NEW YORK STATE

CYBERSECURITY GRANT PLAN

SEPTEMBER 2023

Approved by the New York State and Local Cybersecurity Grant Planning Committee
on September 22, 2023

Table of Contents

LETTER FROM THE COMMITTEE

The New York State and Local Cybersecurity Grant Planning Committee ("the Committee") is pleased to present the New York State Cybersecurity Grant Plan ("the Plan"). The goal of the Plan, developed in concert with State and local leaders, is to set forth initiatives to reduce cyber risk and build cyber resiliency in New York's state and local government entities.

Encompassing past accomplishments and future projects, this document serves to meet the administrative requirements of the State and Local Cybersecurity Grant Program (SLCGP). This Plan was developed in accordance with the requirements of the Fiscal Year 2022 U.S. Department of Homeland Security guidelines for the SLCGP and incorporates the required plan elements defined in the FY22 Notice of Funding Opportunity. The Plan does not create authority over any state or local entities or systems and is intended to serve as guidance for all New York governments.

Representatives from the State, county, city, town, village, and school districts, as well as experts in public health, public safety, and critical infrastructure were key in identifying and prioritizing initiatives designed to improve cybersecurity measures in state and local governments.

The Plan sets forth the following priorities for New York State:

- Understand New York's cybersecurity posture
- Enhance the resilience of state and local government technical environments
- Promote a culture of cyber awareness

As we continue to advance cybersecurity across New York, we must remain committed to improving our resilience through a range of disciplines and developing mechanisms to work across jurisdictional boundaries. This requires open and frequent communication among public, private, and nonprofit leaders in a true whole-of-state approach. The Committee works to achieve this goal through continuous dialogue among both practitioners and policymakers.

In August 2023, Governor Hochul released the first-ever New York State Cybersecurity Strategy that set forth an approach to cybersecurity and resilience based on the principles of unification, resilience, and preparedness. The Cybersecurity Strategy's five pillars –Operate, Collaborate, Regulate, Communicate, and Grow– informed the development of the Plan and are reflected throughout. As an administrative requirement of the SLCGP, the Plan not only represents another facet of New York State's extensive portfolio of cybersecurity measures that builds cybersecurity maturity among our critical institutions, but it is also an iterative effort designed to respond to the shifting needs of our state. As the cyber threat landscape is ever-changing, so shall this Plan evolve to ensure the continued advancement of State and local cybersecurity capabilities.

Chris DeSain
Chief Information Security Officer
New York State Office of Information
Technology Services

Alyssa Zeutzius
Deputy Chief Cyber Officer for Policy
Chair of New York State and Local
Cybersecurity Grant Planning Committee

INTRODUCTION

Developed in concert with state and local leaders, this Plan details current and future initiatives to reduce cyber risk and build cyber resiliency in New York's state and local government entities. While this is a multi-year Plan, it is a living document that will be reevaluated regularly based on the ever-evolving threat landscape, emerging technologies, and current needs.

This document serves to meet the administrative requirements of the SLCGP and incorporates the following required plan elements adapted from the FY22 Notice of Funding Opportunity:

- Manage, Monitor, and Track Assets
- Monitor, Audit, and Track Network Activity
- Enhance Preparedness
- Assess and Mitigate Infrastructure and Applications
- Leverage Best Practices and Methodologies
- Promote Safe, Recognizable Online Services
- Safeguard Continuity of Operations
- Grow the Workforce
- Assess and Protect Critical Infrastructure
- Prioritize Continuity of Communications and Data Networks
- Share Cyber Threat Indicator Information
- Promote and Use CISA Services
- Review Modernization Initiatives in Intergovernmental Systems
- Collectively Address Cybersecurity Risk and Develop Threat Strategies
- Address Gaps In Geographic Disparities (Rural)

Addressing cybersecurity in New York across a range of stakeholders with varying levels of authority and responsibilities requires multiple and simultaneous efforts. The Plan is one of a number of efforts in NYS all aimed at building cyber resiliency across the state. This Plan aligns with and references the following documents:

- New York State Cybersecurity Strategy
- New York State Technology Law
- NYS Statewide Technology Policies and Guidelines

Vision and Mission

The following presents the vision and mission for improving cybersecurity in New York through the SLCGP:

VISION

A unified and resilient cybersecurity approach throughout New York State governments to defend against threats.

MISSION

To expand access to cybersecurity information, tools, resources, and services so that the State's most sophisticated defenses are available to all public sector entities in New York.

Cybersecurity Grant Program Goals and Objectives

Throughout the period of performance, New York will utilize the SLCGP grant funds in support of the following goals and objectives:

Cybersecurity Grant Program	
Program Goal	**Program Objectives**
1. **Understand New York's overall cybersecurity posture**	1.1 Gain a comprehensive picture of the cybersecurity posture of critical infrastructure in New York State
	1.2 Understand the cybersecurity capabilities of local government entities
2. **Enhance the resilience of state and local government systems**	2.1 Increase local government adoption of fundamental cybersecurity best practices
	2.2 Enhance and expand cybersecurity services offered to local government entities
	2.3 Connect state and local government entities with free and low-cost cybersecurity resources and services
3. **Promote a culture of cyber awareness**	3.1 Increase knowledge, skills, and abilities of IT and security professionals at local government agencies
	3.2 Increase access to awareness-level training for local government entities

CYBERSECURITY PLAN ELEMENTS

Manage, Monitor, and Track Assets

New York State encourages state and local government entities to adopt cybersecurity best practices and tools related to the management, monitoring, and tracking of technology assets, including information systems, applications, and user accounts. State and local government entities should establish procedures that effectively control and restrict access to information assets to authorized users based on defined business and legal requirements, including limiting access to a "need-to-use" and/or "need-to-know" basis. To assist in this area, the NYS Office of Information Technology Services (ITS) has published a Local Government Cybersecurity Toolkit which includes Asset Inventory Guidance and Templates to help identify critical information assets and links to existing New York State Cybersecurity Policies, Standards and Guidelines that can serve as templates for local government policy, standards, and practices. Additional resources for local governments on various cybersecurity topics is provided on ITS's Local Government Cybersecurity webpage.

