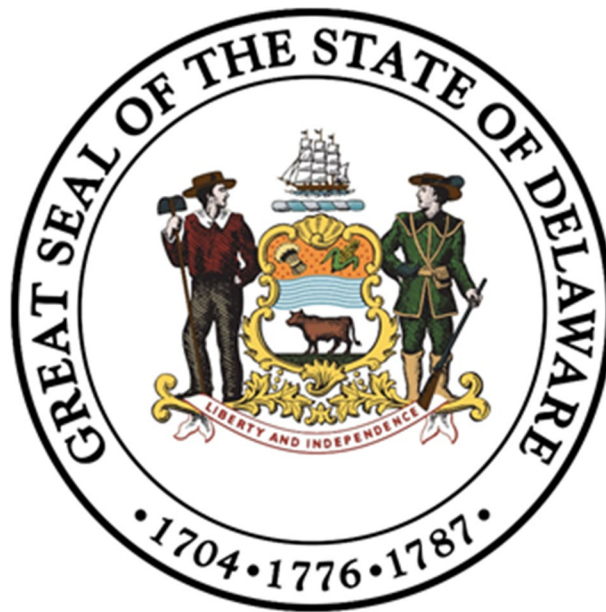


THE STATE OF DELAWARE CYBERSECURITY PLAN



January 2023

Approved by the State of Delaware Cybersecurity Planning Committee
on 5/3/2023
Version 1

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

Letter from DELAWARE COMMITTEE CHAIR	2
Introduction	4
SLCGP Cybersecurity Plan Elements	6
Manage, Monitor, and Track	6
Monitor, Audit, and Track	7
Enhance Preparedness	7
Assessment and Mitigation	7
Best Practices and Methodologies	7
NIST Principles	8
Supply Chain Risk Management.....	8
Tools and Tactics	8
Safe Online Services.....	9
Continuity of Operations	9
Workforce	9
Continuity of Communications and Data Networks.....	9
Cyber Threat Indicator Information Sharing.....	9
Department Agreements	10
Leverage CISA Services	10
Information Technology and Operational Technology Modernization Review	10
Cybersecurity Risk and Threat Strategies	10
Rural Communities	10
Funding & Services	11
Distribution to Local Governments	11
Assess Capabilities	11
Implementation Plan	11
Resource Overview and Timeline Summary.....	12
Metrics	14
Appendix A: Cybersecurity Plan Capabilities Assessment	15
Appendix B: Project Summary Worksheet	18
Appendix C: Entity Metrics	20

LETTER FROM DELAWARE COMMITTEE CHAIR

Greetings,

The State and Local Cybersecurity Grant Program (SLCGP) Planning Committee for Delaware respectfully submits The Delaware SLCGP Cybersecurity Plan for FFY2022 to 2025. The Plan reflects collaborative efforts to advance cyber maturity levels commensurate with risk, utilizing a whole-of-state approach. The Plan is comprised of all of the required elements defined in the Notice of Funding Opportunity (NOFO). It defines project funding priorities to ensure a baseline level of cybersecurity risk controls for threat mitigation, responses to cybersecurity incidents, and resiliency. The latter is achieved in accordance with requirements of the Infrastructure Investment and Jobs Act (IIJA) and SLCGP. The State of Delaware, like most of the states around the country has faced and continues to face increases in targeted cybersecurity attacks. These attacks have exposed the critical relationship between local government and state services. Attacks like Distributed Denial of Service (DDoS) have impacted both state and local government web applications. Ransomware threats are significantly impactful. Their success at the local government level has spotlighted the disparity between security controls at the state and local levels. During these attacks, the lack of detailed activity tracking has made the analysis, response, and recovery difficult.

The Planning Committee includes voting members from state, county, city, and town governments, as well as champions from public education and public health, to ensure the Plan goals are achieved. Care has been taken at each meeting to ensure feedback from all concerned entities, with any decision by the body finalized only after ensuring a quorum of participating organizations were present. These goals focus on leveraging economies of scale to implement programs that directly benefit the entirety of Delaware's government structure. The Committee will monitor, revise as needed, and report Plan progress. It will also assist teams in coordinating cyber efforts. The purpose of this Cybersecurity Plan is to demonstrate Delaware's commitment to continuously improving our security posture with a whole-of-state approach.

