CyberOhio

State of Ohio
Comprehensive Cybersecurity Plan

January 30, 2025

Developed by the Ohio Comprehensive Cyber Planning Committee
with support from
the Cybersecurity and Infrastucture Security Agency (CISA)

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

MIKE DEWINE
GOVERNOR OF OHIO

CyberOhio

77 S. High Street, 30th Floor
Columbus, OH 43215
www.governor.ohio.gov

January 9, 2025

Kirk M. Herath
Cybersecurity Strategic Advisor
77 S. High Street, 30th Floor
Columbus, Ohio 43215

Dear Cybersecurity Partner,

As the Cybersecurity Strategic Advisor (CSA) to the Governor of the State of Ohio, I am pleased to present to you the 2025 Ohio Comprehensive Cybersecurity Plan. The CSA is authorized under Executive Order 2022-7D to coordinate all cybersecurity activities across Ohio. Our updated Ohio Comprehensive Cybersecurity Plan meets the requirements of the current U.S. Department of Homeland Security guidelines for the State and Local Cybersecurity Grant Program (SLCGP).

Over the past two years, Ohio has made great strides in improving cybersecurity. Some highlights include:

- Launching the Ohio Persistent Cybersecurity Improvement initiative, a cybersecurity training and readiness service that supports counties and other local government entities as they develop cybersecurity programs:
- Establishing the Ohio Cyber Integration Center, a one-call, 24 x 7 resource for local government entities experiencing a cybersecurity event, including activation of the Ohio Cyber Reserve;
- Publishing the state-wide Cybersecurity Incident Plan and testing it with 100 participants from across the State of Ohio; and.
- Launching the Ohio Digital Academy, an innovative approach to hiring and training the next generation of cybersecurity professionals.
- Providing grants to local governments to migrate to a .Gov domain, purchase cybersecurity software, and incent collective security arrangements.

Finally, I would like to thank the Ohio Comprehensive Cyber Planning Committee and Executive Committee leaders who dedicated so much innovation, passion, resources, and creativity to create the 2025 Ohio Comprehensive Cybersecurity Plan. Their years of leadership establishing and driving strong cybersecurity practices serves as the foundation of our plan. Now, we are ready to take the next step in our roadmap to expand and evolve cybersecurity practices across state and local communities.

Best,

Kirk M. Herath
Cybersecurity Strategic Advisor to Governor Mike DeWine

VERSION HISTORY

Version Number	Date	Change Summary
1.0	1/5/2023	Original Ohio Comprehensive Cybersecurity Plan (OCCP)
2.0	1/30/2025	• Removed references to untraceable requirements throughout the document. • Changed the tense of the document from future to present, as many initiatives are no longer planned, but currently underway. • Changed the name of the committees from HSAC-Cyber Executive and Planning Committees to the Ohio Comprehensive Cyber Planning Committee (OCCPC) and Ohio Comprehensive Cyber Executive Committee ((OCCEC). • Updated the OCCP goals throughout the document. • Split the previous Capabilities Assessment, which was Appendix A, into two documents (now Appendix A and Appendix B) to facilitate reporting on Ohio Counites and State Agencies separately.

INTRODUCTION

The Ohio Comprehensive Cybersecurity Plan (OCCP) is a key component to helping Ohio build cyber resilience. Our two-year plan consists of all five functions of the cybersecurity framework: identify, protect, detect, respond, and recover. Ohio incorporated existing plans, structures, and other relevant efforts to update our plan. Building upon existing structures and capabilities allows Ohio to provide governance and a framework to meet critical cybersecurity needs while making the best use of available resources.

Vision and Mission

Ohio's vision and mission for improving the maturity of cybersecurity practices across state and local entities:

Vision:

In partnership with state, local, and critical infrastructure entities, expand, and evolve cybersecurity training and practices to anticipate, prevent, defend, and recover from cybersecurity incidents.

Mission:

Provide a "whole-of-state" approach by leveraging existing and new committees, partnerships, and working groups focused on maturing cybersecurity practices and incident response across the State of Ohio. When such groups – public, private, military, and educational experts – combine their experience and dedication, all Ohioans benefit from the resulting state-wide advances in cybersecurity practices, education, and workforce development.