Monitor, Audit, and Track Network Activity

As part of New York State's cybersecurity Shared Services Program established in 2022, an endpoint detection and response (EDR) tool is made available at no cost to eligible local government entities to help them improve the monitoring, auditing, and tracking of network traffic and activity in their environments. As of August 2023, eligible entities include county governments and the cities of Albany, Buffalo, Rochester, Syracuse, and Yonkers.

Through the deployment and enhancement of these services and capabilities, the State can track malicious cyber activity and disseminate actionable information about that malicious activity as rapidly and widely as possible. The State builds its situational awareness of cyber threat activity through the New York Security Operations Center (NY SOC) - the statewide SOC managed by ITS - by monitoring State networks and systems, correlating alerts from county and local government networks provided via the State's Shared Services Program, and processing reports submitted to State agencies about malicious cyber incidents. The State leverages these mechanisms to create a statewide threat picture that feeds finished threat reporting which is disseminated statewide through the New York State Intelligence Center (NYSIC) to enhance the collective defense. Additionally, in 2022 the Joint Security Operations Center (JSOC) was formed in partnership with the State and the cities of Albany, Buffalo, New York City, Rochester, Syracuse, and Yonkers to facilitate the exchange of information and analytical collaboration among members. The State seeks to continue to refine and enhance the JSOC.

The State seeks to expand shared services and other capabilities through the SLCGP by increasing support for new and existing services and programs. The State will also continue to utilize, promote, and coordinate capabilities with organizations like the Multi-State Information Sharing and Analysis Center (MS-ISAC), Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), and other federal partners.

Enhance Preparedness

New York State has worked continuously to enhance preparedness measures for state networks, make best practices and other resources publicly available to state and local entities, and invest in programs that provide services to local governments to help them improve their own preparedness. New York State will seek to enhance and expand these capabilities and services to ensure state and local government entities have access to helpful guidance and can receive assistance when appropriate.

New York State's strategic approach to enhancing the preparation, response, and resiliency of information systems, applications, and user accounts against cybersecurity risks and threats includes:

- **Employee training:** Regular employee training and certifications on cybersecurity best practices, current threats, and use of deployed security tools can help ensure that all staff members are aware of potential risks and how to respond accordingly. An online Information and Cybersecurity Awareness Training designed for New York State employees is made available to local government entities at no cost to assist them in their efforts to increase cybersecurity awareness among their workforce. New York State will explore options to expand cybersecurity training resources for state and local government entities through the SLCGP.

- **Templates and guides:** Providing templates and guides about policy and plan development can help state and local government entities write successful incident response plans and other policies. Statewide technology policies and standards – including incident response plans – are published online for state and local government entities to utilize in their own IT and security programs. The Local Government Cybersecurity Toolkit published by ITS provides these types of resources for local governments, and the State will seek to further enhance such resources in the future.

- **Tabletop exercises:** Regularly conducting tabletop exercises can help identify potential vulnerabilities and improve incident response plans. The NYS Division of Homeland Security and Emergency Services (DHSES) Cyber Incident Response Team (CIRT) provides tabletop exercise services at no cost to eligible entities to help them prepare to respond to a cyber incident. The three-hour tabletop exercises facilitated by the DHSES CIRT are designed to walk each organization through a mock incident to test its cyber incident response plans and preparations and can help drive improvements in existing procedures. State and local government entities are also encouraged to leverage the CISA Tabletop Exercise Packages (CTEPs), MS-ISAC Tabletop Exercises, and other free resources to conduct their own exercises.

- **Comprehensive plans:** Developing comprehensive incident response plans, continuity of operations plans, business continuity plans, and disaster recovery plans can help ensure that an entity is prepared to respond to a wide range of potential threats. The State will continue to assist state and local government entities in developing, testing, and improving their plans.

- **Response:** New York State provides incident response assistance to government and critical infrastructure entities across the state. State Executive agencies are required to report incidents to the ITS Cyber Command, who provides incident response and remediation support. Local governments, non-Executive agencies, and public authorities can request assistance or report a cyber incident 24/7 by calling 1-844-OCT-CIRT (628-2478). DHSES CIRT offers remote or on-site support to eligible organizations. During a cyber incident, the team will provide "in the moment," incident-specific recommendations on containment, eradication, and recovery to reduce the impact of the disruption and help the organization to get back on its feet quickly. DHSES CIRT will also provide post-incident security recommendations, which can help organizations build a more proactive cyber program going forward. In addition, DHSES CIRT can provide analysis of systems or digital artifacts related to an active incident to help determine the root cause and provide remediation guidance. DHSES CIRT uses industry standard tools and offers forensics assistance that many government organizations may not have in-house. These free services are available for active incident response as well as proactive analysis of suspicious events.