Sincerely,

Solomon Adote

[Solomon Adote \(May 4, 2023 08:33 EDT\)](#)

Solomon Adote, State of Delaware Chief Security Officer
State of Delaware
Department of Technology and Information

Michael Hojnicki

Michael Hojnicki, Co-Chair of Cybersecurity Planning Committee
IT Director for New Castle County
New Castle County Delaware

INTRODUCTION

The Delaware Cybersecurity Plan is a two-year strategic plan comprised of the following:

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

The Delaware Cybersecurity Plan aligns with and references the following documents:

1. State of Delaware Information Security Policy
<https://webfiles.dti.delaware.gov/pdfs/pp/DelawareInformationSecurityPolicy.pdf>
2. State of Delaware Standards and Policies <https://dti.delaware.gov/technology-services/standards-and-policies/>
3. State of Delaware Supply Chain Risk Best Practices
<https://digiknow.dti.delaware.gov/dcsac/contentFolder/pdfs/vitalContractComponents.pdf?cache=1643922035514>
4. Center for Internet Security Top 18 Security Controls <https://www.cisecurity.org/controls/cis-controls-list>
5. National Institute of Standards and Technology Cybersecurity Framework
<https://www.nist.gov/itl/smallbusinesscyber/planning-guides/nist-cybersecurity-framework>

Mission and Vision

This section describes the Planning Committee’s mission and vision for improving cybersecurity through the SLCGP funding opportunity:

Mission:

The mission of the Delaware Cybersecurity Plan is to bring all Delaware government entities to an acceptable cyber risk baseline, using SLCGP funding in accordance with The U.S. Department of Homeland Security guidelines. It also strives to continuously assess and address the strengths and weaknesses of the cybersecurity and resiliency programs of those entities. Risks will be prioritized and mitigated commensurate to the cyber threat landscape and a whole-of-state approach that aligns with the concepts of zero-trust. This course delivers a resilient, risk-based, modern threat-mitigated environment, that ensures the confidentiality, availability, and integrity of data and systems.

Vision:

The vision of the Delaware Cybersecurity Plan is to leverage an effective, diverse, and collaborative team to develop, prioritize, and execute cyber enhancement projects statewide that will deliver a risk-based baseline level of security controls. These controls will serve to protect critical services and data of Delaware governments, businesses, and constituents.

SLGCP Cybersecurity Program Goals and Objectives

State of Delaware SLCGP Cybersecurity Program goals and objectives include the following:

Cybersecurity Program	
Program Goal	Program Objectives
1. Establish Acceptable Risk Baseline and Governance Structures	1.1 Engage state & local governments to assess cyber maturity levels
	1.2 Complete Security Risk Assessments
	1.3 Ensure existing security controls are effectively implemented
	1.4 Ensure Delaware Cyber Security Advisory Council (DCSAC) alignment and agreement with governance structures and goals.
	1.5 Develop Incident Response Plans & Playbooks
	1.6 Develop Acceptable Risk Controls for cyber risk mitigation and Resiliency Policies & Standard Operating Procedures
2. Implement Detection and Response tools, protocols, and best practices	2.1 Ensure effective threat detection and response tools are installed and operational at every level of government in Delaware
	2.2 Implement Identity Access Management (IAM) including Multifactor Authentication (MFA) for Email, VPN & Web applications
	2.3 Implement Web Application Shielding & .GOV for website standards
	2.4 Implement Endpoint Detection and Response (EDR)
	2.5 Update Email Security and establish .GOV standards
	2.6 Implement Web URL Filtering and Malicious site blocking

Program Goal	Program Objectives
	2.7 Secure all Remote Access Services
3. Invest in Cyber education, staff development, and building future workforce	3.1 Ensure that security awareness training is mandated and delivered statewide for all staff with network access.
	3.2 Develop Cybersecurity Training for Information Technology (IT) & Operational Technology (OT) staff and management
	3.3 Develop Apprenticeship/Mentorship programs for the future workforce
	3.4 Develop cybersecurity consulting programs & virtual CISOs
4. Re-evaluate Program objectives to continuously improve statewide cybersecurity defenses and resiliency.	4.1 Ensure that Program objectives are aligned with state and local cybersecurity maturity levels commensurate to the cyber risk landscape.
	4.2 Monitor threat intelligence
	4.3 Perform vulnerability testing and risk assessments
5. Monitoring & Threat Intelligence	5.1 Implement Security Monitoring
	5.2 Implement Commercial Threat Intelligence
	5.3 Perform Incident Response Tabletops
	5.4 Implement Breach response retainers & develop internal response team
6. Cyber Hygiene	6.1 Establish a comprehensive patch management program
	6.2 Establish a vulnerability management (App/Sys) / penetration testing program
	6.3 Implement a legacy and End of Life system and application life cycle program
	6.4 Establish Data Security and Data Encryption standards
7. Resilience	7.1 Deploy Backup Solutions and Services
	7.2 Establish IT, IOT and OT guidelines and standards
	7.3 Perform Disaster Recovery and Business Continuity Tabletop Exercises
	7.4 Develop IT, IOT and OT cyber resilience and threat mitigation programs