Governance

The Governor's Cybersecurity Strategic Advisor and Ohio Homeland Security (OHS), under the authority of EO2022-7D, and the Ohio Homeland Security Advisory Council (HSAC) formed a Cybersecurity (HSAC-Cyber) Grant Planning Committee. The HSAC-Cyber Grant Planning Committee approved the Ohio Comprehensive Cybersecurity Plan. To simplify and better align to our mission, forthwith, the State of Ohio's SLCGP planning committees are now named the Ohio Comprehensive Cyber Planning Committee (OCCPC) and Ohio Comprehensive Cyber Executive Committee (OCCEC). These committees operate under the HSAC charter.

Purpose

The purpose of OCCPC and the OCCEC includes:

- Delineating current roles and responsibilities for state agencies, elected officeholders, and local government entities, who collaborate on cybersecurity activities across Ohio.
- Identifying state-level and scalable cybersecurity capabilities that can be beneficial to local governments in reducing cybersecurity risk and speed recovery.
- Documenting processes for collaboration and reporting before, during, and after a cybersecurity incident.
- Assessing and understanding county-level cybersecurity practices and preparedness, using the State Cyber Assessment (part of the Stakeholder Preparedness Report).
- Completing the Cybersecurity Capability Assessment.
- Establishing goals, owners, and performance measures for the two-year Comprehensive Cybersecurity Plan.

This Plan is the result of the combined efforts of staff from the following:

- CyberOhio
- Innovate Ohio
- Ohio Adjutant General's Office
- Ohio Attorney General's Office
- Ohio counties
- Ohio Department of Administrative Services
- Ohio Department of Education and Workforce
- Ohio Department of Higher Education
- Ohio Department of Public Safety
- Ohio Governor's Office
- Ohio K-12 schools, colleges and universities,
- Ohio Secretary of State's Office
- U.S. Department of Homeland Security
- Other local government entities

CYBERSECURITY PLAN ELEMENTS

The 2025 OCCP Goals

- Sustain the Ohio Cyber Integration Center (SLCGP and State of Ohio funded)
- Support Local Government Entities
- Expand the Ohio Persistent Cybersecurity Improvement Ecosystem (SLCGP funded)
- Leverage Internet Service Provider Capabilities (State of Ohio funded)
- Provide Affordable Access to Cybersecurity Services (State of Ohio funded)
- Grant Funding for .Gov Migrations and Cybersecurity Services (SLCGP funded)
- Strengthen Cybersecurity Practices for Small Business (SBA and State of Ohio funded)
- Expand and Evolve Cybersecurity Practices Across State Agencies (State of Ohio funded)
- Conduct Cybersecurity Maturity Security Assessments
- Enhance Incident Response Practices
- Strengthen Cybersecurity Practices of Water and Waste-Water Treatment Facilities (State of Ohio Funded)
- Planning and Grant Management Contractor Services (SLCGP funded)

Manage, Monitor, and Track

For this two-year Plan, the Contractor to Support the OCCP organizes the OCCPC and the OCCEC which focus on maturing local governments cybersecurity knowledge and processes by expanding ongoing training and planning, cyber incident exercise, and cybersecurity information sharing. The Contactor will publish meeting minutes and project plans to ensure progress on the OCCP goals.

Monitor, Audit, and Track

The OCCEC is responsible for monitoring, auditing and tracking the OCCP goals. Each goal owner is responsible for publishing a project plan to document the steps and timeline to achieve the committed outcomes defined in the OCCP. The OCCEC reviews and approves the project plans and metrics. To monitor the progress of the goal owners, the OCCEC meets monthly with each goal owner providing an update of progress in the past month. Additionally, the goal owners provide an update of progress in the quarterly OCCPC meetings.

Each goal owner uses specific tools, processes, and procedures to monitor, audit and track progress of their projects. The goal owners share the metrics and reporting from these with the Committees to highlight progress.

DAS has existing processes to monitor, audit, and track network traffic and activity for state agencies. Additionally, the Office of the Governor and Department of Administrative Services are collaborating on initiatives to mature these practices across state agencies. The Cybersecurity Risk Council will oversee and govern this initiative. For this two-year Plan, the State of Ohio is funding this initiative.

The Innovate Ohio Platform provides a Digital Identity for State of Ohio user accounts, including employees, contractors, and citizens. This Digital Identity capability allows the State to monitor, audit, and track user account activity, proof identities to prevent fraud, and enforce multi-factor authentication.