- **Grant Funding:** As a component of the State Homeland Security Program (SHSP) and the Urban Area Security Initiative (UASI) under the Homeland Security Grant Program (HSGP), enhancing cybersecurity has been a focus of DHS/FEMA as part of the National Priority Areas and funding priorities. Additionally, administered by DHSES, the Cybersecurity Targeted Grant Program utilizes DHS-FEMA SHSP funds to provide a competitive grant opportunity for eligible local government organizations within NYS. These funds aid local jurisdictions by enhancing their ability to identify, protect, detect, respond to and recover from cyber incidents. A risk assessment tool utilizing the Center for Internet Security's (CIS) Critical Security Controls is embedded within the grant application and is designed to assist jurisdictions in assessing and prioritizing their cyber needs. Over the course of four funding cycles, over $5.5 million has been awarded to over 120 recipient organizations. The program is currently capped at $2 million per funding cycle given the demand for the program funds, and to help NYS meet the cybersecurity national priority area, as identified by DHS-FEMA.

Assess and Mitigate Infrastructure and Applications

New York State has developed programs and capabilities to help state and local government entities assess their vulnerabilities, identify gaps and weaknesses, and mitigate threats. New York State's strategic approach to implementing a process of continuous cybersecurity assessment and mitigation to address risks to information systems, applications, and user accounts includes:

- **Templates and guides:** Model policies, standards, and guidelines can help state and local government entities implement risk assessment and management processes. New York State's technology policies and standards are available online as resources for state and local government entities to model risk management best practices, including the **Information Security Policy** (NYS-P03-002), **Information Security Risk Management Standard** (NYS-S14-001), and **Vulnerability Management Standard** (NYS-S15-002).
- **Assessments:** The DHSES CIRT offers several assessment programs to help organizations improve their cybersecurity posture and reduce risk. The services outlined below are available at no cost to local governments, non-Executive State agencies, and public authorities.
    - **Cybersecurity Risk Assessments:** A joint effort between DHSES CIRT, the DHSES Critical Infrastructure (CI) Unit, and the Division of Military and Naval Affairs (DMNA), the Cybersecurity Risk Assessment program provides entities with actionable recommendations to improve their cybersecurity posture. The assessments have three phases: edge assessment, internal vulnerability assessment, and security program posture assessment. The final report from the assessment team consolidates vast amounts of threat and vulnerability information into a handful of action-oriented, prioritized findings for IT, business, and leadership teams to remediate. Additional information about this program and the assessment methodology can be found on the DHSES website.
    - **Phishing Assessments:** DHES CIRT provides a simulated phishing attack for eligible organizations to help them assess the effectiveness of their email security training. At the conclusion of a phishing engagement, targeted training with various learning modules, including modules that educate users on how to spot phishing messages can be provided. DHSES CIRT then delivers a report showing how many users were deceived by the phishing emails, to what extent they interacted with the suspect emails, and how many completed the training. Upon request, the phishing assessments can include an additional simulated phishing attack after the training to measure its effectiveness.
- **Shared Services**: As part of New York State's Shared Services Program, an endpoint detection and response (EDR) solution is offered to county governments in New York and the cities of Albany, Buffalo, Rochester, Syracuse, and Yonkers. The EDR solution provides the government entity continuous assessment of their endpoint vulnerabilities while automating remediation. New York State seeks to expand and enhance cybersecurity shared services and other capabilities for local governments through the SLCGP.

- **Federal Resources:** All state and local government entities in New York are encouraged to sign up for the free services offered by CISA and the MS-ISAC, including Cyber Hygiene (CyHy) Vulnerability Scanning and risk assessments.
    - **National Cybersecurity Review (NCSR):** To be eligible for receiving federal Homeland Security funding through DHS/FEMA, all New York State counties and urban areas are required to participate in the NCSR managed by the MS-ISAC. Initial analysis and assessment information is updated on an annual basis and provided to the stakeholder to help inform the development of cybersecurity planning efforts and projects.

Overall, the strategic approach to implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices is flexible, adaptive, and responsive to changing threats and risks.

Leverage Best Practices and Methodologies

The Statewide technology policies and guidelines published by ITS set standards and define best practices for the State's IT community. These policies, standards, and guidelines provide a comprehensive framework of security controls, best practices, technical standards, and implementation strategies that direct the design, deployment, and management of information security controls for the New York State. These documents are available online for all state and local government entities to reference in their own IT and security programs, and their adoption is encouraged across all levels of government.

Statewide policies, standards, and guidelines are applicable to all State Entities that use or access any ITS information technology resource, including systems managed or hosted by third parties on behalf of the ITS, and are derived from the controls defined by **NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations**. The State also uses the **CIS Critical Controls** framework for the evaluation and prioritization of implementation of security controls.

Whether based on **NIST Security and Privacy Controls**, **NIST CSF**, or **CIS Critical Security Controls**, the following best practices are shared with state and local government entities, and will inform project implementation considerations over the life of the SLCGP:

- Implementation of multi-factor authentication,
- Implementation of enhanced logging,
- Encryption for data at rest and in transit,
- Eliminating the use of unsupported/end of life software and hardware that are accessible from the Internet,
- Prohibition of use of known/fixed/default passwords and credentials,
- Enabling the ability to reconstitute systems (backups), and
- Migration to the .gov internet domain.