SLCGP CYBERSECURITY PLAN ELEMENTS

Manage, Monitor, and Track

At the state and local levels, entities will establish and maintain an inventory of their systems, applications, and user accounts (“information assets”). Entities will establish, monitor, and track procedures for systems, applications, and user accounts. This allows effective controlling and restricting of access to information assets to authorized users based on defined government, business, and legal requirements. Access will be limited to a “need-to-use” and/or “need-to-know” basis. Mechanisms will be implemented that provide for the monitoring, control, administration, and tracking of access to, and the use of information assets. Mechanisms will also allow for the protection of such assets from unauthorized or unapproved activity and/or destruction. Once a detailed inventory is available, legacy systems and applications will be monitored for vulnerabilities and will be given special attention to ensure their protection from a cyber-attack. Various contracted SaaS and cloud services, in addition to leveraged government services, will be utilized.

Monitor, Audit, and Track

At the state and local levels, entities will have a mechanism for monitoring, auditing, and tracking network traffic and activity. Partnerships with CISA and MS-ISAC will be explored to leverage their available low or no-cost services. These services may be augmented with additional commercial solutions or services.

Asset owners/custodians, and information security and privacy officers at state and local levels will:

- a) Ensure the information assets under their purview are assessed for security and privacy risks and configured such that event logging is enabled to confirm an adequate level of situational awareness regarding potential threats to the confidentiality, integrity, availability, and privacy of agency information and information systems are identified and managed; and
- b) Review and retain event logs in compliance with all applicable local, State and federal laws, regulations, executive orders, circulars, directives, internal agency and State of Delaware policies, and contractual requirements.

Enhance Preparedness

State and Local Government entities will implement continuous risk management processes that account for the identification, assessment, treatment, and monitoring of risks that could adversely impact their operations, information systems, and information. These processes will inform the exercise and execution of Incident Response Plans, Continuity of Operations Plans and the Delaware Emergency Operation Plan. Lessons learned from these exercises will be incorporated into future planning, inform organizational decisions, and highlight additional equipment and training needs. Disaster recovery and resiliency needs of state and local systems and applications will be assessed and prioritized as part of the risk management process. Solutions to solve the resiliency of these systems and applications will be addressed.

Assessment and Mitigation

All major IT and OT systems and applications, and general support systems operated by or on behalf of State and Local Government entities will undergo continuous security assessments to ensure adequate security and privacy controls are implemented and risks are managed commensurate with risk levels throughout their lifecycles. Partnerships with CISA, MS-ISAC, E-ISAC, and the Delaware National Guard will be leveraged where possible as low or no-cost service options. Commercial solutions and services will also be funded to meet the needs of the state or local entity for assessments and threat mitigation. Risk management processes will be employed, including identifying, assessing, and addressing security and privacy risks at the inception of the project, to build and secure a system until the decommissioning of the system. These actions enable State and Local Government entities to maintain security and privacy of a system throughout its lifecycle. To aid in satisfying the ongoing assessment requirements, assessment results from the following sources can be used: continuous monitoring, audits and authorizations, and other system development life cycle activities.

Best Practices and Methodologies

State of Delaware SLCGP Cybersecurity Program will prioritize the following goals and objectives according to risk management processes, including identifying, assessing, and addressing security and privacy risks for state and local governments. Specific approaches to satisfy objectives are documented in the Program Goals and Objectives Chart above. Further detail is provided in the following bullet points::

