NEW YORK STATE | Office of Information Technology Services

NYSOC NEW YORK SECURITY OPERATIONS CENTER

E Pluribus Unum

"Out of many, one."

New York's Unified Cyber Defense Initiative

State: New York
Category: Cybersecurity
Agency: New York State Office of Information Technology Services (ITS)
Project Dates: March 2023 – March 2026
Contact: Chris Desain, State Chief Information Security Officer (chris.desain@its.ny.gov)

Executive Summary

The State of New York's Security Operations Center (NYSOC) is the nation's leading model for "whole-of-state" cyber defense, and uniquely spans state, local, and municipal government organizations to extend critical protection to vulnerable public entities that often lack resources for an adequate defense.

Between 2018 and 2024, ransomware attacks against government entities resulted in an estimated $1.09 billion in downtime costs alone.[1] Built in response to an increasingly aggressive threat landscape targeting critical infrastructure, public services, municipalities, educational institutions, and state agencies[2,3], the NYSOC establishes a unified cyber defense ecosystem that brings together state entities, local governments, public authorities, law enforcement, emergency management, and strategic partners in a shared operational model.

The NYSOC is a centralized cyber coordination and operational fusion capability. In collaboration with NY Division of Homeland Security and Emergency Services (DHSES) and through subscriber onboarding, log collection, real-time monitoring, threat intelligence sharing, incident coordination, and proactive threat hunting, the initiative gives New York a new visibility paradigm: broader, deeper, and faster insight across the state's cyber landscape.

When one subscribed entity sees a threat, indicators are rapidly analyzed, shared, and operationalized to help protect many others before the threat spreads.

That shared visibility materially improves the state's defensive posture.

Operating 24x7x365 from Manhattan, Rochester, and Albany, the NYSOC is staffed by 60+ analysts and, as of June 2026, supports all state agency infrastructure managed by the New York State Office of Information Technology Services (ITS), and 34 additional state and local government entities, with many more still being onboarded.

This shared service model extends enterprise-grade cyber operations to public-sector organizations that may otherwise lack the resources to build and sustain such capabilities independently. At the same time, it strengthens statewide situational awareness, accelerates detection and response,

and enables coordinated action at scale.

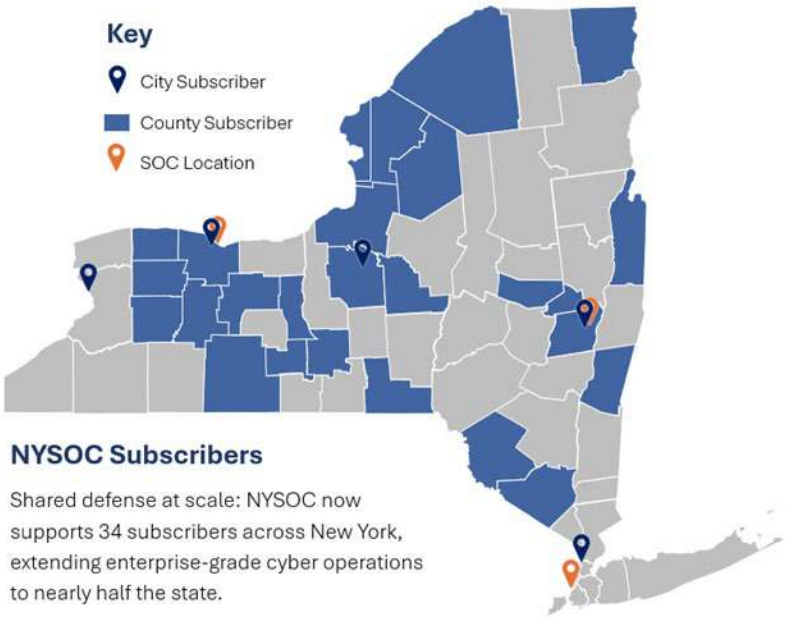
The initiative has transformed how New York identifies, prioritizes, escalates, and responds to cyber threats by combining centralized visibility, advanced analytics, collaborative operational governance, and shared defense services.

In doing so, New York has demonstrated national leadership in operationalizing a modern cyber defense model—one that protects individual subscribers while making the entire state more resilient.

