



Executive
Chamber

KATHY HOCHUL
Governor

MEGHAN COOK
Chief Cyber Officer

Examining the Implementation, Fiscal Impact, and Technical Sufficiency of Mandatory State Water Security and Wastewater Security Regulations

New York State Senate Joint Standing Committee on Local Government

Senate Standing Committees on Local Government, Cities 1, and Cities 2

Testimony of:
Meghan Cook
Chief Cyber Officer
New York State

New York, NY
October 1, 2026

INTRODUCTION

Chairwoman Martinez, Chairman Bottcher, Chairman Ryan, and distinguished members of the Committee:

Thank you for the opportunity to testify and represent New York State on this important topic of cybersecurity of water and wastewater systems and the critical role the State has to play in proactively protecting New Yorkers.

When discussing cybersecurity and preparedness for the water and wastewater sector, we must confront an escalating and deeply asymmetric threat landscape. For years, the intelligence community has warned that nation-state and affiliated actors are targeting critical infrastructure, positioning themselves for potential disruption and destruction, including in water and wastewater systems^{1, 2} Today, these threat actors are becoming increasingly sophisticated, efficient, and dangerous. They are rapidly leveraging the increasing availability of AI to enhance their offensive capabilities and scale their operations. This creates a severe imbalance between offense and defense: adversaries only need to succeed a few times, while our defenders must succeed all the time. This asymmetry is pronounced in the water and wastewater sector, especially at facilities where limited resources for personnel and cybersecurity investments are a challenge.

As we all saw this summer, our nation's water and wastewater systems were targeted in a coordinated cyberattacks that spanned across at least 100 facilities across 12 states; the impact of these attacks varied, ranging from boil water advisory issuance, operators being locked out of their systems temporarily, and switching to manual operations.³ While New York was not one of the affected states, these cyberattacks only underscore the importance of continuing to strategically strengthen our defenses in New York.

Governor Kathy Hochul's 2023 whole-of-state New York State Cybersecurity Strategy recognizes that building New York's security posture requires the State to use two types of levers: control and fortification. Control levers, such as legislation, regulation, and enforcement, provide our water and wastewater systems clear expectations for baseline cybersecurity requirements that are threat- and risk-informed, and cost-conscious. Fortification levers, such as cybersecurity investments and

¹ <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a>

² <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a>

³ <https://www.csis.org/analysis/mapping-iranian-cyberattacks-us-water-systems>

services provide our operators on the frontlines the practical resources needed to shore up their defense. These two key lever types are organized across five strategic pillars that work to reinforce each other: (1) operate New York State government networks securely and resiliently; (2) collaborate with key stakeholders; (3) regulate critical industries; (4) communicate cybersecurity guidance; and (5) grow the cybersecurity workforce and economy statewide.

Over the years, New York State has proactively operationalized the statewide cybersecurity strategy to protect New Yorkers from cyber threats, especially across our critical infrastructure sectors. For the water and wastewater systems sector, Governor Hochul directed the State's regulators with jurisdiction over water and wastewater to work hand-in-hand to promulgate threat- and risk-informed, cost-conscious, and harmonized cyber regulations. These cyber regulations for the sector were adopted in March 2026 through NYS Department of Health (DOH) and NYS Department of Environmental Conservation (DEC). As a result, New York is the first in the nation to set cybersecurity regulations for the water and wastewater sector and has achieved through a coordinated approach to reduce the regulatory burden on covered entities, while ensuring common sense regulations setting minimum cybersecurity baselines.

To ensure that the sector also had access to practical resources to fortify defenses, Governor Hochul also directed NYS Environmental Facilities Corporation to develop a dedicated cybersecurity grant in coordination with DOH and DEC, paired with technical assistance services. In addition to the \$10 billion in investments in water and wastewater infrastructure since 2017, the State has invested over \$9 million in cybersecurity project funding for 153 local governments.