- Establish Acceptable Risk Baseline and Governance Structures – Conduct risk and cyber maturity assessments. Develop Incident Response Plans and Playbooks and risk controls for cyber risk mitigation, resiliency policies, and standard operation procedures.
- Implement Detection and Response tools, protocols, and best practices – Ensure .gov domains are established and effective threat detection and response tools are installed. Ensure protections such as multi-factor authentication, web application shielding, endpoint detection and response, and web URL filtering and malicious site block are in place.
- Invest in Cyber education, staff development, and building future workforce – Ensure that security awareness training is mandated and delivered to all government employees with network access. Develop/utilize cybersecurity training for IT and OT staff and management. Develop/utilize apprentice and mentorship programs and cybersecurity consulting programs.
- Re-evaluate Program Objectives - Continuously improve statewide cybersecurity defenses and resiliency. Confirm alignment of cybersecurity maturity levels commensurate with the cyber risk landscape, and capabilities to adopt policies tools and best practices, and priorities to protect data and critical infrastructure. Perform vulnerability testing and risk assessments.
- Monitoring & Threat Intelligence – Implement security monitoring and commercial threat intelligence. Perform incident response tabletops and develop breach response retainers and internal response teams.
- Cyber Hygiene – Establish comprehensive patch management programs and vulnerability management penetration testing programs as well as data security and data encryption standards. Implement a legacy and end of life system and application life cycle program.
- Resilience – Deploy backup solutions and services. Perform disaster recovery and business continuity exercises. Develop IT, IOT and OT cyber resilience and threat mitigation programs according to established guidelines and standards.

NIST Principles

A detailed description of the application of NIST Principles and the CIS Critical Security Controls is provided in the above Goals and Objectives.

Supply Chain Risk Management

The State of Delaware and local government entities collaborated with DCSAC to document Supply Chain Risk Best Practices and met with local entities to share the materials and learn their vulnerabilities.

[The State of Delaware Supply Chain Risk Best Practices](#), [NIST 800-53](#), [CIS Top 18](#), and [SP800-161](#) will be utilized in assessing any vendor so that all go through the same process of evaluation. An internal group that includes the Senior IT or Security Leaders, Procurement representatives, and Risk Management representatives will be empaneled to advise, research, and inform the State and Local Government IT Leadership in deciding on supply chain risk issues.

Tools and Tactics

Partnerships with CISA, MS-ISAC, E-ISAC, DCSAC, and the Delaware National Guard will be leveraged to gain knowledge of adversary tools and tactics. The council will first explore the federally subsidized programs, such as cybersecurity best practices, cyber threats and advisories, industrial control system vulnerabilities and risks, critical infrastructure security and resilience information. Albert Network Monitoring and Management, endpoint security services, and managed security services, in addition to commercial solutions and services, will also be funded to meet the needs of the state or local entity. The

State of Delaware and local government entities will utilize the MS-ISAC Cyber Alert Levels to understand and measure the likelihood of adversary tools and tactics impacting their computing environment.

Safe Online Services

A plan will be developed for organizations who are eligible to receive SLCGP funds and have not migrated to the .gov domain.

Continuity of Operations

State and Local Government entities will be required to develop or update, implement, test with exercises, and maintain Continuity of Operations Plans (COOP) for all operational and information systems that deliver or support essential or critical functions on behalf of the State of Delaware or their respective local government entities. This will guarantee availability of critical and essential systems and components so that entities can meet mandates that are dictated by statute, executive order, policy, or contract, to ensure delivery of vital government services.

Workforce

Enhanced workforce recruitment and retention policies will be developed based upon the National Initiative for Cybersecurity Education (NICE) framework. This will provide an adequate workforce for cybersecurity. Once State and local Government entities recruit and hire employees, they should guarantee that all users are made aware of the security and privacy risks associated with their roles and that users understand their responsibilities. They must also be aware of applicable laws, regulations, executive orders, circulars, policies, standards, and procedures related to the security and privacy of information assets, information, and systems. State of Delaware and local governments will ensure that general security awareness training is available for the entire workforce and that specialized cybersecurity training is available for IT and OT staff and management. Opportunities for apprenticeship, mentorship, and next-generation workforce development will be explored. State and local governments will have the opportunity to have a consultant available for cybersecurity technical and policy questions.

Continuity of Communications and Data Networks

As part of the COOP plans of the State and Local Governments, options such as a crisis communications service for notification to employees and WebEOC for crisis management will be implemented or updated. Analysis of interconnection issues between the State and Local systems that may lead to a secondary impact when one or the other is affected by an incident will be performed. Using a risk-based approach, state and local governments will be able to deploy backup solutions for the critical services that they provide to their constituents. IT, IOT and OT cyber resilience and threat mitigation programs will be explored and implemented. Guidelines and standards will be established for these critical services. Disaster recovery and business continuity tabletop exercises will be performed as backup solutions and services are developed.

