THOMAS P. DINAPOLI
STATE COMPTROLLER

110 STATE STREET
ALBANY, NEW YORK 12236

STATE OF NEW YORK
OFFICE OF THE STATE COMPTROLLER

April 23, 2025

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

Re: Security Over Critical Systems
Report 2025-F-5

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 followed up on the actions taken by officials of Hudson River–Black River Regulating District to implement the recommendation contained in our initial audit report, *Security Over Critical Systems* (Report 2023-S-24).

Background, Scope, and Objective

The Hudson River–Black River Regulating District (HRBRRD) 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, HRBRRD 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 HRBRRD, monitoring systems, and managing the risks of security exposure or compromise. Additionally, HRBRRD is responsible for adhering to provisions in the Department of Environmental Conservation or Federal Energy Regulatory Commission regulations, which require security risk assessments for certain types of dams.

HRBRRD maintains a State-owned buffer zone around the Great Sacandaga Lake and provides access permits for exclusive use of this land to nearby landowners. HRBRRD 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.

The objective of our initial audit, issued January 3, 2024, was to determine whether security over HRBRRD's critical systems was sufficient to minimize the various risks associated with unauthorized access to systems and data. Our audit covered the period from June 2023 through October 2023. Overall, we found HRBRRD demonstrated effort and timeliness in addressing security issues as they arose. Further, HRBRRD had generally taken appropriate steps to secure processes and systems used to accept credit card payments. However, we identified areas in which HRBRRD could improve to better meet PCI DSS requirements, including documenting certain policies and procedures.

The objective of our follow-up was to assess the extent of implementation, as of March 2025, of the recommendation included in our initial audit report.

Summary Conclusions and Status of Audit Recommendation

HRBRRD officials made significant progress in addressing the problem we identified in the initial audit report. The initial report's one audit recommendation has been implemented.

Follow-Up Observations

Recommendation 1

Develop relevant policies and procedures as required for PCI DSS.

Status – Implemented

Agency Action – On March 12, 2024, HRBRRD's board adopted a revised policy governing acceptance of electronic payments for its access permit system. This revised policy formalizes HRBRRD's compliance with PCI DSS by ensuring that all HRBRRD procedures for accepting payments align. Further, HRBRRD officials stated they will continue to adjust procedures in place as PCI DSS regulations evolve over time. Additionally, on an annual basis, HRBRRD continues to complete a Self-Assessment Questionnaire to attest to its compliance with PCI DSS requirements.

Major contributors to this report were Justin Dasenbrock, Christopher Bott, Madison Adams, and Cullen Spang.

We thank the management and staff of Hudson River–Black River Regulating District for the courtesies and cooperation extended to our auditors during this follow-up.

Very truly yours,

Amanda Eveleth, CFE
Audit Manager

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