[1] *Information Technology & Innovation Foundation (ITIF), Improving State and Local Government Cybersecurity, 2026.*
[2] *FBI Internet Crime Complaint Center (IC3), Internet Crime Report 2024.*
[3] *U.S. Department of Homeland Security, Homeland Threat Assessment 2025.*

Idea

New York State recognizes that modern cyber threats can strike multiple government organizations in an orchestrated fashion. Ransomware groups, nation-state actors, and other sophisticated adversaries increasingly target the interconnected ecosystem of state agencies, local governments, public authorities, critical infrastructure, public safety operations, schools, and other public services. In that environment, a cyber incident affecting one organization can quickly create broader operational risk across multiple jurisdictions and essential services. This aligns squarely with the sentiment of the Cybersecurity and Infrastructure Security Agency (CISA): "To protect our nation's infrastructure, it is essential to foster relationships across government that protect critical infrastructure and reduce cyber risk."[4]



As of 2025, the global average cost of a data breach is a staggering $4.4 million[5]. Traditional agency/municipality-centric cybersecurity models leave the government defending this shared threat landscape in isolated ways. It creates an uneven cybersecurity capability, limited visibility across jurisdictions, slowed collective response, and it leaves smaller municipalities and public-sector organizations without the resources to sustain a robust and aggressive cybersecurity operation (such as, 24x7 monitoring, threat intelligence, incident coordination, and proactive cyber defense). It is a fragmented model for a threat environment that is anything but fragmented.

> **New York's Answer:** Rethink cyber defense as a "whole-of-state" operational mission. Create a cyber defense collaboration, a first-of-its-kind cyber command center for New York—designed to bring together state and local infrastructure partners under one coordinated operational umbrella.

Operationally delivered through NYSOC, this initiative introduces a new statewide visibility paradigm. Instead of seeing threats only within the boundaries of a single organization, New York created a model that enables centralized situational awareness, real-time monitoring, threat intelligence sharing, proactive threat hunting, and coordinated incident response across a broad public-sector ecosystem. **Shared visibility is the breakthrough:** when one subscriber is targeted, indicators can be rapidly identified, correlated, and shared to help protect many others before the threat spreads.

This makes NYSOC different from a traditional SOC. It is not simply a monitoring function for one enterprise; it is a statewide cyber coordination and shared defense capability that integrates state agencies, municipalities,

[4] *Cybersecurity & Infrastructure Security Agency (CISA), State, Local, Tribal and Territorial Government Resources, 2025.*
[5] *IBM, Cost of a Data Breach Report, 2025.*

public authorities, public safety organizations, law enforcement, emergency management, and strategic partners into a unified operational model. It transforms cybersecurity from a decentralized technical activity into a coordinated resilience mission focused on service continuity, faster response, and stronger protection for all participating entities.

This idea matters because every state faces the same core challenge: cyber risk is shared, but cybersecurity capability is often uneven. New York fundamentally transformed cybersecurity from isolated defense to shared defense—**making the state stronger not just entity by entity, but as an interconnected whole**.

