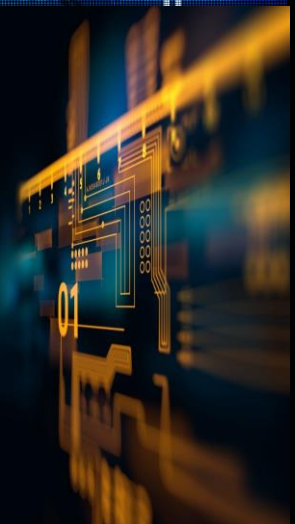

WISCONSIN CYBERSECURITY PLAN

December 2024

Approved by the Cybersecurity Subcommittee on 01/16/2025
Version 2.0

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LETTER FROM THE CO-CHAIRS OF THE CYBERSECURITY SUBCOMMITTEE

Greetings,

As the Co-Chairs for the Cybersecurity Subcommittee of the State of Wisconsin Homeland Security Council, we are pleased to present to you the updated 2022 – 2025 State of Wisconsin Cybersecurity Plan ("Cybersecurity Plan"). The Cybersecurity Subcommittee has been designated as the Cybersecurity Planning Committee for the purposes of the U.S Department of Homeland Security's (DHS) State and Local Cybersecurity Grant Program (SLCGP). The Cybersecurity Plan represents Wisconsin's continued commitment to improving cybersecurity and supporting state and local government entities throughout Wisconsin. The purpose of this plan is to meet the requirements of the SLCGP.

Representatives from local units of government, K-12 and postsecondary education, public health agencies, public safety agencies, tribal, and critical infrastructure 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 increasing our resilience against cyber threats and implementing cybersecurity best practices through programs that directly benefit the represented entities in Wisconsin. They are designed to support our entity in planning for new technologies and navigating the ever-changing cybersecurity landscape to reduce the state's cybersecurity risk and incorporate federal requirements.

As we continue to enhance the state's cybersecurity posture, 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,

Trina Zanow
State of Wisconsin CIO
Wisconsin Department of Administration
Co-Chair, Cybersecurity Subcommittee

COL Jeannie Jeanetta
Chief of Staff, Joint Staff
Wisconsin National Guard
Co-Chair, Cybersecurity Subcommittee

INTRODUCTION

The Cybersecurity Plan is a multi-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, Roles, and Responsibilities:** Describes the current roles, responsibilities, and governance mechanisms for cybersecurity within Wisconsin; successes, challenges, and priorities for improvement are also presented. This section includes the strategy for the cybersecurity program and the organizational structure that identifies how the state's cybersecurity program is supported. The Cybersecurity Plan is a guiding document and does not create any authority or direction over state or local systems or agencies.
- **Feedback and input:** Describes how inputs were collected and have been incorporated from representatives from local units of government, K-12 and postsecondary education, public health agencies, public safety agencies, tribal, and critical infrastructure and will reduce the overall cybersecurity risk across the eligible entity. Throughout this document **State of Wisconsin Cities, Counties, Municipalities, Towns, and Villages will be referenced as local governments**
- **Cybersecurity Plan Elements:** Outlines technology and operations needed to maintain and enhance resilience across the state's cybersecurity landscape.
- **Funding:** Describes funding sources and allocations to build cybersecurity capabilities in Wisconsin along with methods and strategies for sustained funding to meet long-term goals.
- **Implementation Plan:** Describes Wisconsin's plan to implement, maintain, and update the Cybersecurity Plan to enable continued evolution of and progress toward the identified goals. The implementation includes the resources and timeline where practicable.
- **Metrics:** Describes how Wisconsin will measure the outputs and outcomes of the program across the entity.

This plan aligns with and references the following:

- State of Wisconsin 2024 - 2026 Strategic IT Plan
- State of Wisconsin 2023 – 2026 Homeland Security Strategy (not publicly available)
- State of Wisconsin Cybersecurity Policies and Standards[1]

[1] https://det.wi.gov/Pages/policies.aspx

Vision and Mission

This section describes Wisconsin's vision and mission for improving cybersecurity:

Vision:

Establish an inclusive culture of cyber awareness and cyber resilience in partnership with the federal government, local units of government, tribes, K-12 school districts and postsecondary education, and publicly owned critical infrastructure to prevent and deter cyberattacks.