The State's approach to implementing each best practice is outlined below with references to the related ITS policy or standard included where applicable.

Implementation of multi-factor authentication

Through its Cybersecurity Targeted Grant Program, DHSES provides funding to local government entities to implement security controls including Multi-factor Authentication (MFA). DHSES will continue to work with local government entities to drive full adoption of MFA across their environment, and leverage SLCGP funds to do so.

Of the Statewide policies, standards, and guidelines referenced above, requirements for multi-factor authentication is covered by the **Authentication Tokens Standard** (NYS-S14-006), which establishes a framework for issuing and managing trusted identity credentials that aligns with the NIST SP 800-63-3 Digital Identity Guidelines. Statewide technology policies, standards, and guidelines are published online, and all state and local government entities are encouraged to adopt them across their organizations.

Implementation of enhanced logging

The State currently offers enhanced logging capabilities to county and local government entities through the EDR shared service. NYS engineers and support staff are continuing to work with local government entities to drive full adoption of this service across eligible participants. As a centralized State service, these logs are monitored and tracked 24/7 by analysts in the New York Security Operations Center (NY SOC).

Of the Statewide technology policies, standards, and guidelines referenced above, the requirement for enhanced security auditing and logging is covered by the **Information Security Policy** (NYS-P03-002) and **Security Logging Standard** (NYS-S14-005), which define requirements for security log generation, management, storage, disposal, access, and use based on NIST SP 800-92 Guide to Computer Security Log Management. Statewide technology policies, standards, and guidelines are published online, and all state and local government entities are encouraged to adopt them across their organizations.

Encryption for data at rest and in transit

Of the Statewide technology policies, standards, and guidelines referenced above, requirement for encryption of data at rest and in transit is covered by the **Encryption Standard** (NYS S14-007), which is based off of NIST SP 800-111, SP 800-131A, and 800-57 Part 1. Statewide technology policies, standards, and guidelines are published online, and all state and local government entities are encouraged to adopt them across their organizations.

Eliminating the use of unsupported/end of life software and hardware that are accessible from the Internet

The State encourages all state and local government entities to utilize CISA's Cyber Hygiene scanning services to continually evaluate their external network presence for accessible services and vulnerabilities. In addition, the EDR solution offered to eligible local government entities through the State's Shared Services Program provides the ability to detect some end-of-life software and hardware on internal and internet-facing devices.

The State's **Information Security Policy** (NYS-P03-002) states that any "system, software, or Operating System environment which is no longer supported and cannot be patched to current versions (e.g. end of life hardware/software) must be decommissioned and removed from service." Statewide technology policies, standards, and guidelines are published online, and all state and local government entities are encouraged to adopt them across their organizations.

Prohibiting the use of known/fixed/default passwords and credentials

Of the Statewide technology policies, standards, and guidelines referenced above, the requirement to change the default content of authenticators is covered by **Account Management/Access Control Standard** (NYS-S14-013), which is based on NIST Special Publication 800-63-3 Digital Identity Guidelines. Statewide technology policies, standards, and guidelines are published online, and all state and local government entities are encouraged to adopt them across their organizations.

Enabling the ability to reconstitute systems (backups)

Of the Statewide technology policies, standards, and guidelines referenced above, the requirement to maintain and test backup copies of information, software, and system images is covered by **Information Security Policy** (NYS-P03-002), which is based on NIST SP 800-53 and ICO/IEC 27002. Statewide technology policies, standards, and guidelines are published online, and all state and local government entities are encouraged to adopt them across their organizations.

Migration to the .gov internet domain

The **Domain Names for State Government Agencies Policy** (NYS-P08-003) sets a standard domain naming convention to be utilized by all state entity websites and requires that State agencies use only “ny.gov” domains. In addition, N.Y. County Law § 55 was amended in December 2022 to require any county that maintains a website to use a “.gov” domain name for such website. The law will go into effect on August 1, 2024.

Promote Safe, Recognizable Online Services

Ensuring that government services are safe and recognizable is critical in today’s digital world. All State agencies are required to use only “ny.gov” domains and all county governments must migrate to .gov by August 2024 per N.Y. County Law § 55.

The State has encouraged all local government entities to migrate their primary domains to the .gov Top-Level Domain (TLD), and while the domain is free through DHS/CISA, the State recognizes that migration can be costly due to technology changes and re-branding physical and digital assets.

Safeguard Continuity of Operations

Developing comprehensive incident response plans, continuity of operations plans, business continuity plans, and disaster recovery plans can help ensure that an entity is prepared to respond to a wide range of potential threats. The DHSES CIRT provides tabletop exercise services at no cost to eligible entities to help them prepare to respond to a cyber incident. The three-hour tabletop exercises facilitated by DHSES CIRT are designed to walk each organization through a mock incident to test its cyber incident response plans and preparations and can help drive improvements in existing procedures. The State will continue to assist state and local government entities in developing, testing, and improving their plans.

Grow the Workforce

Recruiting and retaining a skilled workforce is a well-documented challenge that both public and private sectors across the nation face. Once an employee is hired, entities must also ensure that all personnel are aware of the security and privacy risks associated with their roles. This includes understanding their responsibilities as well as applicable laws, regulations, executive orders, circulars, policies, standards, and procedures related to the security and privacy of state information and systems.