Moreover, there has also been investment in building capacity and capability within and across the Division of Homeland Security and Emergency Services (DHSES), DEC and DOH (water). The unified mandatory cyber reporting portal now is one place to report cyber incidents, both DOH (water) and DEC have expanded their cyber capacity and capability through the Bureau of Water Supply Protection and the Division of Water, respectively in 2026. Through continued training, inter-agency information sharing, and operational development, DOH (water) and DEC continue to strengthen their ability to oversee the water and wastewater sector, including through cybersecurity regulation enforcement, analysis of cybersecurity risk assessments, and inter-agency information sharing. The DHSES Critical Infrastructure Unit conducts no-cost cybersecurity assessments of critical infrastructure across the state, including for water and wastewater systems, pursuant to NYS

Executive Law, Article 26 as well as reviews Cybersecurity Vulnerability Assessments that public water systems submit to DOH pursuant to Public Health Law §1125. These assessments are important for the State's cybersecurity risk picture across the critical infrastructure sectors, and provides a valuable gateway for critical infrastructure operators to receive trusted and custom recommendations for increased cyber resilience.

With our leading statewide threat intelligence gathering, analysis, and dissemination muscles that are routinely built through the State's cyber intelligence functions. Namely, within the New York State Police is the New York State Intelligence Center (NYSIC) Cyber Analysis Unit (CAU) who provides intelligence analysis and dissemination for critical infrastructure stakeholders across the state; NYSIC CAU serves as the trusted and centralized dissemination arm to curate threat intel and communicate Indicators of Compromise (IoCs) to numerous stakeholders throughout the state.

Additionally, for many local governments that operate water and wastewater facilities, statewide offerings are available. For example, the State's Cybersecurity Shared Services Program serves as an access point to receive cybersecurity tools and defenses through the State. The Cyber Shared Services model leverages economies of scale and the State's buying power to maximize the State's return on cyber investment and continues to be a leading model throughout the nation.

The statewide cyber shared services program works hand in hand with the Joint Security Operations Center (JSOC), that supports state and local governments 24x7x365 by bringing together federal, state, city, and county governments, critical businesses and utilities, and state entities to coordinate and operationalize cybersecurity incident response and threat intelligence exchange.⁴ Through the establishment of the JSOC, the State is able to have a unified visibility of cybersecurity events and incidents across the State's networks, as well as those of the 36 cities and counties currently enrolled in the NYS Cybersecurity Shared Services' Security Information and Event (SIEM) offering. This unification under the JSOC continues to be instrumental in coordinating an effective and efficient cybersecurity incident response operations across a range of partners through purposeful centralization.

My testimony focuses on the evolving threat landscape facing frontline water and wastewater operators daily and showcases New York State's proactive investments and nation-leading,

⁴<https://www.governor.ny.gov/news/governor-hochul-announces-formation-joint-security-operations-center-oversee-cybersecurity>

'whole-of-state' approach to continue to strengthen local resilience, and reliability against cyber attacks.

1. THREAT LANDSCAPE

Today's cyber threats for the water sector, and other critical infrastructure sectors, are increasingly fueled by artificial intelligence (AI) and convergence of threat actors playing out on a complex geopolitical stage.

A. Artificial Intelligence as Accelerant

In an already asymmetrical dynamic favoring adversaries over defenders, advancements in frontier AI and open-weight models is adding fuel to an already volatile threat environment for the water and wastewater systems sector.

Frontier AI and open-weight models lower the technical barriers for sophisticated offensive cybersecurity capabilities. That is, the overall population of adversaries that could launch a sophisticated cyberattack is growing due to accessibility of AI tools. Instead of taking a hacker weeks to prod around, discover vulnerabilities, and exploit them to launch a cyberattack, today we're seeing that adversarial workflow dramatically speed up to just hours.⁵ Long gone are the days of glaring typos and low-quality phishing emails. The barrier to creating an incredibly realistic phishing email and malicious websites has dropped due to availability of deepfakes and generative AI; a sophisticated ransomware attack is that much easier to put together.⁶ With lowered technical barriers, we're seeing increased frequency of cyberattacks.⁷ These factors culminate in AI serving as an accelerant to the threat landscape where threat actors' capacity and capability to compromise and infiltrate a victim's systems are increasing at scale.