Mission:

Help protect the State of Wisconsin by educating its citizens regarding cybersecurity threats by increasing awareness, aligning with cybersecurity best practices, and deploying resources to maximize return on investment.

Cybersecurity Program Goals and Objectives

Wisconsin Cybersecurity goals and objectives include the following:

Cybersecurity Program	
Program Goal	**Program Objectives**
1. **Improve K-12 and postsecondary education, local units of government, tribes and publicly owned critical infrastructure capability and capacity to adopt and use best practices and methodologies to enhance cybersecurity.**	1.1 Recommend risk assessments be performed for all critical infrastructure, K-12 schools and postsecondary education, tribes and local units of government.
	1.2 Provide technical assistance to update local endpoints in line with cybersecurity best practices.
	1.3. Provide direct access to CISA, MS-ISAC and CIS baselines for all K-12 schools and postsecondary education, tribes, local units of government, and publicly owned critical infrastructure entities.
2. **Increase K-12 and postsecondary education, local units of government, tribes and publicly owned critical infrastructure understanding of cybersecurity best practices.**	2.1 Recommend local units of government, K-12 and post-secondary education, tribes, and publicly owned critical infrastructure enroll in MS-ISAC and EI-ISAC.
	2.2 Increase local units of government, K-12 and postsecondary education, tribes, and publicly owned critical infrastructure usage of Baseline and Enhanced Baseline for endpoints and information systems.
3. **Ensure personnel are appropriately trained in cybersecurity.**	3.1 Make cybersecurity awareness training available to local units of government, K-12 and postsecondary education, tribes, and publicly owned critical infrastructure.
	3.2 Provide low-cost alternatives and grants for local units of government, K-12 and postsecondary education, tribes, and publicly owned critical infrastructure employees to receive cybersecurity training including certification tracks.

CYBERSECURITY PLAN ELEMENTS

Manage, Monitor, and Track

The Wisconsin Department of Administration's Division of Enterprise Technology (DET) has established comprehensive cybersecurity policies and standards based on National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 5 to govern management, monitor, and track State of Wisconsin executive branch agency information systems, applications, and user accounts. State of Wisconsin executive branch agencies must follow these policies and standards and may establish procedures to implement the policies and standards within their agency. Pursuant to State law, the University of Wisconsin System, the Wisconsin Legislative Branch, and the Wisconsin Judicial Branch are not required to follow DET cybersecurity policies and standards and have established their own cybersecurity policies and standards. Operationally however, DET works very closely with all Wisconsin entities, and assists in response to cyber incidents that affect any of these entities. As part of this plan, DET is providing access to NIST Policies and Standards, CISA, MS-ISAC, and CIS as example cybersecurity baselines and configurations for these entities. These include one for standard operations and one that incorporates minimum controls needed for information systems that process, store, or transmit protected information like personal identifiable information (PII), protected health information (PHI), etc.

Monitor, Audit, and Track

Asset owners, asset custodians, and information security and privacy officers throughout the state should:

1. Ensure the information assets under their purview are assessed for security and privacy risks and configured to ensure that event logging is enabled to provide an adequate level of situational awareness regarding potential threats to the confidentiality, integrity, availability, and privacy of their data and information systems; and
2. Review and retain event logs in compliance with applicable federal, state, local and tribal laws, regulations, and contractual requirements.

DET is providing access to the above referenced baselines for implementation and access to NIST 800.53 revision 5 policies and standards to demonstrate adherence to these requirements.

Enhance Preparedness

The State is working with local units of government, K-12 and postsecondary education, tribes, and publicly owned critical infrastructure to adopt a continuous risk management framework to identify, assess, and monitor risks that can adversely impact operations, information systems, and data. The State has established standards for this framework through the State Homeland Security Strategy, State Emergency Response Plan, State Energy Security Plan, and State Prevention and Protection Plan. In turn, these standards inform the creation and maintenance preparedness, incident response, and continuity of operations plans.