New York State continues to work with higher education institutions, including community colleges, to advance cybersecurity and technology education across the state. In addition, State agencies continue to invest in training programs to provide students with real-world experience. For example, the internship program at ITS provides students attending State University of New York (SUNY) and City University of New York (CUNY) campuses with an opportunity to gain marketable skills, industry certifications, and hands-on experience to complement their academic studies across a variety of IT and security roles.

New York State provides an Information and Cybersecurity Awareness Training to State employees which is also made available online to local government entities at no cost. The State will explore options to expand cybersecurity training resources for state and local government entities through the SLCGP.

Prioritize Continuity of Communications and Data Networks

New York State has put forth a strategic plan to improve the resiliency of communication and data networks, helping to ensure that these critical systems remain available to deliver vital government services. ITS leads these efforts through their cybersecurity remediation plan, a multi-year program initiated in 2023. This plan will reduce vulnerabilities by eliminating legacy technology and leveraging current best practices for robust and secure connectivity between systems and networks. Building on the improvement of network controls, increased monitoring through the Shared Services Program and additional analytical collaboration of the JSOC also helps ensure the availability of networks as does increased security training for technical staff. Tabletop exercises are performed to test, update, and improve incident communications and procedures involving business continuity and recovery of New York State networks.

Assess and Protect Critical Infrastructure and Key Resources

DHSES currently provides risk assessments to critical infrastructure entities throughout the state. These assessments evaluate both the physical security and IT security posture of participating entities. In the coming year, DHSES will develop and deploy a specialized Industrial Control System Cyber Assessment team that will focus on the security of operations technology systems in select critical infrastructure operators in New York.

Share Cyber Threat Indicator Information

To effectively disrupt cyber threats to New York, the State must track malicious cyber activity and disseminate actionable information about that malicious activity as rapidly and widely as possible. To accomplish these twin objectives, the State is working closely with county and local governments to gain insights into threats to their networks and is refining its methods for sharing threat information.

New York State builds its cybersecurity situational awareness by:

- Monitoring State networks and systems;
- Monitoring alerts from county and local government networks provided via the State's Shared Services Program;
- Processing reports submitted to State agencies about malicious cyber incidents; and
- Distributing cyber threat information from federal and state entities whose mission it is to gather and distribute cyber intelligence.

New York State leverages these mechanisms to create a statewide threat picture that is directly accessible to county and local government participants in the State's Shared Services Program and that feeds finished threat reporting which is disseminated statewide.

The New York State Intelligence Center (NYSIC), a multi-agency fusion center, serves as the hub for the dissemination of finished cyber threat reporting. The NYSIC was established to collect, analyze, and disseminate intelligence related to criminal and terrorist activities, including in cyberspace, and to enhance information sharing and collaboration among federal, state, local, and tribal law enforcement agencies, as well as private sector partners.

Department Agreements

New York State entities, specifically those with the mission to curate and disseminate intelligence information, will continue to work with local government entities to share cyber threat information through established channels and agreements as necessary and feasible.

Promote and Use CISA Services

New York State will continue to support, promote, and utilize CISA's risk and vulnerability services and encourage all SLCGP recipients to enroll in Vulnerability Scanning, Web-Application Scanning, and Cyber Hygiene Services as appropriate.

In addition, New York State supports state and local government participation in the NCSR. The results of these assessments help inform local governments in their development of cybersecurity planning efforts and projects.

CISA's Region 2 personnel are heavily engaged across New York and work closely with both state and local government entities on a regular basis.

Review Information Technology and Operational Technology Modernization Efforts

As part of a continual cycle of modernization efforts, New York State regularly identifies, upgrades, and replaces aging IT/OT infrastructure and legacy systems. These modernization efforts provide an opportunity to eliminate reliance on older, dated technology while also helping to ensure that NYS systems and infrastructure are also aligned with current best practices and security controls.

Collectively Address Cybersecurity Risk and Develop Threat Strategies

The Committee should utilize this Plan and operate under its approved charter to develop and coordinate strategies to address cybersecurity risks and cybersecurity threats with other organizations, including consultation with local governments and associations of local governments.

Specifically, a significant portion of the Committee membership is IT and security leadership from various local government entities, including counties, cities, and towns, to ensure input from stakeholders at all levels of local government. In addition, the Committee includes representatives from the New York State Local Government Information Technology Directors' Association (NYSLGITDA), Madison-Oneida Board of Cooperative Educational Services' Mohawk Regional Information Center (MORIC), and the Greater New York Hospital Association to solicit and receive input and feedback from their respective members.

While the Committee plays a key role in bringing together stakeholders, New York has historically had a strong set of formal and informal relationships among state and local governments. State agency cyber leaders take part in the State Cyber Steering Committee and many local government technology leaders participate in the New York State Local Government Information Technology Directors' Association (NYSLGITDA). Both examples have presented a way for information sharing and shared decision making to collectively address cyber threats across the state.

Address Gaps in Geographic Disparities (Rural)

Per the Homeland Security Act of 2002, a rural area is defined in 49 U.S.C. § 5302 as an area encompassing a population of less than 50,000 people that has not been designated in the most recent decennial census as an "urbanized area" by the Secretary of Commerce.