For the water and wastewater systems sector in particular, these AI developments make it clear that foundational cybersecurity controls are all that more important. While AI-enabled cyberattacks open up the possibility for more sophisticated attacks, we're seeing that hackers are more often using AI to increase their reach of easy targets. As our nation saw in July 2026, over 100 water facilities across the nation fell victim to a coordinated cyberattack due to poor password management.⁸ In February

⁵ <https://www.ibm.com/think/insights/the-mythos-moment-when-discovery-outpaces-defense>

⁶ <https://go.crowdstrike.com/2026-global-threat-report.html>

⁷ <https://mitsloan.mit.edu/ideas-made-to-matter/ai-cyberattacks-three-pillars-defense>

⁸ <https://www.securityweek.com/cisa-over-100-internet-exposed-water-systems-targeted-in-july-cyberattacks/>

2026, a water facility in Mexico fell victim to an AI-assisted cyberattack that targeted the enterprise information technology (IT) environment and used AI to identify operational technology (OT) that was critical to their physical processes.^{9, 10} These examples of cyberattacks on the water and wastewater systems sector did not require any novel or highly sophisticated tactics or techniques. AI allows attackers to speed and scale up exploitation of widely known vulnerabilities that can be mitigated through basic cybersecurity hygiene, such as changing default passwords, enforcing multi-factor authentication, and disconnecting unnecessary internet connections.

These recent developments in the cyber threat landscape that frontline water and wastewater operators face make it clear that baseline cybersecurity hygiene practices are non-negotiable today and the foreseeable future. Based on this understanding of current threats, New York State has prioritized cybersecurity regulations and investments to strengthen our controls and fortification of the sector.

B. Geopolitics and Cascading Impact on Cyber

The cyber threat landscape of the water and wastewater systems sector is increasingly becoming enmeshed in geopolitical dynamics of the U.S. and adversaries, with threats escalating from nation state-sponsored and -aligned cyber actors. In March 2024, the White House and the Environmental Protection Agency (EPA) issued a joint letter to U.S. governors warning that disabling cyberattacks are striking water facilities nationwide, urging states to assess cyber vulnerabilities and implement critical controls.¹¹ A month later, the EPA again emphasized that many facilities are still vulnerable to cyberattack due to lacking foundational cybersecurity controls and practices amidst escalating threats from adversaries,¹² including from Iran,¹³ Russia,¹⁴ and China.¹⁵ Particularly illustrative of the volatile and dynamic nature of the threat landscape U.S. water and wastewater infrastructure face are two notable cyberattack campaigns from 2023 and 2026.

In late 2023 amidst the Israel-Iran conflict, the U.S. government attributed a series of disruptive attacks on water utilities to "Cyber Avengers," a group directly linked to the Islamic Revolutionary

⁹<https://www.dragos.com/blog/ai-assisted-ics-attack-water-utility>

¹⁰<https://gambit.security/blog-posts/a-single-operator-two-ai-platforms-nine-government-agencies-the-full-technical-report>

¹¹<https://cyberscoop.com/epa-water-threats-governors/#:~:text=These%20attacks%20have%20the%20potential%20to%20disrupt,and%20incite%20widespread%20panic%20in%20a%20crisis.>

¹² <https://www.epa.gov/enforcement/enforcement-alert-drinking-water-systems-address-cybersecurity-vulnerabilities>

¹³ <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a>

¹⁴ <https://www.cisa.gov/resources-tools/resources/defending-ot-operations-against-ongoing-pro-russia-hackivist-activity>

¹⁵ <https://www.epa.gov/newsreleases/biden-harris-administration-engages-states-safeguarding-water-sector-infrastructure>

Guard Corps.¹⁶ Back in November 2023, Cyber Av3ngers targeted programmable logic controllers (PLCs) that were made by an Israeli company. Notably, it successfully breached the Municipal Water Authority of Aliquippa, PA, compromising an internet-connected PLC with poor password security, forcing water operators to switch to manual controls.