Cyber Threat Indicator Information Sharing

Cyber Threat intelligence comes from a variety of sources and is migrated among a variety of tools and information sources. Tools selected by organizations should leverage CISA's Cyber Information Sharing and Collaboration Program (CISCP) and the CISA's Automatic Indicator Sharing capability, thereby having the ability to automatically ingest data by applying industry standard formats. MS-ISAC or EI-ISAC data, in the form of Structured Threat Intelligence Expression (STIX) format, OpenIOC, Malware Information Sharing Platform (MISP), or Trusted Automated eXchange of Indicator Information (TAXII) should be used to collect

and share data, but other more localized data collection processes may be implemented using these same data collection tools. Additionally, entities will be strongly encouraged to report all computer security incidents to provide data to assist in analysis of attacks to CISA through the Incident Reporting System | CISA link. State and local governments will also share information through our existing intelligence channels such as the DCSAC, Delaware Information & Analysis Center (DIAC), and any other public private partnerships with which they are affiliated. State and local governments will explore commercial solutions and services to increase visibility in this initiative.

Department Agreements

Threat information will be shared through the DCSAC, DIAC, this committee and other public private partnerships.

Leverage CISA Services

While some of our local government entities already take advantage of the cybersecurity assessments and other services offered by CISA, many do not. All local governments will be advised and encouraged to use, such services in the future by showcasing them at statewide events and through routine communications. Additionally, the SLCGP recipients will be encouraged to enroll in Vulnerability Scanning and Web-Application Scanning as appropriate.

Information Technology and Operational Technology Modernization Review

The strategic approach to modernizing IT and OT technology should employ a cyber-physical systems (CPS) strategy, wherein OT, IoT, Industrial Internet of Things (IIoT) and IT security are managed as part of a coordinated effort. It should model impact to human life, in addition to classification scheme, and incorporate emerging security directives in prioritizing among the various sectors (electricity, natural gas, water/wastewater). State and local governments will use a consistent approach and process to evaluate the implementation or modernization of an OT or IT system. The process will ensure that these critical technologies are developed with network segmentation and follow the security best practice guidelines available through [NIST 800-53](#) and [CIS Top 18](#). Depending on the system, cloud technologies may be explored if it can be secured according to best practices and industry standards.

Cybersecurity Risk and Threat Strategies

The SLCPG Planning Committee will use this Plan and operate under its approved charter to develop and coordinate strategies and projects that address cybersecurity risks and cybersecurity threats with other organizations, including consultation with local governments and associations of local governments, and neighboring entities.

Rural Communities

Unincorporated areas are considered part of the county in which they are located, for the purposes of this cybersecurity plan. Rural communities are assured adequate access to projects under the SLCGP by virtue of their representation on the Planning Committee and outreach activities coordinated by the Committee and the dedicated support of the representative from the Delaware League of Local Governments that is a member of the committee. The committee also understands that the use of these funds is directed to rural communities.

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

FUNDING & SERVICES

The State of Delaware SLCGP Planning Committee intends to focus on 4 key efforts to strengthen cybersecurity across the State. These efforts are:

- Develop and establish appropriate governance structures, as well as develop, implement, or revise cybersecurity plans to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.
- Understand current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.
- Implement security protections commensurate with risk.
- Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.

These efforts are detailed in **Appendix B: Project Summary Worksheet**

Distribution to Local Governments

The State of Delaware will pass through a minimum of 80%, of the funding received through SLCGP to local governments – obligating funds, items, services, capabilities, or activities to local governments where strategic. See **Appendix B: Project Summary Worksheet**. As part of the local pass through requirement, at least 25% of the federal funds provided under the grant will be passed through to rural areas. Funds passed through to rural areas is expected to exceed the 25%, as most of Delaware’s municipalities currently meet the designation of rural area. The committee will prioritize and approve projects for potential subgrants.

ASSESS CAPABILITIES

Initially, the Delaware SLCGP Planning Committee used **Appendix A: Cybersecurity Plan Capabilities Assessment** to assess and document capabilities for the cybersecurity plan elements included in this plan. A more detailed assessment will be developed and utilized, however, also as part of the award for the grant for prioritization of projects.

