify its security assessment for dams that fall under FERC requirements. Our observations at these dams aligned with what was reported to FERC. Due to the nature of operations at these dams, the District did not have to perform an additional cybersecurity assessment as part of FERC requirements.

We further found that the District has generally taken appropriate steps to secure processes and systems used to accept credit card payments. However, there were areas in which it could improve to better meet PCI DSS requirements, including documenting certain policies and procedures.

Recommendation

1. Develop relevant policies and procedures as required for PCI DSS.

Audit Scope, Objective, and Methodology

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

To accomplish our objective and assess internal controls related to the District's security over its systems and data, we interviewed District officials and reviewed relevant documentation such as policies and procedures, data security standards, network diagrams, inventories, surveys, service agreements, and risk assessments. We performed visits to dam sites to evaluate the security of the District's systems and infrastructure and performed technical tests such as firewall analysis, network scans, website application scanning, and Wi-Fi sniffing.

We used a non-statistical sampling approach to provide conclusions on our audit objective as well as test internal controls and compliance. We selected judgmental samples. However, because we used a non-statistical sampling approach for our tests, we cannot project the results to the respective populations. Our sample included a judgmental sample of two of seven dams based on criticality.

We obtained an inventory report of network devices from the District and assessed the reliability of that data by performing our own network scans. We determined the data from the District was sufficiently reliable for the purposes of this report.

Statutory Requirements

Authority

This audit was performed pursuant to the State Comptroller's authority as set forth in Article X, Section 5 of the State Constitution and Section 15-2129(9) of the Environmental Conservation 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 the District, these include reporting the District as a discrete component unit in the State's financial statements and approving selected contracts. 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 the District's oversight and administration of security over critical systems.

Reporting Requirements

We provided a draft copy of this report to District 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, District officials agreed with our audit conclusions and recommendation.

Within 180 days after the final release of this report, as required by Section 170 of the Executive Law, the Chairman of the Hudson River–Black River Regulating District 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 recommendation contained herein, and if the recommendation was not implemented, the reasons why.

Major contributors to this report were Amanda Eveleth, Daniel Raczynski, Justin Dasenbrock, Christopher Bott, and Jonathan Julca.

We wish to thank the management and staff of the District for the courtesies and cooperation extended to our auditors during this audit.

Very truly yours,

Nadine Morrell, CIA, CISM
Audit Director

cc: John Callaghan, Hudson River–Black River Regulating District
Timothy Maniccia, Hudson River–Black River Regulating District

Agency Comments

NEW YORK STATE OF OPPORTUNITY.

Hudson River - Black River Regulating District

December 18, 2023

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

Re: Security Over Critical Systems
Report 2023-S-24

Dear Ms. Morrell:

We have reviewed the draft report on the Regulating District's security over critical systems, and are grateful for the opportunity to address the findings and recommendations.

We appreciate the audit team's conclusion that the Regulating District has demonstrated effort and timeliness in addressing security issues, as well as having taken appropriate steps to secure processes and systems used to accept credit cards. As we were able to demonstrate, the Regulating District uses an approved third-party vendor for credit card transactions in order to comply with the Data Security Standards (DSS) established by the Payment Card Industry (PCI) Security Standards Council. Customer credit card information does not reach, nor is it stored at, any online or physical location maintained by the Regulating District. We acknowledge the recommendation from the audit team that the Regulating District should develop specific policies and procedures which will serve to further enhance its compliance with PCI DSS requirements.

As the audit team found and notes in its report, the Regulating District has worked diligently to implement cybersecurity measures identified in its May 2022 cybersecurity assessment. We are grateful for the collaboration with the team and the additional observations relayed to the Regulating District during the audit process.

Lastly, the Regulating District is appreciative of the professionalism, insight and excellent communication consistently demonstrated by members of the audit team throughout the process.

Sincerely,

Mark Finkle
Chairman

54 State Street, Albany, NY 12207 | 518-465-3491
737 Bunker Hill Road, Mayfield, NY 12117 | 518-661-5535
317 Washington Street, Watertown, NY 13601 | 315-788-5440

www.hrbrrd.ny.gov