In July 2026, the U.S. water and wastewater facilities were targeted in a coordinated series of cyberattacks. We now know that this campaign of attacks successfully struck more than 100 facilities across 12 states;¹⁷ the impact of these attacks varied, ranging from countywide boil water advisory issuance, operators being locked out of their systems temporarily, and switching to manual operations.¹⁸ While the U.S. government has not made any public attributions to a specific nation-state or group, security researchers noted that tactics observed in these coordinated cyberattacks align with Iranian-affiliated state-aligned campaigns.

These cyberattacks targeting the water and wastewater systems in the U.S. in recent years illustrate the complex and dynamic relationship between geopolitics and cyber threats. International geopolitics between nation-states today implicate nation-state aligned threat actors that serve as strategic proxies for nation-states, representing a convergence of threat actors in cyberattacks. The resulting threat landscape for the sector is one where geopolitical scenarios playing out on the world stage have cascading effects on the cyber threat environment.

II. NEW YORK'S WHOLE-OF-STATE APPROACH

A. Unified Governance and Strategy Execution

Governor Hochul first created the Chief Cybersecurity Officer role in 2022 to centrally execute her vision for protecting New York from digital threats. By centralizing cyber leadership and operational oversight under a unified leadership, the State is able to coordinate and align operations across stakeholders and domains. Given that cybersecurity spans across actors and domain areas in today's increasingly digital world, this governance unification has been especially instrumental in strategically aligning resources to develop and mature impactful cybersecurity programs and operations.

In 2023, the Governor released the State's first-ever Cybersecurity Strategy. The strategy is organized across five strategic pillars that reinforce each other: (1) operate New York State

¹⁶ <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a>

¹⁷ <https://www.cisa.gov/resources-tools/resources/exposure-reduction>

¹⁸ <https://www.csis.org/analysis/mapping-iranian-cyberattacks-us-water-systems>

government networks securely and resiliently; (2) collaborate with key stakeholders; (3) regulate critical industries; (4) communicate cybersecurity guidance; and (5) grow the cybersecurity workforce and economy statewide. These strategic pillars work together to build up cybersecurity resilience for the state through control and fortification levers; control levers create and shape systems of rules and enforcement through legislative, regulatory, and enforcement mechanisms, whereas fortification levers increase capacity and capabilities through investments and services to build up defenses. Both control and fortification levers are critical to ensure that the water and wastewater systems across the state have clarity on where to go and have access to funds and services to get them there. This is the New York State cybersecurity model that continues to work for New Yorkers and to serve as a nation-leading model for other states.

B. Vertical View: Water and Wastewater Cyber

In Governor Hochul's January 2025 State of the State, she announced her vision to safeguard New York's water and wastewater infrastructure from cyber threats through harmonized regulations and grants; these regulations paired with grants advance her strategy by taking a multi-pronged approach to leverage build both the controls and fortifications for the sector.

(1) Cyber Regulations

In New York, there are three regulators with different but overlapping regulatory jurisdiction over the water and wastewater systems that serve New Yorkers everyday: Department of Health (DOH), Department of Environmental Conservation (DEC), and Department of Public Service (DPS). Governor Hochul directed the three regulators to set "minimum cybersecurity standards for water and wastewater utilities so New Yorkers will continue to have access to clean, safe, and reliable water and wastewater services" in January 2025.¹⁹

In March and April 2026, DOH, DEC, and DPS each adopted cybersecurity regulations for the sector that were each threat-informed, risk-centric, cost-conscious, and harmonized across regulators to the extent practicable. DOH and DEC regulations set baseline requirements for operational technology (OT) of public water systems and wastewater systems, including mandatory cybersecurity incident reporting, cyber risk assessments, and tiered standards to protect critical operations and sensitive information, as well as designation of a cybersecurity lead role at facilities servicing a larger

¹⁹ <https://www.governor.ny.gov/sites/default/files/2025-01/2025StateoftheStateBook.pdf>

population or designed for a high-volume operations.²⁰ DPS regulations set baseline requirements for information technology (IT) of various utilities, including private water corporations, mandatory cybersecurity incident reporting, cyber risk assessments, and implementation of a cybersecurity program to protect critical operations and sensitive information.²¹ As a result, New York is the first in the nation to set cybersecurity regulations for the water and wastewater sector and has achieved this in a harmonized manner to reduce the regulatory burden on covered entities while ensuring common sense regulations set minimum baselines.