Assessment and Mitigation

Wisconsin needs to continue establishing a continuous risk assessment framework to protect endpoints and information systems by identifying, assessing, and mitigating risks that could adversely impact state and local government operations. This framework is codified for Executive Branch agencies through cybersecurity policies and standards. The State incorporates lessons learned into this framework from internal assessments, as well as external audits and assessments from the Wisconsin Legislative Audit Bureau (LAB) and federal organizations like the Cybersecurity and Infrastructure Security Agency (CISA), the Internal Revenue Service (IRS), the Social Security Administration (SSA), Criminal Justice Information Systems (CJIS) the Federal Bureau of Investigation (FBI), and others.

Best Practices and Methodologies

The State has established policies and standards which create minimum requirements for all Executive Branch agency endpoints and information systems, including heightened requirements for endpoints and information systems that process, store, or transmit protected information. Protected information includes any information whose confidentiality, integrity, or availability is governed by one or more legal, regulatory, or contractual requirements. Examples include personally identifiable information, Social Security numbers, federal tax information, protected health information, criminal justice information, educational information, classified national security information, or payment card information.

The State of Wisconsin will make available technical resources to assist local units of governments, K-12 school districts and postsecondary education, tribes and publicly owned critical infrastructure with remediation of endpoints and information systems in alignment with the example cybersecurity baselines being developed. These baselines, which will be developed from the security policies and standards required for Executive Branch agency endpoints and information systems, will enable all entities to quickly implement and continuously maintain cybersecurity best practices to protect critical endpoints and information systems. The State of Wisconsin will work with the local units of government, K-12 school districts and postsecondary education, tribes, and publicly owned critical infrastructure to determine the best paths to conduct assessments of tribes their own endpoints and information systems to identify their level of compliance with these baselines. Using a risk-based review process, the State intends to identify the entities with the highest level of risk and work with those entities to remediate those challenges.

The “Baseline” for Executive Branch agencies and the other entities will incorporate a comprehensive set of cybersecurity best practices derived from NIST Special Publication 800-53 Revision 5, including implementation of multi-factor authentication, implementation of enhanced logging, implementation of data encryption for data at rest and in transit, ending usage of unsupported/end-of-life software and hardware that is accessible from the internet, and establishing system backups. The State will also provide guidance on enhanced password policies for these endpoints and information systems, including a prohibition on the use of known, fixed, or default passwords and credentials.

The “Enhanced Baseline” for Executive Branch agencies and other entities will incorporate additional security and privacy controls beyond those required in the “Baseline” to meet legal, regulatory, or contractual requirements for endpoints and information systems that process, transmit, or store protected information.

The State has an ongoing project which has already transitioned more than 500 local units of government to utilize the .gov internet domain. As part of our ongoing communications about these efforts, an overview session was provided last fall and grant participants continue to be informed and receive information on how to transition to the .gov domain.

Safe Online Services

As noted in the prior section, the State of Wisconsin has an ongoing effort to transition all eligible government entities to use the .gov internet domain to increase the trustworthiness of online state and local government services. Included below are links to resources that have been created to support those efforts:

Moving to .gov | get.gov

WI Domain Service Request - WI DET - Wisconsin.gov

Continuity of Operations

The State will continue to work with local units of government to develop, implement, test, and maintain contingency plans to ensure continuity of operations for all information systems that deliver or support essential functions on behalf of the State of Wisconsin. Ensuring availability for essential systems and components allows entities to meet legal, regulatory, and contractual requirements to ensure continuous delivery of government services. This will include working with local units of government, K-12 school districts and postsecondary education, tribes and publicly owned critical infrastructure to enhance backup capabilities. This work will occur outside the SLCGP grant.

Workforce

Wisconsin is operating several programs that are not part of the State and Local Government Cybersecurity (SLCGP) grant to enhance our cybersecurity workforce. In 2022, the State initiated a workforce recruitment and retention program, which updated job descriptions, job requirements, and required skills for cybersecurity positions to enhance recruitment and retention. The State is also launching multiple training and growth opportunities for the cybersecurity workforce and partnering with K-12 and post-secondary education partners to increase the availability of cybersecurity education and training programs.

Continuity of Communications and Data Networks

The State of Wisconsin has emergency continuity of operations plans. The State, through Wisconsin Emergency Management and the Wisconsin Department of Administration, is actively working to further enhance continuity of operations planning. This effort includes improvement of existing plans, as well as development, implementation, testing, and maintenance of contingency plans to ensure continuity of operations for all information systems that deliver or support essential or critical functions. Local units of government, K-12 school districts and postsecondary education, tribes and publicly owned critical

infrastructure are responsible for the creation of emergency continuity of operations plans for their jurisdictions.