For this two-year Plan, the Committees will focus on maturing local government cybersecurity knowledge and processes by expanding ongoing training, cyber incident exercise, and cybersecurity information sharing which all support local entities. Additionally, Goal 2 will increase access to cybersecurity services to state, county and local entities using its network. The Plan Goals focus heavily on network security, network monitoring, and information sharing. As the Goal Leads achieve their respective program objectives, they will report their progress and outcomes to the Committees. Ohio has the capability to monitor, audit, and track. demonstrating that the plan meets requirement.

Enhance Preparedness

The OCCPC and OCCEC continue activities to enhance preparation, response, and resiliency against cybersecurity risks and attacks. The Plan goals focus on expanding ongoing training, cyber incident exercise, and cybersecurity information sharing, which all support local entities and will mature preparedness practices statewide. Additionally, the OCCEC coordinates the annual Tabletop Exercise for a large-scale cybersecurity incident. Stakeholders from across the State of Ohio are invited to join the annual Tabletop Exercise, including, local government entities. State of Ohio agencies, Ohio Secretary of State, and Ohio businesses and nonprofits.

Additionally, the Department of Administrative Services has existing practices to prepare and respond to cybersecurity risks and threats across state agencies, boards, and commissions. The Department of Administrative Services also leads collaboration sessions with other elected officeholders, including Secretary of State, Auditor of State, Attorney General, Ohio Treasurer, etc.   Through these activities, the State of Ohio prepares, investigates and responses to cybersecurity incidents.

Lastly, the Ohio Cyber Integration Center and the Ohio Emergency Management Agency, work with local government entities and emergency responders to conduct regular incident response tests.

Assessment and Mitigation

The OCCP focuses on expanding ongoing training, cyber incident exercise, and cybersecurity information sharing which all support local entities. One outcome of the goals is to improve local entity assessment and mitigation, and the OCCEC monitors performance measures indicating improved maturity for vulnerability assessment and mitigation. Through these efforts Ohio supports and expands the capability to train, assess cybersecurity vulnerabilities, and mitigate threats.

The Ohio Cyber Reserve under the Adjutant General's Office currently provides assessment and mitigation services by request to state and local government entities.

The Department of Administrative Services has existing assessment and mitigation practices prioritized by degree of risk which are required for all state agencies, boards, and commissions.

Best Practices and Methodologies

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) forms the foundation of the State of Ohio Comprehensive Cybersecurity Plan. The Plan supports local adoption and use of best practices and methodologies to enhance cybersecurity to ensure that the state, and local governments within the state, adopt and use the best practices outlined below within a reasonable timeline:

- Implement multi-factor authentication
- Implement enhanced logging and endpoint detection
- Data encryption for data at rest and in transit

- End the use of unsupported and end-of-life software and hardware that are accessible from the Internet
- Prohibit use of known/fixed/default passwords and credentials
- Ensure the ability to reconstitute systems (e.g., backups)
- Migration to the .gov Internet domain

Ohio has the capability to incorporate cybersecurity best practices and methodologies statewide.

The Committees follow NIST Cybersecurity Framework (CSF) 2.0 practices. The Plan goals focus on expanding ongoing training, cyber incident exercise, collective defense, and cybersecurity information sharing which all support local entities. An anticipated outcome of the goals will be to improve local entity understanding of and adherence to NIST CSF 2.0. The OCCEC monitors performance measures indicating improved maturity for NIST CSF 2.0 and the 16 elements.

Supply Chain Risk Management

Governments across the State of Ohio rely on vendors to provide a myriad of services to deliver their missions to serve Ohioans. The OCCP's goals incorporate training and recommendations for developing supply chain risk management programs.

Tools and Tactics

The Department of Administrative Services has existing processes to monitor, audit, and track network traffic and activity for state agencies. Additionally, the Office of the Governor and Department of Administrative Services are collaborating on initiatives to mature these practices across state agencies. The Cybersecurity Risk Council will oversee and govern this initiative. For this two-year Plan, the State of Ohio is funding the Council initiative.

Partnerships

The State of Ohio engages with MS-ISAC, CISA, cybersecurity vendors, and other cybersecurity organizations to continuously improve cybersecurity best practices. Among others, employees from the Office of Information Technology, the Department of Public Safety, the Secretary of State's Office, and other state agencies participate in government and cybersecurity conferences and liaise with cybersecurity professionals from federal, state, and private entities to share indicators of compromise, best practices, and threat intelligence.

Safe Online Services

All state agencies, boards, and commissions are required to use the ohio.gov domain per policy. Local government entity adoption of ohio.gov domain is ongoing. Members of the Committees have an approach to provide safe, recognizable, and trustworthy online services using the ohio.gov internet domain for counties. The Committees are successfully using SLCGP funds to expand the use of the .Gov domain through grants and continues to promote the use of the .Gov domain to local government entities.

