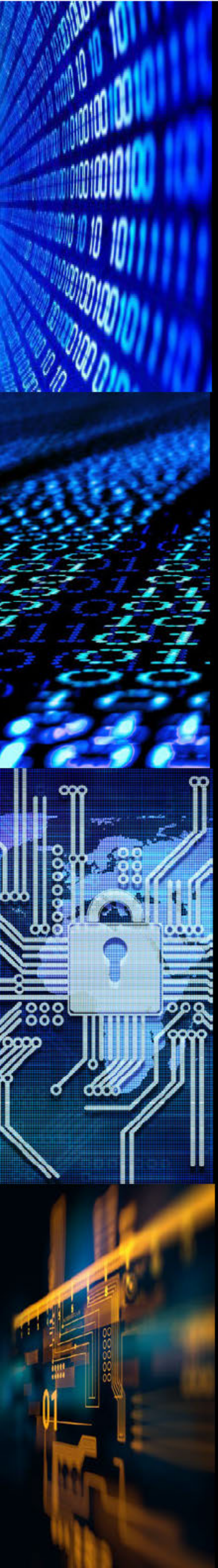

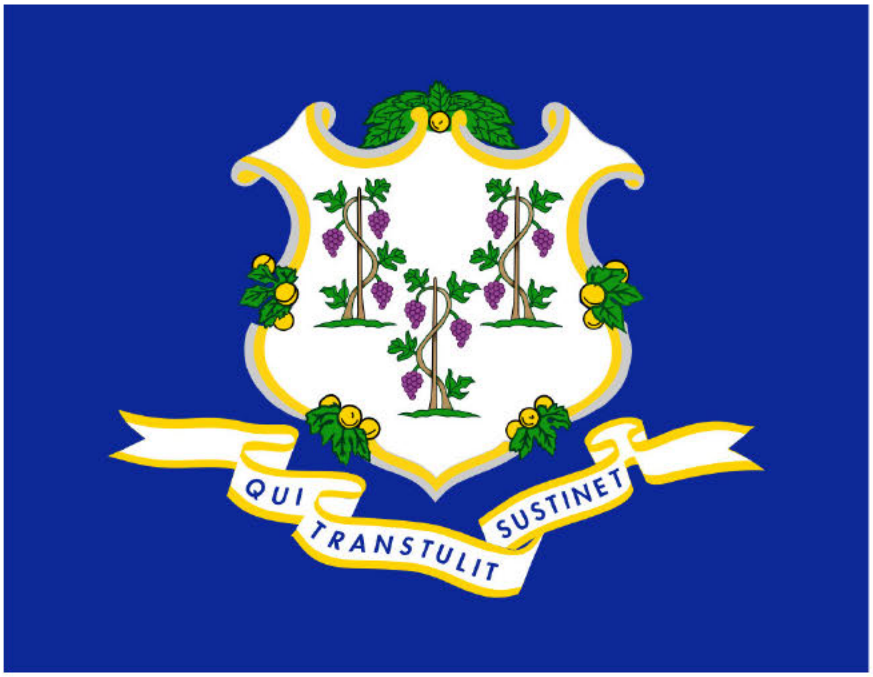

# STATE OF CONNECTICUT CYBERSECURITY PLAN

August 2023

Approved by Connecticut SLCGP Planning Subcommittee on August 28, 2023

Version 2.0

*THIS PAGE INTENTIONALLY LEFT BLANK*

# TABLE OF CONTENTS

# LETTER FROM STATE OF CONNECTICUT SLCGP PLANNING SUBCOMMITTEE

Greetings,

The State and Local Cybersecurity Grant Planning (SLCGP) subcommittee for the State of Connecticut is pleased to present to you the 2023 Connecticut Cybersecurity Plan. The Cybersecurity Plan represents Connecticut's continued commitment to improving cybersecurity and supporting our State, as well as cybersecurity practitioners across our local jurisdictions. In addition, this update meets the requirement of the current U.S. Department of Homeland Security guidelines for the State and Local Cybersecurity Grant Program (SLCGP).

Representatives from the Cyber Security Grant Planning Subcommittee collaborated to develop and update the Cybersecurity Plan with actionable and measurable goals and objectives that have champions identified to ensure completion. These goals and objectives focus on leveraging economies of scale to implement programs that directly benefit government entities within the state. They are designed to support our entity in planning for new technologies and navigating the ever-changing cybersecurity landscape. They also incorporate the SLCGP required plan elements.

As we continue to enhance cybersecurity, we must remain dedicated to improving our resilience among disciplines and across jurisdictional boundaries. With help from cybersecurity practitioners, we will work to achieve the goals set forth in the Cybersecurity Plan and become a model for cyber resilience.

Sincerely,

Jeffrey W. Brown
Chief Information Security Officer, State of Connecticut
DAS/BITS

Mark Raymond
Chief Information Officer, State of Connecticut
DAS/BITS

Brenda M Bergeron

Brenda M. Bergeron
Deputy Commissioner
CT Department of Emergency Services and Public Protection
Division of Emergency Management and Homeland Security

# INTRODUCTION

The Cybersecurity Plan is a three-year strategic planning document that contains the following components:

- **Vision and Mission:** Articulates the vision and mission for improving cybersecurity resilience over the next one-to-three-years.
- **Organization, and Roles and Responsibilities:** Describes the current roles and responsibilities, and any governance mechanisms for cybersecurity within Connecticut as well as successes, challenges, and priorities for improvement. This also includes a strategy for the cybersecurity program and the organization structure that identifies how the cybersecurity program is supported. In addition, this section includes governance that identifies authorities and requirements of Connecticut's cybersecurity program. The Cybersecurity Plan is a guiding document and does not create any authority or direction over any of the State's local systems or agencies.
- **How feedback and input from local governments and associations was incorporated.** Describes how inputs from local governments are used in order to reduce overall cybersecurity risk across the eligible entity. This is especially important in order to develop a holistic cybersecurity plan.
- **Cybersecurity Plan Elements:** Outlines technology and operations needed to maintain and enhance resilience across the cybersecurity landscape.
- **Funding:** Describes funding sources and allocations to build cybersecurity capabilities within the State of Connecticut along with methods and strategies for funding sustainment and enhancement to meet long-term goals.
- **Implementation Plan:** Describes the State of Connecticut's plan to implement, maintain, and update the Cybersecurity Plan to enable continued evolution of and progress toward the identified goals. The implementation plan must include the resources and timeline where practicable.
- **Metrics:** Describes how the State of Connecticut will measure the outputs and outcomes of the program across the entity.