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

All major information systems, applications, and support systems operated by or on behalf of the State of Wisconsin undergo security assessments to ensure adequate security and privacy controls are implemented and utilized. The State also manages risks to acceptable levels. Risk management processes include identifying, assessing, and addressing security and privacy risks throughout system lifecycles.

The State operates under two primary types of cybersecurity assessments: internal and external. Internal assessments are completed by the State to informally assess its posture and educate other entities and organizations about potential gaps in regulatory compliance. External assessments are conducted by regulatory agencies, including CISA, DHS, IRS, FBI, LAB, and others.

This program is overseen by the State Chief Information Officer (CIO) and State Chief Information Security Officer (CISO), who are responsible for coordination with the federal government and other regulatory agencies.

Cyber Threat Indicator Information Sharing

The Wisconsin Statewide Intelligence Center (WSIC), which is operated by the Wisconsin Department of Justice, provides cyber threat indicator information broadly to Wisconsin organizations. WSIC also conducts targeted notifications and shares indicators in close coordination with trusted third parties, including federal partners like DHS (specifically CISA and Homeland Security Investigations - HSI) and the FBI. WSIC is currently working with the Wisconsin Department of Administration and Wisconsin Homeland Security Council to enhance automated, on-demand access to threat indicators. The WSIC works in partnership with the Southeastern Wisconsin Threat Analysis Center, a fusion center that serves Jefferson, Kenosha, Milwaukee, Ozaukee, Racine, Walworth, Washington, and Waukesha counties. The WSIC serves all other portions of the state.

The Cyber Threat Intelligence Group (CTIG), which consists of partners from government, private-sector, education, and critical infrastructure, also shares tactical information about cybersecurity incidents, vulnerability and exploit trends, and other relevant information.

Department Agreements

DET develops memorandums of understanding (MOU) to establish data sharing agreements with other entities. DET will continue to expand these partnerships where necessary to facilitate information flow. All entities entering into data sharing agreements must agree that they are appropriate, relevant, timely, and address any privacy and cybersecurity considerations.

Leverage CISA Services

Many local units of government, K-12 school districts and postsecondary education, tribes and publicly owned critical infrastructure in Wisconsin already take advantage of the cybersecurity assessment services provided by CISA, which will continue and expand in the future. Wisconsin has developed its own capability to assist with CISA assessments by utilizing training offered through the Assessment Evaluation and Standardization program to qualify Critical Response Team (CRT)members to perform the Cyber Resilience Review, External Dependencies Management, and Risk and Vulnerability Assessment.

CRT members will continue to qualify additional assessors and ensure that eligible organizations are aware of these services along with those offered by CISA through community outreach programs. Through this grant, the State will continue to encourage local units of government, K-12 school districts and postsecondary education, tribes and publicly owned critical infrastructure enroll in vulnerability scanning and web application scanning as appropriate.

Information Technology and Operational Technology Modernization Review

The State of Wisconsin's strategic approach is to ensure alignment between information technology and operational technology cybersecurity objectives. Though the funding to protect these systems comes from many sources, the State does not distinguish between the controls applied to information technology and operational technology. SLCGP participants may also replace end-of-life/outdated equipment through existing State enterprise contracts to receive competitive pricing and technical support.

Cybersecurity Risk and Threat Strategies

The Cybersecurity Subcommittee will use this plan to develop and coordinate projects and strategies to address cybersecurity risks and threats with other organizations, including local units of government, K-12 school districts and postsecondary education, tribes publicly owned critical infrastructure, and State agencies to solicit and receive input from their membership.

Rural Communities

Rural communities will have adequate access to projects and grants under the SLCGP through their representation on the Cybersecurity Subcommittee, planning workgroup, and through targeted outreach specific for rural communities.

FUNDING & SERVICES

The Wisconsin Department of Military Affairs' Division of Emergency Management is the State's Administrative Agency (SAA) appointed by the Governor to manage and administer the SLCGP grant. As such, the SAA will approve and manage the grant framework in accordance with the federal Notice of Funding Opportunity (NOFO) and will work with the Wisconsin Department of Administration to ensure project design and implementation is in accordance with the requirements and intent of the NOFO. In addition, the SAA will establish the subrecipient application process embedded within the state's Egrants application and management system.