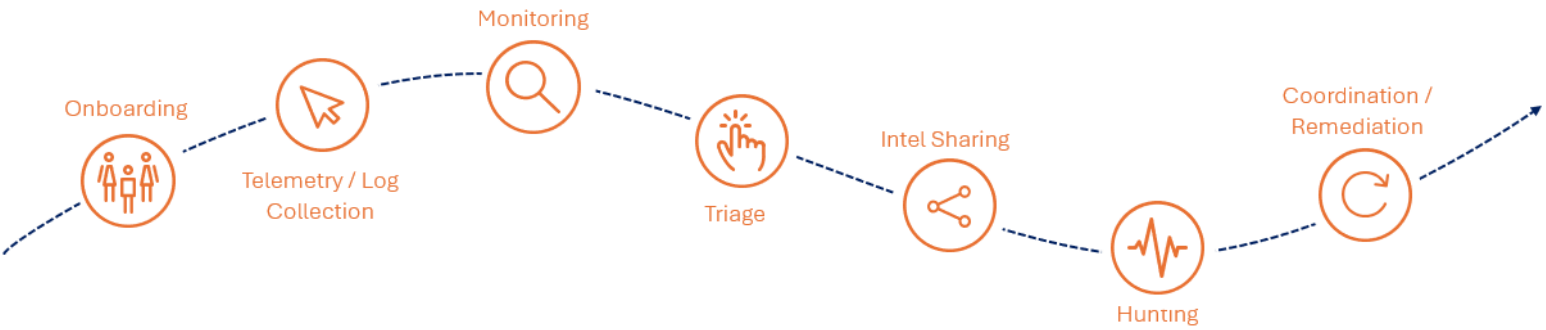
Implementation

New York State implemented NYSOC as a cybersecurity modernization initiative and a new statewide operating model. In line with Governor Kathy Hochul's original vision for a "whole-of-state" cyber defense capability, this implementation was designed to give New York a broader view of the threat landscape, strengthen coordination across jurisdictions, and extend advanced cyber operations to public entities that could not easily build or buy those capabilities on their own.

Operational Model: New York established the NYSOC as an operational fusion capability. The model was built to monitor alerts and to coordinate intelligence, escalation, and action across a wide public-sector ecosystem. The governance structure brought together cybersecurity leadership, operational stakeholders, subscriber organizations, and response partners into a common framework for escalation, information sharing, situational reporting, and coordinated decision-making.

THE IMPLEMENTATION ROADMAP IS CENTERED ON FOUR STRATEGIC OBJECTIVES:

1. Establish statewide cyber situational awareness
2. Enable coordinated incident escalation and response across jurisdictions
3. Deliver scalable shared cybersecurity services to subscribed local governments
4. Reduce cyber-related disruption risk to public services through faster detection, coordination, and response



Shared Service Delivery at Statewide Scale: ITS then operationalized NYSOC as a shared service for counties, cities, and municipalities. New York created a centralized service that provides subscriber onboarding, log collection, real-time monitoring, threat intelligence sharing, and proactive threat hunting through a single operating model. Today, that model operates 24x7x365, supported by three locations—Manhattan, Rochester, and Albany—with more than 60 analysts supporting 34 subscribers, with many more still onboarding.

Standardized Telemetry: For operational effectiveness, the NYSOC standardized onboarding around the log and telemetry sources that provide the clearest, fastest signal across subscriber environments. NYSOC currently targets nine core log categories:

Server OS Security	Web Proxy/Filter	VPN	EDR/AV	E-Mail	IDS/IPS	Firewall	DNS	Identity

This model is centered on central collection and central correlation. Standardized telemetry creates a common visibility layer across subscribers, allowing detection logic and analysts to identify patterns faster, connect related activity, and turn one subscriber's indicators into protective insight for many others.

The Workforce: Implementation also required building a durable operating rhythm across teams of people. NYSOC's multi-location workforce: analysts, cyber operators, and engineers collaborate with and support subscriber entities, NY DHSES, and other state and local stakeholders. From concept to scaled service delivery, success depended on leadership alignment, clear onboarding processes, shared escalation paths, and trust that participating jurisdictions would gain value from centralized monitoring without losing local partnership. That collaboration is consistent with the broader intent of the NYSOC launch, which emphasized breaking down silos and improving coordination among state, local, and other public-sector stakeholders.

Why it Works: NYSOC is a success because New York treated it as a statewide operational mission. The state built a repeatable model for onboarding subscribers, standardizing telemetry, staffing continuous operations, and sharing intelligence and response actions across jurisdictions. That combination of governance, shared services, and centralized visibility is what turned NYSOC from a concept into a functioning statewide cyber defense capability.