The National Institute of Standards and Technology (NIST) Cybersecurity Framework[1], included in Figure 1, helps guide key decision points about risk management activities through various levels of an organization from senior executives to business and process level, as well as implementation and operations.

[1] https://www.nist.gov/cyberframework/getting-started

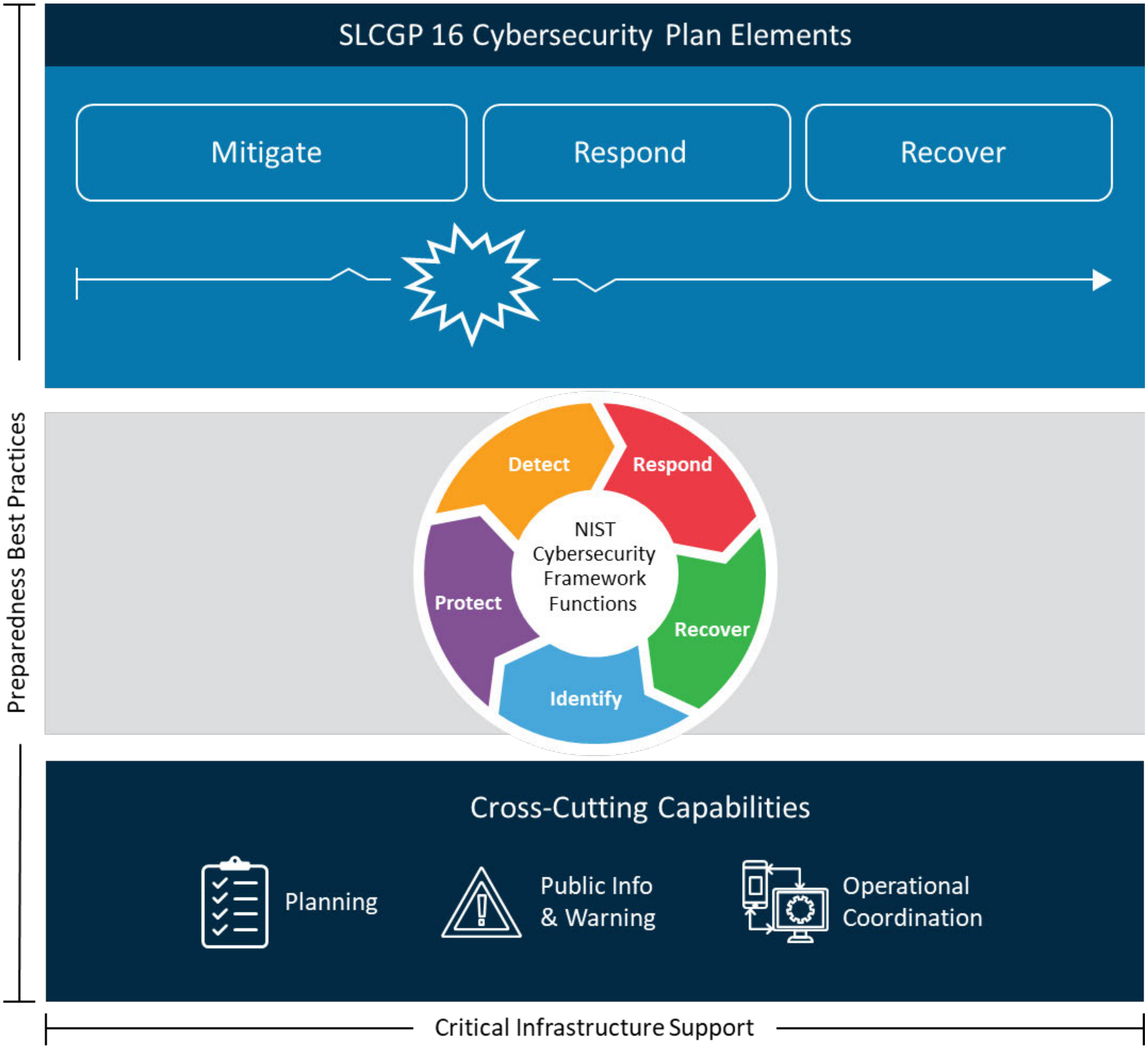
SLCGP 16 Cybersecurity Plan Elements
Mitigate
Respond
Recover
Preparedness Best Practices
Detect
Respond
NIST Cybersecurity Framework Functions
Protect
Recover
Identify
Cross-Cutting Capabilities
Planning
Public Info & Warning
Operational Coordination
Critical Infrastructure Support

*Figure 1: Achieving Cyber Resilience Through Comprehensive Cybersecurity Plans*

## Vision and Mission

This section describes the State of Connecticut SLCGP vision and mission for improving cybersecurity:

**Vision:**

*Work as an inclusive collaborative team to implement risk-based cybersecurity initiatives to improve cybersecurity resilience in the State of Connecticut.*

**Mission:**

*Apply a sustainable, risk-based approach to ensure SLCGP funding is used to improve cyber resilience, protect critical infrastructure and information technology resources, secure critical data, and safeguard the privacy of Connecticut citizens and those that do business with the state, municipalities, school districts, and other local government entities.*

## Cybersecurity Program Goals and Objectives

The State of Connecticut's cybersecurity goals and objectives include the following:

| Cybersecurity Program | |
|---|---|
| **Program Goal** | **Program Objectives** |
| Improve State and Local Entity's capability and capacity to adopt and use best practices and methodologies to enhance cybersecurity. | Improve and refine SLGCP Cybersecurity Plan to serve as the foundational strategy for future funding and cybersecurity improvements across the state. |
| | Identify and approve strategic projects and/or categories of projects that meet the objectives of the cybersecurity plan and the cybersecurity grant. |
| Investigate centralized efforts that help enhance cybersecurity for all state government entities and provide assessment of cybersecurity implementations to eligible subentities for continued improvement and funding prioritization. | Investigate Connecticut Education Network (CEN) and the Public Safety Data Network (PSDN) as a central point that could benefit many state government and education entities by implementing a statewide security operations center (SOC). |
| | Investigate other centralized services that could benefit any government educational entity within the state. |
| | Support and expand assessments being conducted by the Connecticut National Guard |
| Identify and address cybersecurity implementation gaps and prioritize projects commensurate with risk. | Make SLCGP funding available to eligible subentities to enhance cybersecurity protection based on assessments and gaps identified. |
| Identify and establish a cybersecurity training program for state and local cybersecurity practitioners. | Provide training and professional development for frontline cybersecurity professionals to enhance preparedness, response, and recovery skills at the subentity level. |

# CYBERSECURITY PLAN ELEMENTS

This plan incorporates the following plans:

- State of Connecticut Cybersecurity Strategy (March 2022). This document outlines the cybersecurity strategy previously developed with a whole-of-government perspective.
- Connecticut Cyber Disruption Response Plan (CDRP, 2018. This document is a comprehensive plan for consequence management following a significant cyber incident in the state of Connecticut.