Continuity of Operations

The Department of Administrative Services' Office of Business Continuity provides support and solutions and offers guidance to State agencies on the development of viable, comprehensive Continuity of Operations Plans (COOP) and business continuity programs. This is accomplished by management of a singular, business continuity web-based planning tool, available to all state agencies, boards, and commissions. In addition, the office provides for an electronic state employee emergency notification system and is the DAS liaison with the State Emergency Operations Center.

OCCP goals focus on expanding ongoing training, cyber incident exercise, encouraging collective defense through cyber grants, and cybersecurity information sharing which all support local entities. An anticipated outcome of the goals will be to improve local entity continuity planning, and incident response preparedness, and the OCCEC monitors performance measures indicating improved maturity for continuity of operations planning.

The Committees will continue to promote continuity planning support and services to state and local entities

Workforce

Ohio uses the National Initiative for Cybersecurity Education (NICE) Workforce Framework to identify and mitigate any gaps in Ohio's cybersecurity workforce. This includes enhancing recruitment and retention efforts, as well as bolstering state and local personnel's knowledge, skills, and abilities to address cybersecurity risks and threats.

CyberOhio has established the Ohio Digital Academy to cultivate an innovative environment, and a skilled workforce primed to meet the advanced technology and cybersecurity needs of Ohio's public and private-sector employers. The Academy seeks to create an IT workforce pipeline by training and employing early entrants to the industry and setting a path for successful careers in high demand fields, focusing on cybersecurity. As of the publishing of this plan, 26 cybersecurity professionals have participated in the Academy.

Additionally, the Ohio Department of Education and Workforce actively supports the development of cybersecurity and information technology curriculum for K-12 students and has an ongoing pilot to sponsor up to five high school level cyber academies across the State of Ohio. This initiative ensures that students are exposed to and engaged in learning opportunities that prepare them for future technology challenges. In partnership with the Ohio Department of Higher Education, both agencies also support Ohio's many Career Technical Education (CTE) programs for students in grades 7-12 and for High School Graduates and Adult Learners. These programs aim to equip students with the competencies necessary for success in higher education and future careers in cybersecurity and information technology. Finally, the Ohio Cyber Range Institute, funded jointly by the Ohio Adjutant General's Office and the Ohio Department of Higher Education is a scalable cloud platform used to teach cyber courses at colleges, universities, and High and Tech Schools.

The Ohio Technology Consortium (OH-TECH), a division of The Ohio Department of Higher Education, is similarly dedicated to advancing education, workforce development, scientific research and innovation for Ohio. Composed of three organizations — OARnet, OhioLINK and the Ohio Supercomputer Center (OSC) — OH-TECH propels Ohio's knowledge economy through the creation and adoption of next-generation technology and information solutions.

Continuity of Communications and Data Networks

Ohio has the ability to ensure cross-jurisdictional continuity of communications and data networks in the event of an incident involving those communications or data networks. The Ohio Academic Resources Network (OARnet) provides network services with over 5000 miles of fiber optic cable, currently featuring six major rings and 59 Points-of-Presence that extend across the state to most of Ohio's population. Additionally, The Department of Administrative Services operates the Multi-Agency Radio Communication System (MARCS), a statewide, secure, and reliable public service wireless communication for public safety and first responders.

The Ohio Cyber Incident Plan provides instructions for communication during an incident and how to handle situations where the secure and preferred communication method is unavailable. The Communication and Information Management System (CIMS) will be used for information sharing. Traffic

Light Protocol (TLP) will be used when sharing incident information. The TLP is a set of designations used to ensure that sensitive information is only shared with appropriate audiences.

In addition, the preference is to use State of Ohio communication methods such as desk phones, mobile phones provided by the State of Ohio, and Microsoft tools (e.g., Teams and Outlook). However, if these are unavailable, personal mobile phones and Google tools may be used.

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

The Department of Administrative Services supports state agencies operating within the 16 critical infrastructure sectors. The Office of Information Security and Privacy provides cybersecurity and risk management tools and services for these agencies. The State of Ohio is also developing processes and procedures to comply with future Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) requirements. In the meantime, the state continues to work with regional CISA Cyber Security Advisors to communicate and report on cybersecurity risks and threats.