IMPLEMENTATION PLAN

Organization, Roles, and Responsibilities

The State of Delaware SLCGP Planning Committee includes voting members from state, county, city, and town governments as well as champions from public education and public health institutions to ensure the Plan goals are achieved. To ensure statewide perspectives, members of the Committee are also representatives of urban, suburban, and rural areas of the State. The Committee shall develop, approve, implement, monitor, review, and revise as appropriate the Plan that establishes funding priorities and approves projects, which are intended to identify, assess, and address cyber risks within and across state and local government organizations in the State of Delaware in accordance with the requirements of the IJA and SLCGP.

The State Chief Security Officer will act as Chair of this Committee. The CSO will be responsible for ensuring the execution and reporting of Plan priorities and maintaining a diverse committee membership

where all government entities are represented. The Chair of the committee and/or Co-Chair, with the consent of the Committee members, may invite representatives from public and private sector organizations within the State to act as advisors to the Committee. They will provide varied perspectives and guidance. Such relevant groups may include the Delaware Homeland Security Advisory Council, Delaware Cybersecurity Advisory Council, the Delaware League of Local Governments, the Department of Education, the Delaware Emergency Management Agency, and leading vendors in key strategic risk mitigation areas.

The Committee shall provide ongoing communication of required documentation and project reporting to all stakeholders throughout the SLCGP period of performance. The Committee shall meet as deemed appropriate by the Chair or Co-Chair of the Committee. Both will ensure that meetings are documented. The Chair and/or Co-Chair will consult with the Delaware Emergency Management Agency (DEMA) who is the Homeland Security and Preparedness Grants Management State Administrative Agency (SAA). DEMA will be responsible for the management and administration of federal and state homeland security grants. All grant activities shall comply with the requirements set forth in the SLCGP.

Resource Overview and Timeline Summary

Chair:

Solomon Adote, State Chief Security Officer
Department of Technology and Information, State of Delaware

Co-Chair:

Michael Hojnicky, Chief of Technology & Administrative Services
New Castle County

Voting Members:

Sandra Alexander, Director of Risk Management & Governance
Department of Technology and Information State of Delaware

David Baylor, City Manager
Delaware City (Suburban/Rural)

Max Hamby, IT Director
City of Rehoboth Beach (Suburban/Rural)

Lawrence Josefowski, Director of Information Technology
City of Dover (Suburban)

Dwayne Kilgo, Director, Information Technology
Sussex County

Donald Lynch, IT Infrastructure Manager
City of Newark (Suburban)

Kristi Pelezo, Director of Technology and Data Office
Department of Education, State of Delaware

Bill Pettigrew, Director of Information Technology

City of Milford (Rural)

Tabatha Offutt-Powell, Chief of Data and Informatics
Department of Health & Social Services

James A. Robb, Risk Manager
City of Wilmington (Suburban/Rural)

Marcia Scott, Executive Director
Delaware League of Local Governments

Joseph Simmons, Director of Information Technology
Kent County

J. Allan Wagamon, President of Wagamon Technology Group
Representing the towns of Harrington and Fenwick Island (Rural)

William Wharton, IT Director
Town of Bethany Beach (Suburban/Rural)

METRICS

Cybersecurity Plan Metrics			
Program Objectives	Program Sub-Objectives	Associated Metrics	Metric Description (details, source, frequency)
1. Improve State and Local entities capability and capacity to adopt and use best practices and methodologies to enhance cybersecurity	1.1 Improve and refine SLGCP Cybersecurity Plan	Future plan(s) approved by CISA	Email from CISA confirming approval of plan.
	1.2 Understand current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structure assessments	Review and prioritizations of gaps from completed assessments	Assessment is completed initially to determine where gaps exist.
	1.3 Implement security protections commensurate with risk	Number of security protections implemented	Report on implemented protections
	1.4 Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility	Number of organization personnel trained	Report of organization personnel trained