## Manage, Monitor, and Track

The State of Connecticut will investigate the following options to enhance the security and resilience of information systems, applications, and user accounts. We will develop and implement a robust asset management framework to provide a comprehensive view of hardware, software, and services. That state currently performs centralized vulnerability management and systems inventory tracking for tracking hardware, software and services. This will be complemented by continuous risk assessments, focusing on identifying and evaluating potential vulnerabilities, especially in legacy systems. Advanced monitoring and tracking mechanisms, such as SIEM systems, IDS, and EDR tools, will be employed to detect and respond to potential security incidents promptly. We will leverage existing incident response and recovery plans. We will also foster a culture of cybersecurity awareness by providing regular training and educational resources for employees and residents.

## Monitor, Audit, and Track

The State of Connecticut will focus on a largely centralized approach to monitoring, auditing and tracking by leveraging the Connecticut Education Network (CEN) and making services available to all public sector subscribers. We will continue to leverage and encourage the use of the MDBR and MDBR+ service from MS-ISAC as well as adding additional Albert sensors to address any gaps in visibility.

Continuous monitoring and timely identification of potential threats are critical components of an effective cybersecurity strategy. By centralizing monitoring and tracking through a security operations center (SOC) and aligning policies and procedures with the latest security best practices, state entities can better protect against cybersecurity threats and mitigate the risk of data breaches and other security incidents. We will explore a state-level SOC to centralize the monitoring, auditing, and tracking of network traffic and activity to ensure that our systems and networks are continuously monitored and that any potential threats are identified and addressed as soon as possible.

We will additionally establish a comprehensive set of security policies and procedures that govern the use of state-wide networks and systems. These policies and procedures will be aligned with the latest security best practices. Applicable guidance will be made available for local government upon request from the DAS/BITS organization and be communicated via the Connecticut monthly Cyber Security Committee Meeting and disseminated through the ESF17 working groups of the five emergency planning regions of the Connecticut Division of Emergency Services and Homeland Security. The five DEMHS Regions each have a regional emergency planning team (REPT) made up of representatives from each municipality or tribe in the region and representatives from the different emergency support functions (ESF). The state and the municipalities have adopted an ESF-17 cyber security structure to share in forming best practices and emerging issues.

We are also currently supporting State government vulnerability scanning processes, Albert sensors for state elections, and distributed denial of service (DDoS) protection services for any entity using CEN for Internet services.

Our strategic approach emphasizes collaboration with federal, state, tribal and local partners, such as MS-ISAC and CISA, fostering a cooperative environment for information sharing. To complement our technical measures, we will implement regular training and cybersecurity awareness programs for state, tribal and municipal employees and end-users, ensuring that all stakeholders are well-equipped to identify, report, and respond to potential security threats effectively.

## Enhance Preparedness

The State has developed a comprehensive cyber incident response plan with procedures for identifying and mitigating threats, established an incident response team composed of experts from various departments, implemented a training and awareness program for employees, partnered with federal agencies for expert resources, conducted regular exercises to test the effectiveness of the plan, and implemented security measures such as intrusion detection systems. This multifaceted approach is designed to be proactive to protect systems against potential threats and ensure efficient responses in the event of an incident. This strategy includes encouraging individual state and local entities to create tailored incident response procedures and making policies available upon request. The State Cyber Incident Response Plan was provided to municipalities as a template and will be updated as needed. We would also like to make applicable state policies and standards available for tailoring and adoption at the SLTT level. Large scale incident preparedness and response will be enhanced via the State's Cyber Disruption Response Plan (CDRP), all hazard annex and the State Response Framework. Incident response procedures are regularly reviewed, updated, and tested to ensure that they remain effective and relevant in the face of evolving cybersecurity threats. The state has also leveraged federal grant money to conduct municipal cyber vulnerability assessments and to provide cybersecurity training to municipal officials and others.

In addition, the State supports annual utility cybersecurity reviews through the Public Utilities Regulatory Authority (PURA) and conducts exercises through the state emergency operation center (EOC) and regional exercises including Cyber Yankee.

## Assessment and Mitigation

All major systems and applications, and general support systems operated by or on behalf of State and Local Government entities should undergo security assessments to ensure adequacy of security and privacy controls. To aid in satisfying the ongoing assessment requirement, results from the following sources can be used: continuous monitoring, audits and authorizations, CISA scans and other system development life cycle activities. The Executive Branch under the Bureau of Information Technology Solutions (BITS) will make specific recommendations available upon request for use by the other branches of state and local government entities.

The state will continue to leverage a centralized vulnerability scanning service to maintain an accurate security posture of all state systems and will investigate the feasibility of adding this as a service via the Connecticut Education Network (CEN). The state is also engaging CISA for services in this area.

In addition, within the Connecticut Division of Emergency Management and Homeland Security is the Connecticut Intelligence Center (CTIC), our State Fusion center, which provides intelligence information sharing and analysis with regard to cybersecurity working with State, Federal, local and private sector partners.

## Best Practices and Methodologies

Adopting a recognized cybersecurity framework is a key element of our strategy to secure the whole state including municipalities. The State of Connecticut is embracing the Cybersecurity Framework (CSF) developed by the National Institute of Standards and Technology (NIST) and are using it to strengthen our information security capabilities.

Moreover, providing guidelines, templates, lists, published policies, and other resources, such as CISA's Cyber Performance Goals (CPG) documents and continuing the National Guard municipal cybersecurity assessments already underway in Connecticut, can be valuable tools for assisting SLTT entities in adopting these best practices. We will also explore the concept of a virtual CISO (Visco) service that can provide additional support and guidance to SLTT entities. By prioritizing individual projects that assist entities in adopting these best practices, the state can better ensure a comprehensive and consistent approach to cybersecurity across all eligible entities.