(2) Cyber Investments

Governor Hochul paired the State's cyber regulations for the water and wastewater sector with a new cybersecurity grant dedicated to projects to assist with regulatory compliance, in addition to the Governor's five-year \$3.75 billion clean water investments in the 2027 Enacted Budget, bringing the total State grants to more than \$10 billion since 2017.²²

In August 2026, the Governor announced more than \$9 million in grant funds would be made available for cybersecurity assessments and hardening implementation projects across 153 water systems through the NYS Environmental Facilities Corporation (EFC) and their newly established Strengthening Essential Cybersecurity for Utilities and Resiliency Enhancements (SECURE) grant program.²³ Additionally, EFC's Community Assistance Teams provide technical assistance, including cyber technical assistance and SECURE grant navigation, at no-cost to water and wastewater operators.²⁴

(3) Cyber Capability Building

New York State agencies have also built up their cybersecurity capabilities in-house to address the growing cyber-enabled threats on the water and wastewater systems sector and critical infrastructure writ large. Presenting a non-exhaustive list, three agencies are highlighted below.

1. *Inter-Agency Unification of Cybersecurity Incident Reporting Intake*: To ensure that New York's water and wastewater operators that are under the regulatory jurisdiction of multiple legislation

²⁰<https://www.governor.ny.gov/news/governor-hochul-announces-first-nation-cybersecurity-regulations-and-grants-protect-new-york>

²¹ <https://dps.ny.gov/news/psc-adopts-nations-most-aggressive-cybersecurity-regulations-major-electric-gas-steam-and>

²²<https://www.governor.ny.gov/news/governor-hochul-announces-more-9-million-cybersecurity-grants-help-protect-153-water-systems>

²³ <https://efc.ny.gov/cybersecurity-hub>

²⁴ <https://efc.ny.gov/CAT>

and regulations to report cybersecurity incidents to the State, the DOH, DEC, and DHSES has made concerted effort to provide a unified cybersecurity incident reporting mechanism. For example, a municipality-owned and -operated public drinking water facility that also treats wastewater has legislative and regulatory obligations to report qualifying cybersecurity incidents to the NYS Division of Homeland Security and Emergency Services (DHSES) within 72 hours, NYS Department of Health (DOH) within 24 hours, and NYS Department of Environmental Conservation (DEC) within 24 hours with a written follow-up within 30 days. In recognition of this potential reporting burden, DHSES, DOH, and DEC allow covered entities to report a single cybersecurity incident to them through a unified reporting portal, which was rolled out alongside DOH and DEC adoption of cybersecurity regulations for the sector.

2. *Cyber Risk Assessments*. The DHSES Critical Infrastructure Unit conducts no-cost cybersecurity assessments of critical infrastructure across the state, including for water and wastewater systems, pursuant to NYS Executive Law, Article 26. DHSES reviews Cybersecurity Vulnerability Assessments that public water systems submit to DOH pursuant to Public Health Law §1125. These assessments are important for the State's cybersecurity risk picture across the critical infrastructure sectors, and they provide a valuable gateway for critical infrastructure operators to receive trusted and custom recommendations for increased cyber resilience.

C. Horizontal View: Statewide Model

New York's critical infrastructure sectors benefit from unified statewide cybersecurity resources statewide, including nation-leading Cybersecurity Shared Services; unified cybersecurity incident reporting and response; vulnerability assessments and recommendations; proactive threat intelligence dissemination, and statewide AI safety regulations for AI developers.