APPENDIX A: CYBERSECURITY PLAN CAPABILITIES ASSESSMENT

COMPLETED BY The State of Delaware SLGCP Committee				FOR ASSESSOR
Cybersecurity Plan Required Elements	Brief Description of Current Capabilities of SLTT within the Eligible Entity	Select capability level from: Foundational Fundamental Intermediary Advanced	Project # (s) <i>(If applicable – as provided in Appendix B)</i>	Met
1. Manage, monitor, and track information systems, applications, and user accounts	Incomplete implementation across the totality of the State and Local Government entities	Foundational	[3]	
2. Monitor, audit, and track network traffic and activity	Incomplete implementation across the totality of the State and Local Government entities	Foundational	[3]	
3. Enhance the preparation, response, and resiliency of information systems, applications, and user accounts	Incomplete implementation across the totality of the State and Local Government entities	Foundational	[3]	
4. Implement a process of continuous cybersecurity risk factors and threat mitigation. practices prioritized by degree of risk	Incomplete implementation across the totality of the State and Local Government entities	Foundational	[2]	
5. Adopt and use best practices and methodologies to enhance cybersecurity (references NIST)	Incomplete implementation across the totality of the State and Local Government entities	Foundational	[3,4]	
a. Implement multi-factor authentication	Incomplete implementation across the totality of the State and Local Government entities	Foundational		
b. Implement enhanced logging	Incomplete implementation across the totality of the State and Local Government entities	Foundational		
c. Data encryption for data at rest and in transit	Incomplete implementation across the totality of the State and Local Government entities	Foundational		

d. End use of unsupported/end of life software and hardware that are accessible from the Internet	Incomplete implementation across the totality of the State and Local Government entities	Foundational		
e. Prohibit use of known/fixed/default passwords and credentials	Incomplete implementation across the totality of the State and Local Government entities	Foundational		
f. Ensure the ability to reconstitute systems (backups)	Incomplete implementation across the totality of the State and Local Government entities	Foundational		
g. Migration to the .gov internet domain	Incomplete implementation across the totality of the State and Local Government entities	Foundational		
6. Promote the delivery of safe, recognizable, and trustworthy online services, including using the .gov internet domain	Incomplete implementation across the totality of the State and Local Government entities	Foundational	[4]	
7. Ensure continuity of operations including by conducting exercises	Incomplete implementation across the totality of the State and Local Government entities	Foundational	[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)	Incomplete implementation across the totality of the State and Local Government entities	Foundational	[4]	
9. Ensure continuity of communications and data networks in the event of an incident involving communications or data networks	Incomplete implementation across the totality of the State and Local Government entities	Foundational	[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	Incomplete implementation across the totality of the State and Local Government entities	Foundational	[2,3]	

11. Enhance capabilities to share cyber threat indicators and related information between the eligible entity and the Department	Incomplete implementation across the totality of the State and Local Government entities	Foundational	[3,4]	
12. Leverage cybersecurity services offered by the Department	Incomplete implementation across the totality of the State and Local Government entities	Foundational	[3]	
13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives	Incomplete implementation across the totality of the State and Local Government entities	Foundational	[3]	
14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats	Incomplete implementation across the totality of the State and Local Government entities	Foundational	[1,2]	
15. Ensure rural communities have adequate access to, and participation in plan activities	Incomplete implementation across the totality of the State and Local Government entities	Foundational	[1]	
16. Distribute funds, items, services, capabilities, or activities to local governments	Incomplete implementation across the totality of the State and Local Government entities	Foundational	[1]	

APPENDIX B: PROJECT SUMMARY WORKSHEET

Project Number	1. Project Name	Project Description	Related Required Element #	Cost	Status	Priority	Project Type
1	A Delaware League of Local Governments (DLLG) consultant to represent local/rural entities in support of SLCGP & Cyber Planning Subcommittee	This project aligns with the required elements [14,15,16] and supports the development of a statewide cybersecurity plan [Plan Development]. DLLG consultant would be designated as a local government representative (counties, cities, towns) to the SLCGP Committee unless otherwise represented. Responsibilities include: attend all subcommittee meetings and represent local entities; ensure adequate access to, and participation in, the services and programs provided by the SLCGP to local and rural areas within the state; support project implementation to include the distribution of funds, items, services, capabilities, or activities to local and rural entities; support the development of the statewide cybersecurity plan, ensuring that local and rural governments are represented, risks and capabilities are integrated into the plan, and that the plan aligns with grant guidelines. Federal share for this project is \$30,000 with a cost share of \$3,333.	[14,15,16]	\$30,000	Future	High	Organize
2	Statewide Cybersecurity Risk/Capabilities Assessment	This project aligns with the required elements [4,10,14] and supports the development of a statewide cybersecurity plan [Plan Development]. The SLCPG Committee will leverage an existing state contracted vendor to conduct a statewide risk and capabilities	[4,10,14]	\$600,000	Future	High	Plan