The State of Connecticut is taking proactive steps to ensure the security and safety of its citizens, businesses, and government entities by implementing the NIST Framework. Whether based on NIST Special Publications, CIS Critical Security Controls or other sources, the following best practices are included and projects to implement will be considered over the life of the SLCGP: (a) implementation of multi-factor authentication, (b) implementation of enhanced logging, (c) encryption for data at rest and in transit, (d) eliminating use of unsupported/end of life software and hardware that are accessible from the Internet, (e) prohibition of use of known/fixed/default passwords and credentials, and (f) enabling the ability to reconstitute systems (backups). The municipal cybersecurity assessments conducted by the Connecticut Military Department will identify gaps in cybersecurity at the local level and the cybersecurity grant as well as other resources will be used to help close those gaps and increase cybersecurity hygiene at the State and local levels.

### *Supply Chain Risk Management*

The State of Connecticut will implement cyber supply chain risk management (C-SCRM) best practices identified by NIST. This involves identifying, prioritizing, and assessing information technology suppliers, vendors, and service providers to understand the related and/or cascading risks to their (and all other jurisdictions') supply chain. Additionally, the state will use a risk-based approach of continuous monitoring, which involves regularly assessing the state's cyber security posture and implementing mitigation techniques when needed. As part of planning, the State will also investigate possible adoption scenarios for StateRamp-certified vendors as a way to streamline the procurement process. We can additionally offer workshops, policies and templates as a resource to local government to perform their own due diligence. The state will continue to develop workshops, training and exercises to encourage and enhance cybersecurity.

### *Tools and Tactics*

Tools and tactics are identified, distilled, risk-ranked and communicated through the Connecticut Intelligence Center (CTIC) and disseminated via the Connecticut monthly Cyber Security Committee Meeting. These monthly meetings include Federal, State, local, private sector and tribal partners. This monthly meeting distills threat intelligence and other information and puts it in a consumable format by attendees. We will also encourage leveraging MS-ISCA, CISA and CTIC distributions to share information of adversary tools and tactics. The monthly Cybersecurity Committee meetings include local ESF 17 members who bring this information to other local partners.

## Safe Online Services

Entities who are eligible to receive funds under the SLCGP will be encouraged to migrate to the .gov domain, which may only be provided by government established governmental entities, to help ensure that online services are safe, recognizable, and trustworthy. A project under consideration is creating a managed service to assist with this migration if it's deemed necessary. Enhancing Connecticut Education Network (CEN) and Public Safety Data Network (PSDN) services will also have benefits for many of the public-sector and educational entities within the state.

We have also established partnerships with federal agencies such as DHS and CISA to access their expertise and resources in online service security and delivery. These partnerships allow us to access the latest best practices and standards for online service delivery and security.

Moreover, we have also implemented a comprehensive set of citizen identity and access management controls to ensure that only authorized individuals have access to sensitive information. We will work closely with municipalities to establish similar security policies, procedures and best practices, in order to ensure that all online services across the state are protected against potential threats and vulnerabilities.

## Continuity of Operations

Our strategic approach to achieving this goal involves several key elements, including the development and implementation of robust continuity of operations plans, the integration of these plans with our overall cybersecurity strategy, and regular training and exercises to practice COOP response actions. State and Local Government entities should develop, implement, test, and maintain contingency plans to ensure continuity of operations for all information systems that deliver or support essential or critical functions on behalf of the State of Connecticut or their respective Local Government Entity.

Continuity of operations is very specific to an agency's mandate, but best practices are encouraged via the Connecticut monthly Cyber Security Committee Meeting and reinforced via the National Guard municipal cybersecurity assessment process under the Secretary of the State. In order to further enhance the resilience and preparedness of organizations within the state, the proposed grant application will incorporate the execution of Continuity of Operations (COOP) exercises. These exercises will aim to help organizations better understand and develop their own COOP plans. Recognizing the recent expansion of the Division of Emergency Management and Homeland Security (DEMHS) Training Unit, we will leverage their expertise and resources to help facilitate these exercises. State agencies like Connecticut DEMHS and DAS/BITS will work together with federal and local partners to develop corporative exercises and training to maintain and enhance capabilities during cyber incidents.

## Workforce

Workforce development and retention is a challenge for both public and private sectors. State and local government are often tied to legacy personnel policies and collective bargaining frameworks. Efforts are being made to streamline the state's hiring process. Additionally, the Connecticut Cyber Hub (CT Hub) initiative is a public/private sector partnership that aims to educate the next generation of cybersecurity professionals within the state. This program is aligned with the NIST National Initiative for Cybersecurity Education (NICE) framework as well as CompTIA's Security+ and ISC2's entry-level certification, Certified in Cybersecurity (CC). State employees are provided ample training opportunities through SANS.org, LinkedIn Learning and vendor partners. Information on this program can be found here. State agencies are also working closely with the state university system to increase educational opportunities in the areas of public safety including cybersecurity.

## Continuity of Communications and Data Networks

Much of the public sector network traffic in Connecticut is connected and routed through the Connecticut Education Network (CEN) and the Public Safety Data Network (PSDN), low-cost public sector Internet Service Provider (ISPs). CEN has robust distributed-denial-of-service (DDOS) protection and enhanced cybersecurity controls. Large scale incident response is managed via the State's Cyber Disruption Response Plan (CDRP). The CDRP outlines procedures that must be followed to maintain operations and communication functions during a large-scale emergency or crisis.

Both PSDN and CEN have been architected to withstand targeted attacks on physical and logical communication structures. Multiple network routing and operating topologies provide the required levels of resiliency. In addition, the centrally managed nature of these networks provides cost-efficient business models for security protection measures.

## Assess and Mitigate Cybersecurity Risks and Threats to Critical Infrastructure and Key Resources

The State of Connecticut is a leader in engaging owners and operators of critical infrastructure to assess and mitigate cyber security risks. Cybersecurity reviews of in-scope utilities are conducted annually through the Public Utilities Regulatory Authority (PURA). The goal of these reviews is to identify and address any potential risks or vulnerabilities in the critical infrastructure before they can be exploited. Additionally, the State is expanding this relationship to include telecommunications providers. This partnership is designed to help ensure that the State's infrastructure remains secure and resilient against cyber-attacks or other threats. The State has also participated in a variety of regional and national cybersecurity exercises, including The North American Electric Reliability Corporation (NERC) GridEx to further strengthen its defensive posture against emerging threats. Finally, the State will continue supporting private sector and local government outreach via the Connecticut monthly Cyber Security Committee Meeting. In addition, the State of Connecticut will leverage the Infrastructure Coordination Group (ICG), a working group of DEMHS which includes representatives from DHS and CISA, as well as other federal, state, and local partners, to enhance the assessment and mitigation of cybersecurity risks and threats to critical infrastructure and key resources within its purview.