(1) Cybersecurity Shared Services

Since 2023, New York State established and has since expanded the Cybersecurity Shared Services program, which is available to eligible counties and local governments, including those that own and manage their own water and wastewater facilities. This program has been instrumental in maximizing the State's returns on investment in fortifying statewide cybersecurity resilience. The Shared Services Program leverages economies of scale and the State's buying power to bring enterprise-grade

cybersecurity tools and services to resource-challenged local governments that would have otherwise been cost-prohibitive.

Today, the Cybersecurity Shared Services Program offerings include: Endpoint Detection and Response (EDR), Attack Surface Management (ASM), Security Information & Event Management (SIEM), and Multi-Factor Authentication (MFA) tokens that continue to build statewide cybersecurity protections. As of September 2026, EDR protects 100,792 endpoints from suspicious activity; ASM covers 112,320 assets to track their exposure from the internet; SIEM services 36 counties and cities that send their security logs to the State's Joint Security Operations Center for 24x7x365 monitoring and response; and more than 112,000 MFA tokens have been distributed to more than 160 eligible local government entities, school districts, and public authorities to bolster their digital locks.

The value and impact of these Shared Services cannot be understated. EDR and ASM together have saved about \$19 million for county and local governments over a three-year period, bringing enterprise-grade cybersecurity tools to resource-constrained jurisdictions that would otherwise have been cost-prohibitive. On cybersecurity value and impact, EDR meaningfully reduces time to identify and recover from a cybersecurity incident: a county enrolled in our EDR program took about 37 seconds to recover from an incident,²⁵ whereas a peer county without EDR took 2,880 minutes or two days. Over the course of a month in 2025, EDR has remediated 1,178 incidents, 40 of which required human intervention. When it comes to combatting AI-enabled increase in volume of cyberattacks, enterprise-grade tools make a meaningful difference in defense by automating detection and remediation of cyberattack attempts wherever possible.

The Cybersecurity Shared Services Program is a successful model that works and scales across New York. This model continues to serve as a blueprint for peer states that are taking our unified, strategic approach of whole-of-state cyber operations.

(2) Cybersecurity Incident Reporting & Response

In 2022, Governor Hochul launched the Joint Security Operations Center (JSOC) operated by New York State Information Technology Services (ITS). The JSOC supports state and local governments 24x7x365 by bringing together federal, state, city, and county governments, critical businesses and utilities, and state entities to coordinate and operationalize cybersecurity incident response and threat

²⁵ In 2024, Shared Services EDR identified a malicious payload on a county host traced to a user interacting with a fraudulent form. Detection, containment, and confirmed remediation took 37 minutes thanks to EDR in this case.

intelligence exchange.²⁶ Through the establishment of the JSOC, the State is able to stitch together a unified visibility of cybersecurity events and incidents across the State's networks, as well as those of the 36 cities and counties enrolled in the NYS Cybersecurity Shared Service's SIEM offering. This unification under the JSOC continues to be instrumental in coordinating an effective and efficient cybersecurity incident response operations across various partners through centralization; while duplicating a security operations center for each State and local entity would be fiscally impractical and operationally dubious, the JSOC has proved instrumental in ensuring that the State orchestrates an effective cybersecurity incident response across stakeholders when needed.

Through cyber incident reporting metrics, we see strong evidence that New York's approach to building up statewide cyber controls and fortifications is working. New York has been tracking mandated and voluntary reporting of cybersecurity incidents reported to the State through NYS Division of Homeland Security and Emergency Services (DHSES); municipal corporations and public authorities are required by law to report cybersecurity incidents to DHSES.²⁷ While the State's cybersecurity incident reporting requirements are likely correlated with the overall increase in reported incidents, a key metric is dropping: ransomware incidents. Compared to 14 reported ransomware incidents in 2023, the first quarter of 2026 saw none. This indirect relationship of reported incidents and ransomware incidents together suggest that the State is improving its visibility of incidents while increasing cyber resilience and reliability by bolstering our controls and fortifications.

When incidents are reported centrally to DHSES' Cyber Incident Response Team (CIRT), municipalities and public authorities benefit from the centralized response communications and assistance through DHSES CIRT. On the other hand, the State benefits by being able to consistently and repeatedly kick off the statewide cybersecurity incident response workflow through centralized triaging via DHSES CIRT. The statewide response workflow includes assessment of potential impact to the State network and taking remediation measures as appropriate, often erring on the side of caution to mitigate potential risks to the State.