The SLCGP is managed and serviced by the SAA.

Distribution to Local Governments

To ensure 80% of the SLCGP funds are distributed to local units of government, K-12 school districts and postsecondary education, tribes, and publicly owned critical infrastructure, the State of Wisconsin will leverage existing local units of government and associated consortia.

Examples of external partners include, but are not limited to:

- Wisconsin Department of Public Instruction
- Wisconsin Department of Natural Resources
- Wisconsin Public Service Commission
- Cooperative Educational Service Agencies

- Wisconsin Water Works Association
- Wisconsin Counties Association
- Wisconsin Towns Association
- Wisconsin Educational Technology Leaders Association
- Wisconsin Healthcare Emergency Readiness Coalition

Depending on the type and quantity of subgrantee applications that are received and prioritized for funding, the SAA, other state agencies, or regional agencies may contract for services directly on behalf of these entities with their consent. Alternatively, the SAA may issue direct subawards to these entities or use a combination of these strategies. The SAA will ensure that at least 25% of funds or equivalent dollar value of services are directed to rural communities and at least 80% of funds are either passed through to these entities or utilized to provide services that benefit them with their consent. All project requests must align with the projects listed in Appendix B. A detailed list of program goals, objectives, and desired outcomes are listed in Appendix A for reference.

ASSESS CAPABILITIES

The Cybersecurity Subcommittee used Appendix A to assess and document capabilities for the cybersecurity plan elements in this plan. To assess the capabilities of local units of government, K-12 school districts and postsecondary education, tribes, and publicly owned critical infrastructure, the State will be conducting assessments of potential grant subrecipients as part of the grant application process. Their responses will inform the State's determination of their capabilities and provide a source of information for the State's risk-based review process.

IMPLEMENTATION PLAN

Organization, Roles, and Responsibilities

The State of Wisconsin's Homeland Security Council (HSC) is a 16-member council responsible for advising the Governor on homeland security issues. The HSC has established a Cybersecurity Subcommittee to coordinate cybersecurity issues within State government and liaise with local units of government, K-12 school districts and postsecondary education, tribes and critical infrastructure sectors throughout Wisconsin.

Governor Tony Evers has empowered the Cybersecurity Subcommittee to act as the planning committee for Wisconsin's SLCGP grant program and the Wisconsin Department of Military Affairs to act as the State Administrative Agency (SAA) for management and administration of the SLCGP grant.

The Cybersecurity Subcommittee is well-positioned as an influential driver of cybersecurity policy in Wisconsin and works closely with federal, state, and local partners to enhance our cybersecurity posture. This plan integrates and complements our State's recently updated Homeland Security Strategy and Statewide Strategic IT plan.

The Cybersecurity Subcommittee currently includes the following members:

- Trina Zanow, State Chief Information Officer, Wisconsin Department of Administration (Co-Chair)
- COL Jeannie Jeanetta, Chief of Staff, Joint Staff, Wisconsin National Guard (Co-Chair)
- Lucas Munz, Chief Information Officer, Wisconsin Department of Public Instruction
- Marshall Ogren, Special Agent in Charge, Wisconsin Department of Justice
- Robert Kehoe, Deputy Administrator, Wisconsin Elections Commission
- Ed Murphy, Chief Information Security Officer, University of Wisconsin System
- Ed Snow, Chief Information Security Officer, Educational Communications Board
- Jay Schaefer, Cybersecurity Architect, Winnebago County
- Jennifer Mueller, Chief Information Security Officer, Wisconsin Department of Health Services
- Mary Beth Lewis, Director, Enterprise Security and Compliance, WEC Group
- Ruhamah Bauman, Director, Bureau of Operations and Planning Support, Wisconsin Emergency Management
- Jason Neilitz, Chief Information Officer, Sokaogon Chippewa Community

The cybersecurity subcommittee has convened grant-related workgroups to ensure comprehensive representation from the different entities that will receive grant funding. These workgroups will provide input throughout the grant lifecycle and help rank programmatic priorities.