The Ohio Emergency Management Agency (Ohio EMA) conducts a federally required Threat and Hazard Identification and Risk Assessment (THIRA) every three years and Stakeholder Preparedness Review (SPR) with all 88 counties on an annual basis. Ohio EMA utilizes the Comprehensive Preparedness Guide (CPG) 201, Third Edition, which provides guidance for conducting a THIRA and SPR. The THIRA/SPR assesses Ohio's capabilities across five mission areas (Prevention, Protection, Mitigation, Response, Recovery) in 32 core capabilities, one of which is Cybersecurity. This state assessment process is used to target federal and state funding to mitigate, to the greatest degree possible, cybersecurity risks and threats relating to critical infrastructure and key resources (such as power and telecommunications) that may impact the performance of information systems statewide.

Leverage Cybersecurity and Infrastructure Security Agency (CISA) Services

The State of Ohio participates in the CISA Cyber Hygiene services for web application scanning and vulnerability scanning and maintains memberships in MS-ISAC and EI-ISAC. The Ohio Department of Public Safety and the Ohio Department of Administrative Services both participate in the National Cybersecurity Review (NCSR). As part of this Comprehensive Cybersecurity Plan, CyberOhio, the Ohio Emergency, Management Agency and CISA partner to conduct an annual statewide test of the Ohio Cyber Incident Plan.

The Committees continuously promote local adoption of CISA free cybersecurity services through outreach efforts through state and federal partnerships.

Cyber Threat Indicator Information Sharing

The OCCPC and OCCEC promote partnership between CISA and local government entities. The State of Ohio shares cyber threat indicators of compromise and related information through various lines of effort, including leveraging CISA's Cyber Information Sharing and Collaboration Program (CISCP), CISA's Automated Indicator Sharing capability and systems and subscribing to and participating in the MS-ISAC Real-Time Indicator Feeds or other applicable systems and processes to share cyber threat indicators and related information. The Department of Public Safety, Department of Administrative Services, and the Adjutant General launched the Ohio Cyber Integration Center, a one-stop service for incident response and threat information sharing.

Information Technology and Operational Technology Modernization Review

Today, the State of Ohio uses the procurement and architecture review processes to assess alignment between information technology and operational technology. Additionally, the Committees continuously promotes modernization review processes to local government entities to ensure cybersecurity controls are in place for both information technology and operational technology. Local government entities can leverage negotiated contracts from the state and OH-TECH. Additionally, the Committees promote the use of state aggregate purchasing contracts for cyber capabilities for all local governments, including K-12's.

Cybersecurity Risk and Threat Strategies

The Committees regularly review cybersecurity risk and threat information provided by the Department of Administrative Services, CISA and other sources. The Committees use this information in the creation of the strategy and goals.

Additionally, the Department of Administrative Services conducts an annual risk assessment, which includes a threat assessment and controls assessment, to determine cybersecurity priorities and projects. Additionally, the State of Ohio subscribes to different threat intelligence services and partners with suppliers and cybersecurity organizations to deploy protective measures against these threats. The State of Ohio also partners with CISA and other federal law enforcement agencies to share threat intelligence.

Rural Communities

The OCC Plan and goals have a dedicated focus on rural communities (those with less than 50,000 residents). Goal owners engage rural communities in cybersecurity activities, services, and programs to ensure they have adequate access to and are able to participate in cybersecurity activities. Here are a few examples.

Rural communities rely on the OARnet network, consisting of more than 5,500 miles of fiber-optic backbone operating at ultrafast 100 Gbps speeds across the entire state. The network blankets the state, providing connectivity to Ohio's colleges and universities, K-12 schools, public broadcasting stations, academic medical centers, government agencies, and partnering research organizations.

Rural communities take advantage of the Ohio Cyber Incident Plan and contact the Ohio Cyber Integration Center for cybersecurity incident support, including deploying the Ohio Cyber Reserve to assist during cyber incidents. The Ohio Cyber Integration Center also assists with cyber assessments, information sharing, and connections with other state and federal resources. Ohio EMA provides pre-incident planning, training and exercise resources. The Ohio Cyber Reserve provides cybersecurity assessment and response services to rural communities. The Ohio Persistent Cyber Improvement program provides almost 30 hours of free cyber training and tabletop exercises to local governments.

The work led by Ohio in the Ohio Cyber Range Institute, which connects the Cybersecurity Range to Regional Programming Centers reaches every corner of the state of Ohio. Using the Cyber Range, colleges, K-12 and local entities conduct cybersecurity exercises to test their ability to respond to and recover from a cybersecurity event.