(3) Cybersecurity Threat Intelligence

²⁶<https://www.governor.ny.gov/news/governor-hochul-announces-formation-joint-security-operations-center-oversee-cyber-security>

²⁷ <https://www.governor.ny.gov/news/governor-hochul-announces-legislation-now-effect-strengthen-cybersecurity-across-new-york>

In escalating cyber-enabled threat scenarios, the Chief Cyber Officer has orchestrated threat intelligence briefings for public- and private sector critical infrastructure leaders and operators across the state. For example, when the Israel-Iran conflict was quickly evolving in June 2025, the State ensured that critical infrastructure leaders and operators in New York had timely and relevant information through a unified series of sector-specific briefings for the water and wastewater, healthcare, transportation, energy, and finance sectors; NYS Executive Chamber, New York State Police (NYSP), New York State Division of Homeland Security and Emergency Services (DHSES), and various State leadership provided a unified threat intelligence briefing to over 1,200 total attendees over two days in July 2025. Additionally, when the State became aware of coordinated cyberattacks on the water and wastewater systems sector this summer, the State once again provided a sector-specific threat intelligence briefing through the Chief Cyber Office, NYSP, and DHSES with over 525 total attendees attended in a single day.

These ad hoc threat intelligence briefings are made possible through statewide threat intelligence gathering, analysis, and dissemination muscles that are routinely built through the State's cyber intelligence functions. Namely, NYSP New York State Intelligence Center (NYSIC) Cyber Analysis Unit (CAU) provides intelligence analysis and dissemination for critical infrastructure stakeholders across the state; NYSIC CAU provides various threat intelligence services and products, including timely advisories as well as regular digests of relevant advisories, notifications, and news relevant for the New York audience. Moreover, the New York State Office of Information Technology Services (ITS) operates the Joint Security Operations Center, which serves as a shared space for whole-of-government cyber threat intelligence exchange.

(4) Responsible AI Development

In June 2025, Governor Hochul signed the nation-leading Responsible AI Safety and Education (RAISE) Act to protect New Yorkers from emerging threats from frontier AI companies and their products, including cybersecurity risks.²⁸ Come November, large frontier AI developers will be statutorily required to register with the Office of Digital Innovation, Governance, Integrity and Trust (DIGIT) housed under the NYS Department of Financial Services (DFS) and comply with safety requirements. They include reporting of critical safety incidents to DIGIT within 72 hours; establishing and making publicly available safety and transparency frameworks; and filing quarterly risk

²⁸ https://www.dfs.ny.gov/reports_and_publications/press_releases/pr20251222

assessments to DIGIT. It also empowers the public to file suspected critical safety incident reports to DIGIT, which will be compiled into an annual public report.²⁹ The AI safety framework codified through the RAISE Act represents a proactive step in protecting New Yorkers from emerging threats from AI development, including autonomous cyberattacks, by requiring safety and transparency protocols to be implemented.

III. CONCLUSION

Advancing cybersecurity for New York means that all professions and leaders know what role they can play to protect our assets. Everyone has a part to play to ensure that New York continues to build resilience and reliability across the critical services on which New Yorkers rely everyday, like safe and reliable water. Given today's dynamic and volatile threat environment shaped by advances in AI, it's becoming that much more dangerous and challenging for our water and wastewater operators to defend against threat actors. In New York, they're not alone. In New York, they have clarity on what cybersecurity baselines should be and have access to the State's cyber defenders and investments to build their cybersecurity posture. In New York, we will continue to lead the nation in strengthening the state's cyber resilience by taking a sector-aware, whole-of-state cybersecurity strategy and framework to build up controls and fortifications in service of New Yorkers.

²⁹<https://www.governor.ny.gov/news/ai-safety-governor-hochul-announces-next-steps-regulate-major-ai-developers-and-protect-new>