The Wisconsin Department of Military Affairs, in its capacity as the SAA for this grant, will report on open/active grant programs to the Cybersecurity Subcommittee at least quarterly. This includes obtaining appropriate consent and funding approvals from grant subrecipients for grant services they receive.

Resource Overview and Timeline Summary

The Wisconsin Departments of Administration and Military Affairs are providing staff resources to ensure the successful execution of this grant and are currently working to determine how best to provide services under the grant. The Department of Military Affairs received partial non-federal matching funds for the upcoming biennium and will determine how best to fulfill the remaining non-federal match requirement. The State of Wisconsin has submitted a non-federal match waiver request for its FY2022 and FY2023 grant award, both of which have been approved.

The State is actively working with the Wisconsin League of Municipalities; Wisconsin Towns Association, Wisconsin Counties Association; Wisconsin Department of Public Instruction; Wisconsin Department of Natural Resources; Wisconsin Public Service Commission; Wisconsin Department of Agriculture, Trade, and Consumer Protection; and other partners to leverage their existing relationships with certain categories of grant subrecipients to advise the core grant team on the execution of the grant process.

METRICS

Program Goal	Program Objectives	Metric Description
1. Improve K-12 school districts and postsecondary education, local units of government, tribes, and publicly owned critical infrastructure capability and capacity to adopt and use best practices and methodologies to enhance cybersecurity.	1.1 Recommend risk assessments be performed for all critical infrastructure, K-12 schools and postsecondary education, tribes and local units of government.	Number of sites assessed per fiscal year.
	1.2 Provide technical assistance to update local endpoints in line with cybersecurity best practices.	Number of local units of government, K-12 school districts and postsecondary education, tribes and publicly owned critical infrastructure assisted per fiscal year. Number of endpoints remediated per fiscal year.
	1.3. Provide direct access to CISA, MS-ISAC and CIS baselines for all K-12 schools and postsecondary education, tribes, local units of government, and publicly owned critical infrastructure entities.	Completion of task.
2. Increase K-12 school districts and postsecondary education, local units of government, tribes, and publicly owned critical infrastructure understanding of cybersecurity best practices	2.1 Recommend local units of government, K-12 and post-secondary education, tribes, and publicly owned critical infrastructure enroll in MS-ISAC and EI-ISAC.	Number of local units of government enrolled in MS-ISAC per fiscal year. Number of local units of government enrolled in EI-ISAC per fiscal year.
	2.2 Increase local units of government, K-12 and postsecondary education, tribes, and publicly owned critical infrastructure usage of Baseline and Enhanced Baseline for endpoints and information systems.	Number of local units of government adopting Baseline and Enhanced Baseline for endpoints and information systems.
3. Ensure personnel are appropriately trained in cybersecurity.	3.1 Make cybersecurity awareness training available to local units of government, K-12 and postsecondary education, tribes, and publicly owned critical infrastructure.	Number of participating entities by fiscal year. Number of employees completing training by fiscal year.
	3.2 Provide low-cost alternatives and grants for local units of government, K-12 and postsecondary education, tribes, and publicly owned critical infrastructure employees to receive cybersecurity training including certification tracks.	Number of local government employees receiving cybersecurity certifications.

APPENDIX A: CYBERSECURITY PLAN CAPABILITIES ASSESSMENT

COMPLETED BY State of Wisconsin				STATUS
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) *(If applicable – as provided in Appendix B)*	In Progress Pending Complete
1. Manage, monitor, and track information systems, applications, and user accounts	Incomplete implementation across state and local government entities.	Foundational	1	In Progress
2. Monitor, audit, and track network traffic and activity	Incomplete implementation across the totality of state and local government entities.	Foundational	1	In Progress
3. Enhance the preparation, response, and resiliency of information systems, applications, and user accounts	Incomplete implementation across the totality of state and local government entities.	Foundational	1	In Progress
4. Implement a process of continuous cybersecurity risk factors and threat mitigation. practices prioritized by degree of risk	Incomplete implementation across the totality of state and local government entities.	Foundational	1	In Progress
5. Adopt and use best practices and methodologies to enhance cybersecurity (references NIST)	Incomplete implementation across the totality of state and local government entities.	Foundational	1	In Progress