Impact

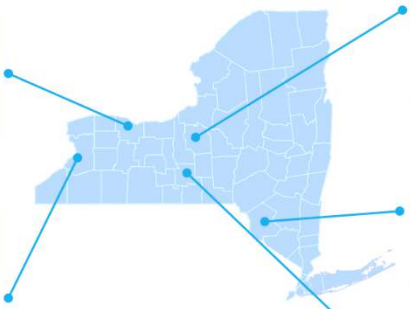
The NYSOC materially strengthens New York State's cybersecurity posture, operational resilience, and ability to coordinate cyber defense across a diverse public-sector ecosystem. By centralizing visibility, improving collaboration, and operationalizing statewide cyber coordination, New York has defined a model for unified and scalable cybersecurity operations, a model for detecting, managing, and responding to cyber threats affecting government operations and citizen services that can be replicated by others. What was once fragmented and imbalanced has evolved into a broader statewide operational capability where communities across the state benefit from strong, persistent, and consistent protection.

"I've got nothing but good things to say – you guys have been absolutely fantastic, [go-live] couldn't have gone any better. Whatever next project we're on, we hope to engage a team like you because you have been fantastic"

– Bill Boudreaux | Rochester Chief Technology Officer

"CrowdStrike and this project have gone extremely well and at a rapid pace, absolutely wonderful to see government organizations come together like this and be able to deploy something so quickly… hats off to everybody, all the teams that had to get together to do this, DHSES, ITS, and NYSOC … Great job everybody, looking forward to a great relationship with all of you moving forward"

– Daryl Springer | Buffalo Chief Information Officer (CIO)



"DHSES, CIO's office… really gaining momentum with the product offering and the depth of the team you are putting forward to stand it up. This went really well"

– Dave Prowak | Syracuse Director of Information Technology

"This has been one of the most proactive New York State initiatives that I've seen in my entire career here. I just want to thank everybody for their involvement and their contributions to making this happen. It's critical, and I can't state how thankful we are for the fact that this exists."

- Lorne Green | Sullivan County Chief Information Officer

"Can't say enough good things about this process, it could've been a really complicated project, and we never would've been able to get to this point without the teamwork of everyone on this call" [Go-Live]

- Kim Moore | Tompkins County Deputy Director of ITS

Stronger Detection | Coordinated Response | Expanded Protection: NYSOC significantly improved New York's ability to identify, triage, and respond to cyber activity through a shared operational model. For many participating organizations, this introduced and provided capabilities that would otherwise not be possible. The shared services model enables organizations with limited cybersecurity resources to benefit from enterprise-scale cyber defense capabilities. As participation has expanded, NYSOC has broadened protection across New York's public-sector environment.

Cross-Boundary Collaboration: One of NYSOC's most significant achievements has been the creation of an operational collaboration model that extends across traditional organizational boundaries. The initiative has helped unify cyber defense activities among the State, its cities, counties, and its agencies. This collaboration model demonstrates how statewide cyber defense can be operationalized through shared governance, common visibility, and coordinated operational responsibility.

Public Impact: NYSOC directly supports the continuity and resilience of essential services relied upon by millions of New Yorkers. By improving statewide cyber resilience, NYSOC helps reduce the risk that cyber incidents will disrupt critical public services and strengthens the state's ability to maintain operations during periods of heightened threat activity.

What's Next?

NYSOC was designed as an evolving statewide operational capability. As cyber threats continue to grow in speed, scale, and complexity, New York is now advancing the next phase of its cybersecurity transformation, which includes modernization of the state's security operations platform through migration to a next-generation toolset. This transformation is intended to enhance data integration, improve automation, strengthen analyst workflows, and support faster, more scalable detection and response across the enterprise.

At the same time, the state is leaning forward on the use of Artificial Intelligence to improve operational efficiency and augment cyber defense activities. Applied responsibly, these capabilities will help streamline investigation workflows, accelerate triage, improve signal-to-noise management, and support faster decision-making by analysts and operators.

New York's direction is clear: as a "whole-of-state" continue evolving NYSOC into a more intelligent, automated, and scalable statewide cyber defense capability that better protects government operations, critical infrastructure, and the citizens who depend on them.

Conclusion

NYSOC demonstrates how a state can turn cybersecurity from a fragmented local challenge into a coordinated statewide capability. By delivering a SOC as a shared service, New York has expanded protection, increased operational maturity, and brought enterprise-grade cyber defense to jurisdictions that need it most. The model is practical, scalable, and replicable. It demonstrates how states can strengthen resilience across a complex, diverse, and interconnected public ecosystem.