The Ohio Persistent Cyber Improvement (O-PCI) program offers FREE cybersecurity training to all local governments in Ohio, with a focus on rural communities.

Distribution to Local Governments

The section below describes how Ohio is distributing funds, items, services, capabilities, or activities to local governments, including distributing at least 25% of cybersecurity grant funding to rural areas. The table in **Appendix C: Project Summary Worksheet** lists items, services, capabilities, or activities that Ohio provides to local governments.

The State of Ohio developed state projects to provide cost effective and scalable cybersecurity services to local governments, including rural communities. These services include, but are not limited to, assessments, audits, continuity planning, response planning, exercises, and skill enhancement for local entities. These state projects build upon established statewide programs that provide high quality services that engage with local governments, including in rural areas.

Project 1 - Ohio Cyber Integration Center (OCIC) - Initial funding by SLCGP

Build and maintain the Ohio Cyber Integration Center (OCIC) for reporting, threat analysis, secure information sharing, and outreach activities to support local governments in Ohio. As a component of the Statewide Terrorism Analysis and Crime Center (STACC) and in partnership with the Adjutant General, the OCIC mission is to build a collaborative, operational and interdisciplinary model for cybersecurity that transforms Ohio's ability to protect against cyber threats, promote information sharing, coordinate response efforts, and provide cybersecurity education and outreach.

Through strategic, technical and tactical analysis, services provided by the OCIC include vulnerability notifications to organizations; written intelligence products on cyber threats and tactics, techniques and procedures (TTP); incident response support; sharing federal, state and local partner cyber products; and fulfilling requests for service such as providing information to other agencies or briefing on current cyber issues.

Project 2– Support Local Government Entities

Ohio Persistent Improvement (O-PCI) - Funding by SLCGP

Ohio is providing services to local governments in lieu of direct funding through the Ohio Persistent Cyber Improvement (O-PCI) ecosystem, administered by the Ohio Cyber Range Institute (OCRI) oversees five distinct categories of measurable performance (4 main performance measure categories and one subset performance measure category):

Persistent Cyber Improvement curriculum covers basic, standard, and advanced elements (gateways 1,2,3) of cyber security awareness and practice through a combination of learning and doing through courses, training requirements, and exercises. Each gateway requires the completion of curriculum objectives in the form of courses, requirements, and exercise participation.

Leverage Internet Service Provider Capabilities

The Ohio Academic Resources Network (OARnet) delivers technology-based solutions that reduce costs, increase productivity, and improve customer service through increased access to affordable broadband service, reduced the cost of technology through aggregate purchasing, and maximized shared services opportunities.

OARnet services include access to affordable bandwidth, aggregate pricing for Vulnerability Management services, distributed denial-of-service (DDoS) mitigation, and domain name service (DNS) management.

Provide Affordable Access to Cybersecurity Services

CyberOhio is working with vendors to reduce licensing and services costs to local governments. Recent victories include negotiating reduced rates for Endpoint Detection and Response (EDR) and Multi-Factor Authentication (MFA) solutions.

OARnet is working to expand the services that they currently provide to Ohio local government entities. A Request for Proposal (RFP) was released in 2024 seeking to add twelve cybersecurity services to the OARnet catalogue. These services will provide a wide range of cyber security options for local governments to choose from.

Grant Funding for .Gov Migrations and Cybersecurity Software and Services

The OCCPC and OCCEC continue to support Dot Gov migration projects and cybersecurity software and services projects for local governments. In 2024, CyberOhio received approx. 300 applications requesting assistance with approx. 475 projects from local governments to support cybersecurity initiatives across Ohio.

Project 3 – Strengthen Cybersecurity Practices for Small Businesses – SBA and State Funded

The OCCEC has been working with the Ohio State University, who received a grant through the Small Business Administration (SBA) to provide security training to small businesses. The OCRI-Regional Programming Center at OSU has been collaborating with the OCRI at the University of Cincinnati, and the O-PCI program, to leverage Ohio investments such as the OCRI Learning Management System (LMS) built at UC. This collaboration is helping to reduce costs.

Project 4 – Expand and Evolve Cybersecurity Practices Across State Agencies – State Funded

Conduct Cybersecurity Risk Assessments

DAS Office of Information Security and Privacy (OISP) has established processes to assess state agencies to the NIST CSF and regularly report on progress addressing identified risks. DAS continues to deploy tools and services to state agencies to share in the responsibility to reduce risk to state government. Additionally, OISP has implemented processes to formally evaluate state IT suppliers and the risk they introduce to state agencies, and work with them to address those risks.