## Cyber Threat Indicator Information Sharing

The State of Connecticut utilizes multiple mechanisms of information aggregation and sharing, including MS-ISAC, CISA, FBI and other partners. Coordination of information sharing is managed through the State fusion center, CTIC (Connecticut Intelligence Center), which makes use of many feeds for threat intelligence including CISA, DHS and MS-ISAC. Sanitized information is presented under non-disclosure agreements (NDAs) at the Connecticut monthly Cyber Security Committee Meeting. Additionally, local entities are encouraged to sign up for MS-ISAC via the National Guard assessment under the Secretary of the State and this process shall continue under the grant through DEMHS.

Additionally, we will explore the possibility of extreme cyber alerts coming from the Department of Emergency Services and Public Protection (DESPP) regarding emerging threats as well as a Connecticut Education Network (CEN) firewall where real-time threat indicators are integrated.

### *Department Agreements*

Connecticut will continue to leverage CTIC, our state fusion center, as the primary center for cyber information sharing and threat assessment. CTIC will continue to hold sanitized information sharing under non-disclosure agreement (NDA) at the Connecticut monthly Cyber Security Committee Meeting. This meeting includes representatives from both public and private sector, Federal government and regional ESF 17 representatives from across the State. Local partners serve in CTIC, and local partners serve on the cyber security committee and additionally cyber security messaging can be sent through the DEMHS regional coordinators, CEN, and other partners to reach the greatest number of local government officials.

## Leverage CISA Services

Many local government entities already take advantage of the cybersecurity assessment services offered by CISA as well as services provided through other federal partners including MS-ISAC. The State of Connecticut is collaborative with federal partners, and we anticipate continuing to strengthen this relationship. We will also require SLCGP recipients to enroll in Vulnerability Scanning and Web-Application Scanning as applicable.

We periodically provide briefings of CISA and MS-ISAC offerings to the Statewide Cybersecurity Committee on a monthly basis, to ensure visibility as offerings change and mature.

## Information Technology and Operational Technology Modernization Review

The State of Connecticut's strategy will take a risk-based approach to determine the likelihood and impact of threats to information technology and operational technology, with an emphasis on mitigating potential vulnerabilities. Additionally, our strategy will require the evaluation of existing controls, processes and architecture against applicable standards such as NIST 800-53A or ISO 27001. This review process should ensure that effective security and privacy controls are implemented. SLCGP participants may also request to replace end of life/outdated equipment found at this convergence only if approved by the SLCGP Planning Committee. The state generally will not approve grant funding for the replacement of legacy systems, due to the impracticality of allocating limited funds for that purpose. We will also continue to support the Public Utilities Regulatory Authority (PURA) annual assessments and continue outreach to include other critical infrastructure utilities where appropriate.

## Cybersecurity Risk and Threat Strategies

The planning committee will develop and coordinate strategies to address cybersecurity risks and threats across multiple levels of government. This process is largely underway under the Secretary of the State with coordinated cybersecurity assessments utilizing the National Guard. As part of this process, we are also encouraging the use of industry sharing groups including the Multi-State Information Sharing and Analysis Centers (MS-ISAC). We are strongly encouraging any entity that wants to participate in the cyber grant to have a completed assessment. We expect that international frameworks and agreements with neighboring countries will be largely coordinated through Federal partners and supported by Connecticut should the need arise. In addition, we will look to leverage regional cyber security committees from neighboring states and other forums including NASCIO for best practices and information sharing.

## Rural Communities

Rural communities are assured adequate access to projects under the SLCGP by virtue of their representation on the planning committee and from outreach activities by DEMHS Regional Coordinators to the ESF-17 cyber security working groups in each DEMHS emergency planning region and will include all municipalities and tribal nations. Regional ESF-17 representatives are kept informed via the Connecticut monthly Cyber Security Committee Meeting. We will also explore the concept of a virtual CISO (vCISO) service that can provide additional support and guidance to SLTT entities as well as providing training specific to the needs of rural communities and engaging with local community organizations and leaders to increase awareness and understanding of cybersecurity issues. The no cost National Guard cyber assessments are available to all Connecticut municipalities and will help to identify low cost and no cost cybersecurity improvements that can be made by rural towns as well as to identify gaps that could be filled with a portion of the federal cybersecurity grant funding. Additionally, training on the state's Cyber Disruption Response Plan (CDRP) can be provided so that communities are prepared for cyber events.

# FUNDING & SERVICES

The State of Connecticut SLCGP Planning Committee intends to focus on key efforts to strengthen cybersecurity across the State. These efforts include:

- Continue to refine the cybersecurity plan document and implement procedures for administering the SCLGP funding to eligible subentities.
- Continue with National Guard cybersecurity assessments.
- Begin an organized effort encouraging migration to .gov domains.
- Investigate feasibility of a statewide SOC.
- Strengthen and augment multi-factor authentication (MFA) tools and other protections commensurate with risk.
- Establish a comprehensive vulnerability management process that can be replicated at all state entities.

## Distribution to Local Governments

The State of Connecticut intends to use 80% and up to 100% of the funding received through SLCGP to deliver services and capabilities to local government entities as described in Appendix B: Project Summary Worksheet.

[redacted]

[redacted]

# IMPLEMENTATION PLAN

## Organization, Roles and Responsibilities

Each goal and its associated objectives have a timeline with a target completion date, and one or more owners that will be responsible for overseeing and coordinating its completion. Accomplishing goals and objectives will require support and cooperation from numerous individuals, groups, or agencies, and may be added as formal agenda items for review during regular governance body meetings.

Appendix B: Project Summary Worksheet provides a list of cybersecurity projects to complete that tie to each goal and objective of the Cybersecurity Plan.