In accordance with the SLCGP FY22 Notice of Funding Opportunity (NOFO) and the IIJA, NYS will ensure at least 80 percent of the funds (dispersed in a range of mechanisms including statewide contacts for cyber goods and services) are targeted and allocated to local government organizations, with at least 25 percent of that 80 percent allocated to local government entities in rural communities. Rural communities are assured adequate access to projects under the SLCGP by virtue of their representation on the Committee and outreach that will be done by the State Administrative Agency (SAA) and the DHSES CIRT.

GRANT FUNDING DETERMINATIONS

The program has several key initiatives that will leverage existing state programs as well as previous federal Homeland Security investments to help local governments mature their cybersecurity.

As there are over 2,300 entities eligible for funding through this program, it is not feasible for each of those entities to completely secure their technical environment with the money available to New York. Therefore, New York State intends to establish four key initiatives for the first year of funding that will provide the most value to meaningfully strengthen cybersecurity across the state with the limited amount of funds available. These efforts include:

- Multi factor authentication services for any eligible entity
- Cybersecurity certification for IT personnel who carry out cyber functions
- General cybersecurity awareness and anti-phishing training
- Industrial control systems (ICS) risk assessment of municipal energy providers

Funding for subsequent years will be determined each funding cycle in accordance with the requirements of the grant. Year one initiatives are detailed in **Appendix B: Project Summary Worksheet**.

Distribution to Local Governments

New York State intends to use the funds received through the SLCGP to establish statewide contracts for the services listed above and as described in the **Appendix B: Project Summary Worksheet**.

Due to the large number of entities eligible for this grant, New York State does not intend to provide sub-grants or direct pass through of funds for the first year of funding. In lieu of passing through funds to each eligible entity in nominal amounts of less than $3,000 in year one, New York State intends to use the funds strategically to provide services to help eligible entities meaningfully improve cybersecurity.

In accordance with the SLCGP FY22 NOFO and the IIJA, NYS will ensure at least 80 percent of the funds are allocated to contracts for offerings to local governments with at least 25 percent of that 80 percent allocated to provide services to local government entities in rural communities. The SAA will retain 5 percent of the grant for management and administration.

CAPABILITY ASSESSMENT

New York State's approach to assessing capabilities is currently based on data collected from three efforts:

- DHSES cyber grant administration process (local governments provide a self-assessment for cybersecurity)
- Nationwide Cybersecurity Review (NCSR)
- A cyber assessment survey focused on the 16 required elements of this Plan and administered to NYS local governments for the purposes of gathering data for this grant

The data collected in these efforts, along with the informal information sharing that takes place in state and local government conferences, meetings, and workshops, make up the current assessment of capabilities. There will be a continual effort to gather information on current cybersecurity capabilities among all local governments. A pre-assessment of local government capabilities measured before the implementation of this Plan can be found in **Appendix A: Cybersecurity Grant Plan Capabilities Pre-Assessment**.

IMPLEMENTATION APPROACH

Organization, Roles, and Responsibilities

In New York, cybersecurity is a shared responsibility. The following are the organizations within the state and their respective cyber roles and responsibilities:

- New York State Office of Information Technology Services (ITS). ITS operates State networks on behalf of many executive agencies. The ITS Chief Information Security Officer (CISO) provides cybersecurity support and assistance to agencies, conducts around-the-clock cybersecurity monitoring and operations, manages an incident response team, and promulgates policies, standards, and programs relating to cybersecurity and resilience.

- New York State Division of Homeland Security and Emergency Services (DHSES). DHSES provides leadership, coordination, and support to prevent, protect against, prepare for, respond to, recover from, and mitigate disasters and other emergencies. DHSES is responsible for working with Federal, state, local, and private entities to protect the State's critical infrastructure from cyber threats and vulnerabilities and to coordinate and facilitate information sharing and intelligence amongst these entities to assist in the early detection of, and response to, natural and man-made disasters. DHSES is also the State Administrative Agency (SAA) for FEMA grants.

- New York State Police (NYSP). The NYSP operates the New York State Intelligence Center (NYSIC), a multi-agency, all-crimes fusion center that identifies, prevents, and protects New York against threats. The NYSIC Cyber Analysis Unit (CAU), provides cyber threat intelligence, outreach, analysis, and support. NYSP also operates the Computer Crime Unit (CCU), which provides outreach and education to community groups, training to law enforcement agencies, and administers the Internet Crimes Against Children Task Force (ICAC), which identifies, investigates, and prosecutes individuals who use the internet and technology to exploit children.

- New York State Division of Military and Naval Affairs (DMNA). DMNA is the State's executive agency responsible for managing New York's Military Forces, including its Cyber Protection Team (CPT). The CPT is jointly staffed and managed by the New York and New Jersey National Guard in support of State and Federal missions. DMNA also provides full-time State Active Duty Service Members to augment and coordinate training, security assessments, and incident responses for government agencies and critical infrastructure.

- New York State Chief Cyber Officer. The Chief Cyber Officer reports to the Director of State Operations and Infrastructure and is the principal advisor to the Governor for reducing cyber risk, managing significant cyber incidents, and increasing cybersecurity and resilience in New York State.

- County and local governments. County and local governments are responsible for the cybersecurity and resilience of their own information technology environments. They partner with the State, industry, non-profits, and other local governments to share threat information and best practices. They can expect the State to collaborate with them to disrupt malicious cyber actors, provide grant funding to modernize their information technology environments, and, when requested or directed, provide cyber support.

