New York State Comptroller
THOMAS P. DiNAPOLI

# Olympic Regional Development Authority

## Security Over Critical Payment Systems

**August 2026 | Report 2025-S-23**
Prepared by the Division of State Government Accountability

# Contents

## Authority

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 Olympic Regional Development Authority to determine whether it complies with the Payment Card Industry Data Security Standard and whether its access controls and vulnerability management over payment systems are sufficient to minimize the various risks associated with unauthorized access to systems and data.

## Background

The New York State Olympic Regional Development Authority (ORDA) was established by the New York State Legislature to operate, manage, and maintain the facilities used during the 1932 and 1980 Olympic Winter Games in Lake Placid. Its main objective is to safeguard the public's investment in these Olympic sites, as well as the venues that have been added to the list of ORDA facilities since 1980.

ORDA's mission is to bring economic and social benefits to the Adirondacks and Catskills by managing venues that offer recreational and athletic opportunities. To fulfill this mission, ORDA aims to fully utilize the Olympic and other facilities year-round. ORDA encourages fitness, hosts national and international athletic training and competitions, and operates and maintains its facilities for the general public, including young and amateur athletes.

ORDA operates and manages three downhill ski areas, including Gore Mountain and Belleayre Mountain, each approximately 80 miles from Albany, and Whiteface Mountain, just 15 minutes from Lake Placid. Additionally, ORDA operates and manages the Olympic Center, Olympic Oval, and Olympic Training Center in Lake Placid, and the Olympic Jumping Complex and Mount Van Hoevenberg Olympic Sports Complex in the town of North Elba. ORDA hosts numerous national and international competitions, and other events at its venues, attracting millions of visitors each year.

As a part of its operations, ORDA accepts credit card payments. In general, all organizations that accept credit cards as a method of payment must comply with the Data Security Standard (DSS) established by the Payment Card Industry (PCI) Security Standards Council. PCI DSS's comprehensive technical and operational requirements address security management, information security policies and procedures, and other critical protective measures associated with credit card standards. These standards are intended to help an organization proactively protect customer credit card data stored, processed, or transmitted on its network. As part of this, organizations must complete a self-assessment of their compliance with said standards.

Additionally, as a public benefit corporation, ORDA must adhere to the Office of Information Technology Services' (ITS) policies, including ITS Information Security Policy and ITS' Standards over: Account Management and Access Control, Authentication Tokens, and Vulnerability Management. Further industry standards and best practices such as the National Institute of Standards and Technology Cybersecurity Framework provide guidance to organizations of all

sizes and sectors—including industry, government, academia, and non-profit—to manage and reduce their cybersecurity risks.

## Results of Audit

We identified areas where ORDA could improve its overall governance of information technology, compliance with PCI DSS requirements, and 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 seven recommendations in a separate, confidential report to ORDA officials for their review and comment. ORDA officials agreed with our findings and have already begun actions to implement our recommendations. ORDA has proactively implemented changes to increase cybersecurity awareness and controls across the organization.

## Recommendation

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

## Audit Objective, Scope, and Methodology

The objective of our audit was to determine whether ORDA complies with PCI DSS and whether its access controls and vulnerability management over payment systems are sufficient to minimize the various risks associated with unauthorized access to systems and data. The audit covered the period from January 2024 through January 2026.

To accomplish our objective and assess related internal controls, we reviewed PCI DSS requirements and ORDA's policies and procedures. We also interviewed ORDA's officials to understand their PCI compliance, access controls, and vulnerability management processes; conducted site visits to ORDA's facilities; and reviewed governance documentation, assessments, vulnerability scans, penetration test results, and system and network configurations. We also evaluated access controls, vulnerability management, disaster recovery, data classification, PCI compliance, and third-party oversight practices, and examined supporting compliance evidence to assess ORDA's overall security posture and inform recommendations to strengthen governance and operational resilience.

We used a non-statistical sampling approach to provide conclusions on our audit objective and to 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. The details of our samples were provided to ORDA officials in our confidential report.

We obtained data from Active Directory and ORDA's HR Employee Listing System and assessed the reliability of that data by reviewing existing information, interviewing officials knowledgeable about the systems, and performing electronic testing. We were not able to directly test the

completeness, only the accuracy, of this data due to privacy concerns. However, based on other audit work, we determined that the data was sufficiently reliable for the purposes of this audit.

## 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 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. These duties could be considered management functions for the 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 ORDA's oversight and administration of compliance with payment card industry standards.

### Reporting Requirements

We provided a draft copy of this report to ORDA officials for their review and formal comment. Their response was considered in preparing this final report and is attached in its entirety at the end of the report. ORDA officials agreed with our findings and have already started to take significant actions to implement the recommendations.

Within 180 days after final release of this report, as required by Section 170 of the Executive Law, the Director of Technology of the Olympic Regional Development Authority 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 where the recommendation was not implemented, the reasons why.

## ORDA Response

NEW YORK STATE
OLYMPIC REGIONAL
DEVELOPMENT AUTHORITY

July 24, 2026

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

Dear Nadine Morrell:

This letter responds to the Office of the State Comptroller's (OSC) Draft Audit Report 2025-S-23, which addresses the New York State Olympic Regional Development Authority's (Olympic Authority) Security Over Critical Payment Systems.

The Olympic Authority agrees with the audit's findings and recommendations and appreciates OSC's review of our information technology governance, Payment Card Industry Data Security Standard (PCI DSS) compliance program, and cybersecurity controls.

Recognizing that many of the identified gaps stem from the absence of a formal governance framework rather than a lack of technical controls, the Olympic Authority is focusing on establishing sustainable governance processes that align with the Office of Information Technology Services (ITS) policies and PCI DSS requirements.

Since the Audit began, the Olympic Authority has started implementing a comprehensive cybersecurity and governance improvement initiative to strengthen compliance, improve risk management, and enhance the overall maturity of our information security program. We have implemented a Governance, Risk & Compliance (GRC) platform, deployed a new network management platform, expanded vulnerability management and penetration testing activities, modernized security policies and procedures, and developed formal governance processes.

The Olympic Authority has engaged external professionals to assist with these efforts, while evaluating and procuring additional technologies to further strengthen our cybersecurity posture.

The report's recommendations have been incorporated into our ongoing improvement program and are being tracked through formal project management and governance processes. Several

recommendations are implemented or substantially complete. The remaining initiatives are being prioritized based on risk, operational impact, available resources, and procurement timelines.

The Olympic Authority remains committed to continuous improvement and to maintaining a secure, resilient, and compliant technology environment. We appreciate OSC's engagement on this audit.

Sincerely,

Michael Costantino

Michael Costantino
Director of Technology

## Contact

Office of the New York State Comptroller
110 State Street
Albany, New York 12236

(518) 474-4044

www.osc.ny.gov

Prepared by the Division of State Government Accountability

August 6, 2026

### Executive Team

Andrea C. Miller – Executive Deputy Comptroller
Tina Kim – Deputy Comptroller
Stephen C. Lynch – Assistant Comptroller

### Audit Team

Nadine Morrell, CISM – Audit Director
Amanda Eveleth, CFE – Audit Manager
Justin Dasenbrock, CISA, ITIL, CC – IT Audit Manager
Monal Patel, CISA, GISF – IT Audit Supervisor
Madison O'Donnell – IT Auditor
Cullen Spang – IT Auditor
Rahim Uddin – IT Auditor