## Resource Overview and Timeline Summary

The following information is provided to meet the requirement in the **State and Local Cybersecurity Improvement Act: e.2.E.** This information represents the best estimation based on current reference material. It is subject to revision over time. The Human Resources in the following table will be required to implement the plan over the next four years:

*Table 1: The Members of Cybersecurity Planning Committee*

| Role | Organization |
|---|---|
| Chair/Voting Member | State of Connecticut, DAS BITS Chief Information Officer |
| Chair/Voting Member | CT DESPP/DEMHS Deputy Commissioner |
| Vice Chair/Voting Member | State of Connecticut, DAS BITS Chief Information Security Officer |
| Vice Chair/Voting Member | Municipal representative |
| Voting Member | CT DESPP/DEMHS State Emergency Management Director or designee |
| Voting Member | CT DESPP/DEMHS State Fusion Center Director or designee |
| Voting Member | CT DESPP Division of Statewide Emergency Telecommunications |
| Voting Member | The Adjutant General or designee CT National Guard |
| Voting Member | CT Secretary of the State or designee |
| Voting Member | Department of Public Health |
| Voting Member | Executive Director or designee CT Conference of Municipalities (CCM) |
| Voting Member | CT GMIS |
| Voting Member | Executive Director or designee CT Organization of Small Towns (COST) |
| Voting Member | DEMHS Region 1 REPT ESF 17 Chair or designee |
| Voting Member | DEMHS Region 2 REPT ESF 17 Chair or designee |
| Voting Member | DEMHS Region 3 REPT ESF 17 Chair or designee |
| Voting Member | DEMHS Region 4 REPT ESF 17 Chair or designee |
| Voting Member | DEMHS Region 5 REPT ESF 17 Chair or designee |
| Voting Member | CT State University System, Information Technology |
| Voting Member | University of Connecticut Information Technology |
| Voting Member | University of Connecticut Health Center CISO |
| Voting Member | CT Judicial Branch Chief Court Administrator or designee |
| Voting Member | CT Legislative Management/Chief Information Officer |
| Voting Member | Representative of CT Tribal Nations |

| Role | Organization |
|---|---|
| Voting Member | CT Education Network (CEN) |
| Voting Member | CT Bipartisan Infrastructure Law Team (BILT) |
| Voting Member | Criminal Justice Information System (CJIS) |
| Non-Voting Members | |
| Project Management | CT DESPP/DEMHS |
| SAA | CT DESPP/DEMHS |
| Advisory | DHS Intelligence and Analysis Officer |
| Advisory | DHS CISA Cybersecurity Advisor |
| Advisory | DHS CISA Protective Services Advisor |

The State of Connecticut intends to utilize the FY 2022 and future years of the State and Local Cybersecurity Grant Program to improve and enhance the state's capabilities to respond to cybersecurity threats. Federal and non-federal funding will be distributed to support a myriad of projects covering multiple solution areas which will support eligible sub-entities in their preparedness to cybersecurity threats.

The table below represents the State of Connecticut's year 1 (FY 2022) funding allocation under the State and Local Cybersecurity Grant Program. Using the grant program allocation, in conjunction with non-federal money, Connecticut will implement a wide array of projects to support eligible sub-entities in their cybersecurity preparedness and response capabilities, as defined in Appendix B.

## FY 2022 SLCGP - Connecticut Allocations

| | | | | | |
|---|---|---|---|---|---|
| **Total FY2022 SLCGP - $2,978,432.00** | **$2,978,432.00** | **Total Local Passthrough** | **$2,382,745.60** | *Total State Amount (20%)* | **$595,686.40** |
| | | **Rural Jurisdiction Requirement** | $744,608.00 | | |
| Federal Share | $2,680,588.80 | Federal Share | $2,144,471.04 | Federal Share | $536,117.76 |
| Non-Federal | $297,843.20 | Non-Federal | $238,274.56 | Non-Federal Share | $59,568.64 |

[redacted]

| | [redacted] |
|---|---|
| Cybersecurity Plan Required Elements | [redacted] |
| 1. Manage, monitor, and track information systems, applications, and user accounts | [redacted] |
| 2. Monitor, audit, and track network traffic and activity | [redacted] |
| 3. Enhance the preparation, response, and resiliency of information systems, applications, and user accounts | [redacted] |
| 4. Implement a process of continuous cybersecurity risk factors and threat mitigation. practices prioritized by degree of risk | [redacted] |
| 5. Adopt and use best practices and methodologies to enhance cybersecurity (references NIST) | [redacted] |
| a. Implement multi-factor authentication | [redacted] |
| b. Implement enhanced logging | [redacted] |
| c. Data encryption for data at rest and in transit | [redacted] |
| d. End use of unsupported/end of life software and hardware that are accessible from the Internet | [redacted] |

| | |
|---|---|
| e. Prohibit use of known/fixed/default passwords and credentials | [redacted] |
| f. Ensure the ability to reconstitute systems (backups) | [redacted] |
| g. Migration to the .gov internet domain | [redacted] |
| 6. Promote the delivery of safe, recognizable, and trustworthy online services, including using the .gov internet domain | [redacted] |
| 7. Ensure continuity of operations including by conducting exercises | [redacted] |
| 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) | [redacted] |
| 9. Ensure continuity of communications and data networks in the event of an incident involving communications or data networks | [redacted] |
| 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 | [redacted] |
| 11. Enhance capabilities to share cyber threat indicators and related information between the eligible entity and the Department | [redacted] |
| 12. Leverage cybersecurity services offered by the Department | [redacted] |

| | |
|---|---|
| 13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives | [redacted] |
| 14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats | [redacted] |
| 15. Ensure rural communities have adequate access to, and participation in plan activities | [redacted] |
| 16. Distribute funds, items, services, capabilities, or activities to local governments | [redacted] |