		assessment. The purpose of the assessment would be to understand current government entities cybersecurity posture and areas for improvement. The risk and capabilities assessment would be integrated into the statewide cybersecurity plan and the State Local Cybersecurity Grant Planning Committee would prioritize potential projects based on assessment outputs. Federal share for this project is \$600,000 with a cost share amount of \$66,666.					
3	Protect Modern Perimeter	This project aligns with the required elements [1,2,3,5,9,10,11,12,13]. The following project examples align with the overarching goal to protect modern perimeters and implement security protections commensurate with risk: web application protection; endpoint detection and response; .gov email and websites; threat intelligence licenses; state network data leakage prevention. Following the cybersecurity plan submission and approval, revised IJs and Project worksheets will be submitted that identify prioritized projects and refined descriptions/budgets. Federal share for this project is \$1,100,000 but may be revised with the updated IJ submission pending plan review and approval.	[1,2,3,5,9,10,11,12,13]	\$1,100,000	Future	High	Equip
4	Workforce Development Commensurate with Responsibilities	This project aligns with the required elements [5,6,7,8,11]. The following project examples align with the overarching goal of workforce development, ensuring appropriate cybersecurity training is provided commensurate with responsibilities: cybersecurity training for IT & OT staff and	[5,6,7,8,11]	\$313,411.80	Future	Medium	Train

		management; apprentice, mentorship, and next generation workforce development; cybersecurity consulting and virtual ISOs. Following the cybersecurity plan submission and approval, revised IJs and Project worksheets will be submitted that identify prioritized projects and refined descriptions/budgets. Federal share for this project is \$313,411.80 but may be revised with the updated IJ submission pending plan review and approval.					
--	--	--	--	--	--	--	--

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 Delaware has an approved Cybersecurity Plan that meets the SLCGP requirements.	1.1 Collaborate to draft Plan	Drafted Plan	CSO confirms draft plan is in Document Library
	1.2 Planning Committee approves Cybersecurity Plan	Signed letter by CSO	Committee Approval meeting minutes
	1.3 Submit the Plan to CISA	Confirmation of receipt	Upload via grants.gov
	1.4 CISA Approves Plan	Statement of Approval	CISA approves
2. Receive funding from SLCGP	2.1 Funding received to execute approved projects	Receipt of Funds	Accept and expend with approval from State Clearinghouse
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

Program Goal	Program Objectives	Associated Metrics	Metric Description (details, source, frequency)
4.Process services for local entities the request inclusion	4.1 Enroll local entities in services	Number of entities enrolled in each approved project	Financial reporting via SAA
	4.2 Communicate service offerings to local entities	Number of communities contacted Number of communities participating/responding	Based on feedback from CSO messages/meetings
5. Review, Revise, and update plan for next Fiscal year as required	5.1 Repeat objectives for Goal 1 for subsequent fiscal year	See Program Goal 1	See Program Goal 1

Signature: *Michael Hojnicky*
Michael Hojnicky (May 5, 2023 09:04 EDT)

Email: michael.hojnicky@newcastlede.gov










DE_SLCGP_CyberPlan_Final

Final Audit Report

2023-05-05

Created:	2023-05-04
By:	Sandra Alexander (Sandra.Alexander@delaware.gov)
Status:	Signed
Transaction ID:	CBJCHBCAABAA0F4WXrHTY1Q4ugqb-pO2DU30XAkKRt0Z

"DE_SLCGP_CyberPlan_Final" History

-  Document created by Sandra Alexander (Sandra.Alexander@delaware.gov)
2023-05-04 - 12:25:13 PM GMT
-  Document emailed to Solomon Adote (solomon.adote@delaware.gov) for signature
2023-05-04 - 12:26:43 PM GMT
-  Email viewed by Solomon Adote (solomon.adote@delaware.gov)
2023-05-04 - 12:33:25 PM GMT
-  Document e-signed by Solomon Adote (solomon.adote@delaware.gov)
Signature Date: 2023-05-04 - 12:33:54 PM GMT - Time Source: server
-  Document emailed to michael.hojnicki@newcastlede.gov for signature
2023-05-04 - 12:33:55 PM GMT
-  Email viewed by michael.hojnicki@newcastlede.gov
2023-05-05 - 12:59:42 PM GMT
-  Signer michael.hojnicki@newcastlede.gov entered name at signing as Michael Hojnicky
2023-05-05 - 1:04:35 PM GMT
-  Document e-signed by Michael Hojnicky (michael.hojnicki@newcastlede.gov)
Signature Date: 2023-05-05 - 1:04:37 PM GMT - Time Source: server
-  Agreement completed.
2023-05-05 - 1:04:37 PM GMT