COMPLETED BY State of Wisconsin				STATUS
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) *(If applicable – as provided in Appendix B)*	In Progress Pending Complete
a. Implement multi-factor authentication	Incomplete implementation across the totality of state and local government entities.	Foundational	1	In Progress
b. Implement enhanced logging	Incomplete implementation across the totality of state and local government entities.	Foundational	1	In Progress
c. Data encryption for data at rest and in transit	Incomplete implementation across the totality of state and local government entities.	Foundational	1	In Progress
d. End use of unsupported/end of life software and hardware that are accessible from the Internet	Incomplete implementation across the totality of state and local government entities.	Foundational	1	In Progress
e. Prohibit use of known/fixed/default passwords and credentials	Incomplete implementation across the totality of state and local government entities.	Foundational	1	In Progress
f. Ensure the ability to reconstitute systems (backups)	Incomplete implementation across the totality of state and	Foundational	1	In Progress

COMPLETED BY State of Wisconsin				STATUS
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) *(If applicable – as provided in Appendix B)*	In Progress Pending Complete
	local government entities.			
g. Migration to the .gov internet domain	Incomplete implementation across the totality of state and local government entities.	Foundational	1	In Progress
6. Promote the delivery of safe, recognizable, and trustworthy online services, including using the .gov internet domain	Incomplete implementation across the totality of state and local government entities.	Foundational	1	In Progress
7. Ensure continuity of operations including by conducting exercises	Incomplete implementation across the totality of state and local government entities.	Foundational	n/a year one	In Progress
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 state and local government entities.	Foundational	2, 3	In Progress
9. Ensure continuity of communications and data networks in the event of an	Incomplete implementation across the totality of state and	Foundational	1	In Progress

COMPLETED BY State of Wisconsin				STATUS
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) *(If applicable – as provided in Appendix B)*	In Progress Pending Complete
incident involving communications or data networks	local government entities.			
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 state and local government entities.	Foundational	1	In Progress
11. Enhance capabilities to share cyber threat indicators and related information between the eligible entity and the Department	Incomplete implementation across the totality of state and local government entities.	Foundational	1	In Progress
12. Leverage cybersecurity services offered by the Department	Incomplete implementation across the totality of state and local government entities.	Foundational	1	In Progress
13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and	Incomplete implementation across the totality of state and local government entities.	Foundational	n/a year one	Pending

COMPLETED BY State of Wisconsin				STATUS
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) *(If applicable – as provided in Appendix B)*	In Progress Pending Complete
operational technology cybersecurity objectives				
14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats	Incomplete implementation across the totality of state and local government entities.	Foundational	2, 3	In Progress
15. Ensure rural communities have adequate access to, and participation in plan activities	Incomplete implementation across the totality of state and local government entities.	Foundational	2, 3, 5	In Progress
16. Distribute funds, items, services, capabilities, or activities to local governments	Incomplete implementation across the totality of state and local government entities.	Foundational	2, 3, 5	In Progress

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 **Appendix A: Sample Cybersecurity Plan Capabilities Assessment**. This table reflects what was planned for FFY22 funding.

	Project Name	Project Description	Related Required Element #	Cost	Status	Priority	Project Type
1	Technical Assistance to Local Units of Government, K-12 and postsecondary education, tribes, and publicly owned critical infrastructure	This project will provide technical assistance to bring local endpoints in alignment with cybersecurity best practices.	1, 2, 3, 4, 5 (a) – (g), 6, 9, 10, 11, 12, 14, 15, 16	$2,755,000	Future	High	Equip
2	Increase Local Units of Government, K-12 and postsecondary education, tribes, and publicly owned critical infrastructure Understanding of Cybersecurity Best Practices	Encourage local government adoption of cybersecurity best practices and resources.	8, 15, 16	$50,000	Ongoing	High	Train
3	Cybersecurity Certifications	This project will make grants available to local government employees to receive cybersecurity certifications.	8, 15, 16	$550,500	Future	High	Train
4	Program Manager	Program administration	15, 16	$200,000	Future	High	Organize, Plan
5	SAA M&A	Grant administration	15, 16	$189,000	Future	High	Organize

6	Cybersecurity Plan	Development and approval of the State's cybersecurity plan.	15, 16	$50,000	Ongoing	High	Plan

APPENDIX C: ENTITY METRICS

See Metrics section above.