FACT SHEET:
New York's First-Ever Cybersecurity Strategy

In New York's first-ever cybersecurity strategy, Governor Hochul outlines her plan for ensuring that New Yorkers continue to reap the benefits of the digital age while remaining protected from digital threats. The safe and secure functioning of the economy, critical infrastructure, and government services depends on our ability to protect digital infrastructure and sensitive information. However, the increasing sophistication and volume of global cyberattacks is raising the bar for what is necessary to successfully defend networks and systems from cyberattacks.

New York State's Chief Cyber Officer will oversee the implementation of the strategy, which will require continued teamwork and coordination between stakeholders, including the Federal government, state, tribal, and local governments, and the private sector.

A Vision for Statewide Cybersecurity

Today's cyber threats are marked by a convergence of criminal and nation-state actors. Nation-states increasingly rely on cyber criminals to execute state actions. Those criminals, in turn, continue to perpetrate crimes, aided by additional resources and technical capabilities. This blending of criminal and nation-state malicious activity has increased the magnitude and complexity of cyber threats.

The strategy seeks to ensure all New Yorkers are equally protected from digital threats by making New York more:

- ***Unified,*** by working to increase access to cybersecurity information, tools, and services so that the State's most sophisticated defenses are available to its least well-resourced entities.
- ***Resilient,*** by moving to expand the scope of cybersecurity regulations, requirements, and recommendations so that New York's critical infrastructure is better protected.
- ***Prepared,*** by providing advice and guidance to ensure New Yorkers are empowered to take charge of their own cybersecurity.

These measures will help to level the cybersecurity playing field and ensure that New York's security and resilience is greater than the sum of its parts.

This strategy also acknowledges that cybersecurity and resilience are collective public, private, and individual responsibilities. Breaches that span thousands of devices and multiple networks often come down to a single opened email or file. Every New Yorker has a role to play in cybersecurity, from an employee at a State agency to a resident seeking to access government services via the Internet.

Strategic Pillars

The strategy is composed of five mutually reinforcing strategic pillars that, taken together, will contribute to a defense that levels the cybersecurity playing field and ensures New York's cybersecurity and resilience is greater than the sum of its parts.

1. **Operate Government Networks Securely and Resiliently.** New York State Government systems and networks must be secure, resilient, and designed in accordance with modern security principles while delivering services and functioning efficiently.
2. **Collaborate with Key Stakeholders.** The State will continue to collaborate with key stakeholders, like city, county, and local governments, private sector partners, and non-profit organizations, including by continuing to offer shared cybersecurity services such as endpoint detection and response.
3. **Regulate Critical Industries.** New Yorkers must be able to trust that the critical infrastructure they rely on is secure from disruption by cyberattacks. Regulations ensure that critical infrastructure owners and operators are meeting, or exceeding, the minimum level of security necessary to protect the vital services they deliver. New York will continue to leverage its nation-leading financial services and energy grid cybersecurity regulations aligned with existing frameworks.
4. **Communicate Cybersecurity Advice and Guidance.** The State will continue to empower New York residents and businesses to take charge of their own cybersecurity, and to respond appropriately in a crisis. New York will continue amplifying the importance of cyber hygiene for individuals and communities.
5. **Grow New York's Cybersecurity Workforce and Economy.** The State is working to increase New York's cybersecurity talent pool both to keep New York a preferred hiring destination and to meet the demand for cybersecurity personnel in the private sector and governments throughout the State, including by continuing cybersecurity education and workforce development.

Building on Success

The strategy builds on steps the Governor has already taken to increase the cybersecurity and resilience of New York, including by:

- Providing $500M to enhance New York State healthcare IT and cybersecurity infrastructure as part of the Department of Health's health care technology capital grant programs.
- Increasing the State's centralized cybersecurity budget between FY2022 and FY2024, from roughly $20 million to over $90 million, including expanding funding for the shared services program for county and local governments; the shared services program has to date protected over 53,000 county and local government computers in nearly every upstate county and the largest 5 upstate cities.
- Allocating $7.4 million from the FY2024 budget to expand the New York State Police's Cyber Analysis Unit, Computer Crimes Unit, and Internet Crimes Against Children Center.
- Passing legislation in 2022 to create nation-leading cybersecurity protections for New York's energy grid by requiring electric distribution utilities to prepare for cyberattacks in their annual emergency response plans and providing the New York Public Service Commission (PSC) with enhanced auditing powers.
- Building a first-in-the nation Industrial Control System Cyber Assessment team as part of the statewide Cyber Incident Response Team at the Division of Homeland Security and Emergency Services.
- Creating the Joint Security Operations Center in partnership with the Mayors of Albany, Buffalo, New York City, Rochester, Syracuse, and Yonkers.
- Establishing the position of Chief Cyber Officer to serve as the principal advisor to the Governor for reducing cyber risk, managing significant cyber incidents, and increasing cyber resilience in New York State.