# APPENDIX B: PROJECT SUMMARY WORKSHEET

**Purpose:** The **Project Summary Worksheet** is a list of cybersecurity projects that the entity plans to complete to develop or improve any needed cybersecurity capabilities identified in [redacted]

| Obj | Project Name | Project Description | Related Required Element # | Total Cost | [redacted] | Project Type |
|---|---|---|---|---|---|---|
| 1 | Connecticut Cybersecurity Organization and Plan Development | This project created and established a statewide cybersecurity planning subcommittee of the Connecticut Cyber Security Committee of the CT Division of Emergency Management and Homeland Security (DEMHS) Advisory Council. The statewide cybersecurity strategy has been developed with this group and moving forward, this subcommittee will continue to work to establish and document a uniform cybersecurity governance structure that sets the vision for the State's cyber risk management. | 14, 15, 16 | $0.00 | [redacted] | Planning and Governance |
| 1 | Connecticut Cybersecurity Grant Program Development | This project leverages the Cybersecurity Planning Subcommittee to identify and approve strategic projects and/or categories of projects that meet the objectives of the cybersecurity plan and the cybersecurity grant. | 14, 15, 16 | $0.00 | [redacted] | Planning and Governance |
| 2 | Monitoring, Assessing, and Identifying cybersecurity events | This project will invest in creating the first Cybersecurity Operations Center (SOC) using the Connecticut Education Network (CEN) and the Public Safety Data Network (PSDN) as a central point that could benefit many state government and education entities by implementing a statewide security operations center (SOC). | 8, 10 | $55,555.56 | [redacted] | Assessments |
| 2 | Post Implementation Assessment | Following the implementation of cybersecurity planning, equipment upgrades, and cybersecurity training, a post-implementation assessment will be conducted to assess a sub-entity's cyber security status, existing policies/procedures and provide a report of deficiencies and recommendations. Each eligible sub-entity will receive a report of the identified cyber security deficiencies from the Connecticut National Guard. | 8, 10 | $166,666.67 | [redacted] | Assessments |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | The Regional Emergency Planning Teams and RESF-17 committees will assist in setting the priority order of municipalities to be assessed in each phase of the project. | | | [redacted] | |
| 3 | Implementing Cybersecurity Protections for Eligible Sub-entities | This project establishes the funding mechanism to deliver cybersecurity protections to eligible sub-entities through multiple avenues, through a fair and equitable approach to ensure funding is delivered to a wide range of eligible sub-entities. Sub-entities will leverage the Connecticut Education Network (CEN) or submit individual project applications for review by the State Cybersecurity Planning Committee. Projects will be capped at fair costs to ensure adequate dispersal of funds. Eligible and prioritized activities have been identified by the State Cybersecurity Planning Committee | 1, 2, 3, 4, 5, 6, 9, 11, 12, 13, 14, 15, 16 | $2,382,745.60 | [redacted] | Equipment |
| 4 | State Agency Training Series | This project provides funding for vendor-provided cybersecurity training for the State employees with cybersecurity-related roles in order to build the capability and capacity of cyber subject matter experts across state agencies. | 7 | $116,666.67 | [redacted] | Training |
| 4 | Municipal Cybersecurity Training Licenses | This project provides funding to bring cyber security training programs (conducted by contractors) to Connecticut. Bringing the training to the State will allow more participants at the local, regional and State level to participate in training. Programs selected will align with the CT Cyber Security Strategy | 7 | $112,353.07 | [redacted] | Training |
| 4 | Annual State Cybersecurity Symposium | The State will host an annual cybersecurity symposium to foster collaboration and coordination between local, state, and federal cybersecurity experts, encourage networking and partnerships between eligible sub-entities, and provide information and awareness on emerging trends and gaps in cybersecurity | 7 | $88,888.89 | [redacted] | Training |
| 4 | Cybersecurity Training and Professional Development | This project will support professional development and training opportunities for the state and local cybersecurity planning committee, which includes cybersecurity experts and professionals from state agencies and Regional Emergency Support Function (17), Cybersecurity Chairs. | 7 | $55,555.56 | [redacted] | Training |

# APPENDIX C: ENTITY METRICS

The below table should reflect the goals and objectives the Cybersecurity Planning Committee establishes.

**Cybersecurity Plan Metrics**

| Program Goal | Program Objectives | Associated Metrics | Metric Description (Details, source, frequency) |
|---|---|---|---|
| 1. The State of Connecticut has an approved Cybersecurity Plan that meets the SLCGP requirements as defined in the NOFO | 1.1 Draft the plan (see Appendix B for specific program projects) | Draft plan exists | CISO attestation |
| | 1.2 Committee approves the plan | Signed letter from CIO | Signed letter from CIO |
| | 1.3 Submit plan to CISA | Confirmation | Email confirmation from CISA |
| | 1.4 CISA approves the plan | Statement of approval | Email confirmation from CISA |
| 2. Receive Funding from SLCGP | 2.1 Funding received to execute approved projects | Receipt of funds | SAA accepts funds in accordance with cybersecurity plan |
| 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 for Local Entities and Rural areas that request inclusion | 4.1 Enroll Local Entities in Services | Number of entities enrolled in each approved project | Financial Reporting via SAA |
| 5. Review, Revise and Update Plan for next FY as required. | 5.1 Repeat Objectives for Goal 1 for subsequent FY | See goal 1 | See goal 1 |

# APPENDIX D: CONNECTICUT FY 2022 STATE AND LOCAL CYBERSECURITY GRANT (SLCGP) PROGRAM IMPLEMENTATION PLAN

## Overview

The following appendix is an overview of the FY 2022 State and Local Cybersecurity Grant (SLCGP) Program Implementation Plan for the funding allocated to the State of Connecticut.

## Proposed Implementation of Funding

To effectively administer the SLCGP funding to meet the federal grant requirements and equitably disperse the funding to eligible subrecipients, the following implementation plan is being presented for consideration:

- Participating institutions **must** adhere to the required components of the grant including:
    - Participation in Nationwide Cybersecurity Review (NCSR) program annually.
    - Participate in the following Cyber Hygiene Services:
        - Web Application Scanning is an "internet scanning-as-a-service." This service assesses the "health" of your publicly accessible web applications by checking for known vulnerabilities and weak configurations. Additionally, CISA can recommend ways to enhance security in accordance with industry and government best practices and standards.
        - Vulnerability Scanning evaluates external network presence by executing continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts.