Enhance Incident Response Practices

DAS OISP is continuously enhancing practices surrounding cyber and privacy incident response. This includes formalizing and testing plans and procedures, establishing vendor relationships prior to incidents, sharing threat information, and exercising response and recovery plans with state agencies.

Project 5 – Strengthen Cybersecurity Practices at Water and Waste-Water Treatment Facilities (State Funded)

The OCCPC and OCCEC are committed to assisting public and private critical infrastructure partners in securing their systems, with a focus on water and waste-water treatment facilities. Many of these critical systems are connected to the Internet making them vulnerable to cyber-attacks. CyberOhio has been working with the Ohio Environmental Protection Agency (OEPA) to coordinate and assist water and waste-water facilities with uplifting their cybersecurity maturity.

Project 6 – Planning and Grant Management Contractor Services

Contractor services are needed to support CyberOhio in the execution of the statewide Comprehensive Cybersecurity Plan, as required by the SLCGP. The contractor facilitates committee meetings; publishes agendas, meeting minutes, notes, project plans, and weekly status reports; serves as the grant program manager; develops and reviews grants applications for local governments to apply for funding; and supports Ohio EMA grant administrators in collecting data for annual reporting.

ASSESS CAPABILITIES

Appendix A: Cybersecurity Plan Capabilities Assessment was originally created to assess capabilities for the 16 required plan elements outlined above. The OCCPC decided to break out the Assessment into two sections, one for State Agencies and another for Ohio Counties. The assessment is a key factor in determining the Cybersecurity Plan Elements and Goals.

See Appendix A for summary of element maturity levels for Ohio Counties.

See Appendix B for summary of element maturity levels for State Agencies in Ohio.

IMPLEMENTATION PLAN

Organization, Roles, and Responsibilities

In this section, Ohio denotes the individual responsibilities of appropriate entities within the State of Ohio and its local governments in implementing the plan.

Ohio Executive Offices: Roles and Responsibilities in Cybersecurity

Ohio Governor's Office

CyberOhio coordinates the efforts of state agencies under the Governor's authority and leads the collaboration with other state offices and branches, counties, and local governments, academic institutions, and critical infrastructure partners to protect Ohio's information technology infrastructure and data across sectors. CyberOhio, led by the Cybersecurity Strategic Advisor to the Governor, is responsible for coordinating and guiding Ohio's wide-ranging cybersecurity efforts across all state executive branch agencies. Leveraging risk assessments and threat intelligence, CyberOhio's Cybersecurity Strategic Plan sets the direction for Ohio to expand and evolve cybersecurity practices across state agencies. The team also establishes uniform reporting standards on cybersecurity programs, resiliency, and preparedness to help state agencies make risk-based decision that support their mission while protecting Ohio systems and citizens.

CyberOhio fosters the cybersecurity preparedness and resiliency of local entities, including rural communities, through initiatives, such as the State and Local Cyber Grant Program administered by CISA. Another CyberOhio-led initiative occurs in partnership with OARnet, Ohio's fiber-optic backbone covering over 5,500 miles across the state~~,~~ lowering broadband access costs. The Affordable Access to Cybersecurity Services initiative uses aggregated purchasing to lower the cost of cybersecurity tools for local entities. Additionally, the Cybersecurity Strategic Advisor partners closely with the Ohio Cyber Range Institute (more information below) and the Ohio Cyber Reserve, which provide~~s~~ a myriad of programs to help local entities practice and improve their cyber response capabilities.

CyberOhio collaborates with public and private entities on initiatives to support cybersecurity workforce development to inject skilled cybersecurity experts into the workforce. CyberOhio and Ohio Department of Public Safety partnered to update and test Ohio's state-wide Incident Plan. Part of this activity includes establishing a central "one-stop" team to intake, assess, and help remediate cybersecurity incidents at local and critical infrastructure entities. CyberOhio also works closely with federal partners including CISA, U.S. Department of Homeland Security, and the Federal Bureau of Investigation.