- School Districts. Some school districts maintain and operate their own networks and systems, while many others receive a range of technology services through the Boards of Cooperative Educational Services (BOCES) and NYS Regional Information Centers (RICs). Some of the 37 BOCES provide shared educational programs and services to school districts within the state, including technology services to support instructional technology through planning, purchasing, installation, and technical support. The 12 RICs each offer a range of services from classroom tools that optimize student achievement to support for administrative systems, data analysis, integration and verification, technology integration, and general technical support.

- Critical infrastructure owners and operators. Critical infrastructure operators manage their own systems and networks and are responsible for their own cybersecurity and resilience. They can expect the State to collaborate with them to disrupt malicious cyber actors, regulate them to ensure the security of critical services New Yorkers rely on, and, when requested or directed, provide cyber support.

- State Board of Elections. The New York State Board of Elections (NYSBOE), as a bipartisan agency vested with the responsibility for administration and enforcement of all laws relating to elections in New York State. As part of their leadership in NYS, NYSBOE has offered grants and provided funding for statewide contracts for cybersecurity good and services. In addition, NYSBOE set forth cybersecurity regulations for all county election departments.

The New York SLCGP Planning Committee Charter establishes the roles and responsibilities of the Committee in developing, approving, implementing, monitoring, reviewing, and revising a Plan that establishes goals, objectives, and funding priorities to ultimately reduce cyber risk within and across New York's state and local government organizations in accordance with the requirements of the IIJA and the SLCGP NOFO.

As the SAA for the SLCGP, DHSES is responsible for meeting the administrative requirements of the grant program. DHSES Grants Program Administration (GPA) is responsible for the management and administration of the SLCGP in compliance with eligible activities as outlined in the NOFO and award terms and conditions.

While this Plan fosters the principles of a whole-of-state or collective defense model, it also recognizes the authorities, roles, and responsibilities of individual state and local government entities in New York. Each organization is responsible and primarily accountable for maintaining its own cybersecurity program and executing day-to-day security and IT management functions of the information systems and networks under its respective purviews. Each state and local government entity is responsible for establishing its own risk tolerance threshold while also applying administrative, physical, and technical controls and safeguards in accordance with such thresholds. The funds, services, equipment, and software that may be provided to these entities through the SLCGP do not usurp or supplant their authorities or responsibilities. They are intended to augment the entity's resources to help reduce cyber risk, strengthen their security postures, and make them more resilient to current and emerging threats.

Resource Overview and Timeline Summary

As the SAA, DHSES GPA will provide the necessary resources to oversee management and administration of the SLCGP.

The timeline for the 2022 funding cycle will be dependent on when New York's Plan is submitted and how long it takes FEMA/CISA to approve the Plan and associated projects. The estimated activities associated with the grant are as follows:

Step	Activity
1	Submission of the New York State Cybersecurity Grant Plan
2	FEMA/CISA approval of New York State Cybersecurity Grant Plan
3	Grant applications available to eligible NY entities
4	Grant application submissions due
5	Applications evaluated and grant recipients notified
6	Grant agreements executed with recipients
7	Submission of revised Investment Justifications to FEMA
8	FEMA releases funds
9	Services/tools deployed to recipients

METRICS

Cybersecurity Grant Program			
Program Goal	**Program Objectives**	**Metric Description**	**Outcome**
Understand New York's overall cybersecurity posture	1.1 Gain a comprehensive picture of the cybersecurity posture of critical infrastructure in New York State	• Synthesis of data collected from NCSR, grant applications, and other methods conducted over the period of performance • Number of New York critical infrastructure entities receiving goods or services through SLCGP funds	[To be filled out after year 1]
	1.2 Understand the cybersecurity capabilities of local government entities	• Synthesis of data collected from NCSR, grant applications, and other methods conducted over the period of performance • Number of New York local government entities receiving goods or services through SLCGP funds	
Enhance the resilience of state and local government systems	2.1 Increase local government adoption of fundamental cybersecurity best practices	• Number of MFA licenses deployed to local government entities	
	2.2 Enhance and expand cybersecurity services offered to local government entities	• Number of local government employees completing cybersecurity awareness training • Number of New York entities completing the NCSR • Number of New York entities enrolled in CISA's Cyber Hygiene (CyHy) service	
	2.3 Connect state and local government entities with free and low-cost cybersecurity resources and services	• NYS local governments continuing to use DHSES CIRT proactive and reactive services • Number of New York entities registered with MS-ISAC • Number of New York entities enrolled in CISA CyHy service • Number of New York entities completing the NCSR	

Cybersecurity Grant Program			
Program Goal	**Program Objectives**	**Metric Description**	**Outcome**
Promote a culture of cyber awareness	3.1 Increase knowledge, skills, and abilities of IT and security professionals at local government agencies	• Number of local government IT and cybersecurity employees enrolled in cybersecurity certification course	[To be filled out after year 1]
	3.2 Increase access to awareness-level training for local government entities	• Number of local government employees completing cybersecurity awareness training	

APPENDIX A: CYBERSECURITY GRANT PLAN CAPABILITIES PRE-ASSESSMENT

As mentioned previously in the ***Capability Assessment*** section, the State has collected a sampling of the cybersecurity maturity of local government entities across the state through several efforts. Below is a table aligning the plan elements with a capability level of local government entities across the state (based on sample population data) along with the project # of the investment proposed in this Plan to help mature the capability level at the local level.