- The following items represents eligible grant activities that have been identified as "Priority 1" items that meet gaps identified in municipal cybersecurity assessments and support the Statewide Cybersecurity Strategy. If the planning group reaches consensus on these eligible cybersecurity activities to be funded with Year 1 funds, a maximum price and standards will be established for the following activities:
    - Migration to the .gov internet domain
    - Implement endpoint detection and response (EDR)
    - Implement Multi-factor authentication (MFA / 2FA)
    - Conduct annual cyber assessment (would continue to use CT National Guard for standardized review)
    - Implement assistance of CISA and MS-ISAC cyber hygiene capabilities including:
        - Malicious Domain Blocking and Reporting (MDBR) by MS-ISAC
        - Vulnerability Scanning by CISA
        - Albert Sensors for CEN members by MS-ISAC
    - Addressing other gaps or priorities identified in the cybersecurity assessments and/or Statewide Cybersecurity Strategy.
- Additional Priority (or Priority 2) funding items that align with State priorities and CISA best practices may include:

- Prohibiting use of known/fixed/default passwords and credentials.
- Ensuring the ability to reconstitute systems (backups).
- Implementation of enhanced logging.
- Data encryption for data at rest and in transit.
- End use of unsupported/end of life software and hardware that are accessible from the Internet.
- Other priority gaps specifically identified in the CTNG Cyber Assessments

## Methods to Accomplish Priorities with Year 1 Funding

The group agrees that a statewide target of Year 1 funding is to have at minimum all towns meet the Priority 1 goals. Additional eligible subrecipients, include:

- A county, municipality/eligible entity, city, town, township, local public authority, school district, special district, intrastate district, council of governments, regional or interstate government entity, or agency or instrumentality of a local government.

To accomplish this target, the group will reach consensus on the following implementation options to offer to the eligible subrecipients:

1. **Connecticut Education Network:** Municipality/eligible entity or eligible subrecipient may choose to amend its current network service agreement with Connecticut Education Network (CEN) and CEN will receive the funding to accomplish the priority activities for that municipality/eligible entity. The municipality/eligible entity will match at the appropriate federal/nonfederal cost share. CEN will aggregate requests and seek out the most advantageous contract and price on behalf of participants. Municipalities committed to the ARPA-CPF funded project who have signed an agreement may also participate (https://ctedunet.net/mficp/). CEN will also create an affiliate agreement if demand for such services warrant one.

2. **Municipality/eligible entity-Driven**: Municipality/eligible entity may choose to make its own application for funding to accomplish these priority activities, and DEMHS will administer the grant funds in the same manner as Citizen Corps Program funds (i.e., reimbursement for eligible work performed.) The municipality/eligible entity will be reimbursed at appropriate federal/nonfederal cost share.

3. **Multi-town/eligible entity Submission**: Municipalities may choose to submit a multi-town/eligible entity application for funding to accomplish these priority activities on a regional basis.

Alternative proposals to options 2 or 3, above should cost the same or less than the CEN established costs. State will only provide funding up to the costs established for CEN services.

## Sub-Application and Program Development

Applications will be reviewed to ensure that all are aligned to the priority areas, and that at least 25% of the funding is going to rural communities. Rural is defined 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.’ (FY 2022, Notice of Funding Opportunity page 32)[2]

CEN will develop a program to help communicate, organize, and facilitate workshops, webinars, and training for executive, administrative, and technical leaders to improve:

- Cyber hygiene / end user awareness and training
- Disaster Recovery and Continuity Planning
- Vendor risk management and best practices for MSP contract language

CEN will collaborate with DESPP, CISA, and others for content and training that is high quality and relatively low cost. Program cost to be determined and will be provided as scope is refined through the committee. If there is funding remaining after priority projects have been funded, the group will reconvene to determine how to allocate to meet the next level of priorities**.**

[2] The Department of Homeland Security Notice of Funding Opportunity Fiscal Year 2022 State and Local Cybersecurity Grant Program | FEMA.gov

# APPENDIX E: CONNECTICUT MILITARY DEPARTMENT CYBERSECURITY ASSESSMENT AND FINDINGS

## Overview

Prior to the State and Local Cybersecurity Grant Program, Connecticut has been prioritizing and addressing cybersecurity preparedness with efforts funded by the Homeland Security Grant Program (HSGP). Using HSGP funding, the Connecticut Military Department provided no cost cybersecurity assessments to local municipalities to provide a gap assessment and deficiency report regarding the cybersecurity posture and preparedness of the participating municipality. The findings of this report are included as an appendix to the 2023 Cybersecurity Strategy.

## Executive Summary

This report is a summary of the assessment results of the Connecticut Military Department's (CTMD) Municipal Cybersecurity Initiative in conjunction with the Division of Emergency Management and Homeland Security (DEMHS) during 2023. The CTMD was asked to provide assistance to the 169 municipalities located within Connecticut by the DEMHS for the review of their municipal information technology infrastructure. Because some of these municipalities' information technology infrastructure was assessed during a separate effort in 2022/2023 with the Secretary of the State's (SOTS) office regarding Elections Security, their data is included in the final report metrics and conclusion.

As part of this initiative, the CTMD developed a Municipal Cybersecurity Best Practices guide that was based on the National Institute of Standards and Technology Cybersecurity Framework, as well as input from the Connecticut Interlocal Risk Management Agency (CIRMA) and the Federal Cybersecurity and Infrastructure Security Agency (CISA). The Best Practices guide was used to evaluate the risk to Information Technology (IT) and election infrastructure at the municipal level. Additionally, each municipality was given the choice to opt in to receive an on-site IT infrastructure risk assessment visit from the CTMD.

For those municipalities that engaged an on-site visit, the CTMD performed assessments in accordance with the Municipal Cybersecurity Best Practices guide. After review and compilation of the data, the CTMD wrote out an assessment of each municipality. The following pages detail municipal-specific findings from the 159 assessments that have been completed between October 11, 2022, and June 13, 2023, as well as generalized recommendations from the CTMD.

Due to the sensitive nature of the information contained within this report, it should be considered exempt from public disclosure. This report is exempt from public disclosure under the Connecticut Freedom of Information Act (FOIA) because it is a cybersecurity report and a record of standards and procedures the disclosure of which would compromise the security or integrity of an IT system (CGS 1- 210 (b) (19) (I) and (20)). Any requests for disclosure of this report should be coordinated between your municipal FOIA Coordinator and CTMD.

## About the Municipal Cybersecurity Best Practices Guide

The Municipal Cybersecurity Best Practices guide is a no-cost assessment to identify cyber security vulnerabilities and provide recommendations to prevent, correct, and detect information security risk. This assessment consists of 54 questions, each with an associated risk level ranging between 1 (low risk) and 5 (high risk), which was determined by a proprietary formula by CTMD cyber experts based on the NISF Cybersecurity Framework. The Best Practices guide is divided into 9 sections:

1. End User Training
2. Patching and Vulnerability Management
3. Multifactor and External Access
4. Endpoint Hardening & Security
5. Network Boundary Hardening & Security
6. Operational Policies
7. Detecting, Responding and Recovering from Attack
8. Vendor Management and Audit
9. Physical Security