Cybersecurity Plan Required Elements	**Select capability level from:** Foundational Fundamental Intermediary Advanced	**Project # (s)** (If applicable – as provided in Appendix B)
1. Manage, monitor, and track information systems, applications, and user accounts	Fundamental	1
2. Monitor, audit, and track network traffic and activity	Foundational	1
3. Enhance the preparation, response, and resiliency of information systems, applications, and user accounts	Foundational	1, 2, 3, 4
4. Implement a process of continuous cybersecurity risk factors and threat mitigation practices prioritized by degree of risk	Foundational	1, 2, 3, 4
5. Adopt and use best practices and methodologies to enhance cybersecurity (references NIST)	-	-
a. Implement multi-factor authentication	Fundamental	1
b. Implement enhanced logging	Foundational	
c. Data encryption for data at rest and in transit	Foundational	
d. End use of unsupported/end of life software and hardware that are accessible from the Internet	Foundational	2
e. Prohibit use of known/fixed/default passwords and credentials	Foundational	2
f. Ensure the ability to reconstitute systems (backups)	Foundational	
g. Migration to the .gov internet domain	Foundational	

6. Promote the delivery of safe, recognizable, and trustworthy online services, including using the .gov internet domain	Foundational	1, 2, 3, 4
7. 7. Ensure continuity of operations including by conducting exercises	Foundational	2, 3, 4
8. Identify and mitigate any gaps in the cybersecurity workforces, enhance recruitment and retention efforts, and bolster the knowledge, skills, and abilities of personnel (reference to NICE Workforce Framework for Cybersecurity)	Foundational	2, 3, 4
9. Ensure continuity of communications and data networks in the event of an incident involving communications or data networks	Foundational	2, 4
10. Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the eligible entity	Foundational	1, 2, 3, 4
11. Enhance capabilities to share cyber threat indicators and related information between the eligible entity and the Department	Foundational	2, 4
12. Leverage cybersecurity services offered by the Department	Fundamental	1, 2, 3, 4
13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives	Foundational	2, 4
14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats	Foundational	1, 2, 3, 4
15. Ensure rural communities have adequate access to, and participation in plan activities	Foundational	1, 2, 3, 4
16. Distribute funds, items, services, capabilities, or activities to local governments	Intermediate	1, 2, 3, 4

APPENDIX B: PROJECT SUMMARY WORKSHEET

The **Project Summary Worksheet (Year 1)** is a list of cybersecurity projects that the entity plans to complete in year 1 to develop or improve cybersecurity capabilities of state and local government entities.

Project Name	Project Description	Related Required Element #	Cost	Status	Priority	Project Type
1. Multi-Factor Authentication Contract	The State will leverage economies of scale to procure a MFA solution to provide to eligible local government entities. The State will seek a vendor who can offer flexible MFA solutions (hardware and software tokens) and professional services to assist entities with deployment/configuration.	1, 2, 3, 4, 5a, 6, 10, 12, 14, 15, 16	TBD	Action Pending Plan Review	High Priority	Equip
2. Scholarship for cybersecurity certification for local government professional	Grant funds will be utilized to provide cybersecurity training and certification exam vouchers to IT and cybersecurity employees at eligible local government entities (likely CompTIA Security+).	3, 4, 5d, 5e, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	TBD	Action Pending Plan Review	Medium Priority	Train
3. Cyber awareness and phishing campaign training	The State will leverage economies of scale to procure licenses for a security awareness and phishing training platform to provide to eligible local governments. Eligible local governments will be able to enroll their employees in security awareness and phishing training.	3, 4, 6, 7, 8, 10, 12, 14, 15, 16	TBD	Action Pending Plan Review	Medium Priority	Train
4. Industrial Control Systems (ICS) risk assessment	Using the State's portion of funds, DHSES OCT will assess municipal energy providers statewide.	3, 4, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	TBD	Action Pending Plan Review	Medium Priority	Evaluate

APPENDIX C: ENTITY METRICS

The metrics below will be used to measure implementation of this plan.

Cybersecurity Grant Plan Metrics			
Planning Goal	**Plan Objectives**	**Associated Metrics**	**Metric Description**
1. New York has an approved Cybersecurity Grant Plan that meets the SLCGP requirements as defined in the FY22 NOFO	1.1 Draft the Plan	Draft Plan is approved by SAA	SAA reviews and approves draft Plan
	1.2 Committee approves Plan	Plan signed by CISO	Committee meeting minutes
	1.3 Submit the Plan to CISA	Confirmation of Receipt	Email from CISA
	1.4 CISA Approves Plan	Statement of Approval	Email from CISA
2. Receive funding from SLCGP	2.1 Funding received to Execute approved projects	Receipt of funds	Accept funds
3. Execute procurement process for each approved project	3.1 Execute approved projects	Projects are invoiced and paid	Financial Reporting via SAA
	3.2 Closeout approved projects	Projects are terminated or renewed	Financial Reporting via SAA
4. Process services to local entities	4.1 Enroll local entities in services	Number of entities enrolled in each approved project	Financial Reporting via SAA
5. Review, revise, and update the Plan for next FY, if needed	5.1 Repeat Objectives for Goal 1 for subsequent FY	See Goal 1	See Goal 1

01001110
01011001
00001010

01110
11001
01010

NEW
YORK
STATE

01001110
01011001
00001010