Governor's Office of Workforce Transformation (OWT)

The Governor's Office of Workforce Transformation (OWT) sets the strategy for workforce development in Ohio and coordinates with Ohio's state agencies and partners that impact the workforce. Led by Lt. Governor Jon Husted, OWT works closely with the Governor's Executive Workforce Board, state partners, and local communities to meet the needs of job seekers and businesses. OWT's mission is to connect Ohio's business, training, and education communities to build a dynamically skilled, productive, and purposeful workforce. OWT manages the implementation of the state's TechCred program to upskill the current cybersecurity workforce. The office also establishes new cybersecurity recruitment pipelines through two state supported internship programs, the High School Tech Internship pilot program and the Diversity & Inclusion Technology Internship program in partnership with the Ohio Department of Development and Ohio Department of Education.

State Agencies: Roles and Responsibilities in Cybersecurity

Ohio Adjutant General (ADJ)

As part of its homeland defense mission, the Adjutant General's Department of Ohio is leading several efforts in Ohio to protect state and local government, critical infrastructure, businesses and private citizens from cyber threats and attacks.

- Ohio Cyber Reserve (OhCR) – ORC 5922 authorizes the Ohio Cyber Reserve as a volunteer force under the command of the Adjutant General. OhCR teams of experienced civilians are available for the Governor to assist eligible municipalities with cybersecurity assessments and to provide recommendations to reduce cyber threats. OhCR volunteers provide workforce development to train the current and future cyber workforce. Additionally, the OhCR will provide incident response teams to support municipal organizations dealing with cyberattacks.
- Ohio Cyber Range (OCR) - The Ohio Cyber Range is a secure virtual environment used for cybersecurity training and technology development. OCR is accessible for competitions, training, and as a testing environment for schools, governments and businesses. The OCR is managed through the Ohio Cyber Range Institute (OCRI), created in 2017 under a Memorandum of Agreement between the ADJ, Ohio Department of Higher Education (ODHE) and University of Cincinnati (UC) to manage the OCR through the OCRI. Range Core Service Sites are located at the UC and the University of Akron, with an additional 21 regional programming centers (RPC) throughout the state.
- Ohio National Guard Cyber Force - Ohio National Guard's cyber force supports and defends state agencies and critical infrastructure in Ohio. These Citizen-Soldiers and -Airmen leverage their military-specific training with cyber expertise they bring from their civilian jobs to assist in emergency cyber response.
- Air National Guard Cyber Warfare Wing - the U.S. Air Force announced that the Mansfield Air National Guard Base, home of the 179th Airlift Wing, has been selected as the preferred site for the Air National Guard's first Cyber Warfare Wing. Once it is operational, it will be an invaluable resource to the State of Ohio's cyber capabilities.

Ohio Cyber Range Institute (OCRI) Executive Committee and Advisory Board

- The OCRI is a partnership between the University of Cincinnati, the Ohio Department of Higher Education and the Ohio Adjutant General's Department to explore and demonstrate the use of an Ohio Cyber Range. Featuring two core service sites and 21 regional programming centers (RPC) throughout the state, it develops education modules to support instructors which includes learning resources and labs that utilize the Ohio Cyber Range virtual environment. The OCRI also conducts Cyber Education Bootcamps, and cyber exercises to train students, members of the Ohio Cyber Reserve, and state and local government employees. The OCRI Executive Committee oversees budgetary issues, reviews applications for new RPCs, and maintains the MOA between the ADJ, ODHE and UC to manage the OCR through the OCRI. An Advisory Board provides external input on programming. https://www.ohiocyberrangeinstitute.org/

Ohio Department of Administrative Services (DAS)

DAS provides the services listed below for all state agencies. When local government entities experience a cyber incident, DAS contacts the entity to determine if there could be an impact to state agencies. If so, DAS launches an investigation and takes action to protect state agencies and state data. Broadly, the Office of Information Security and Privacy is divided into the following sections:

- Cyber Operations provides tools and services to monitor state agency environments and detect inappropriate or unauthorized activities. The team provides vulnerability management tools and analysis, supports secure implementation of cloud services, conducts penetration tests and table top exercises. Using a myriad of cybersecurity tools, the team analyzes threat intelligence, contains systems to protect state data.
- Governance Risk & Compliance (GRC) team assesses and reports on cybersecurity maturity, risk and policy adherence across state agencies. The team also supports audits from multiple regulatory authorities and assesses the risk of state suppliers as part of the procurement process.
- Agency Information Security Officers - cybersecurity ambassadors who help agencies assess, prioritize and mitigate, cybersecurity risk in the agency. This team also works on cybersecurity incidents.
- Incident Response – a cross-functional team convenes to investigate suspected unauthorized access to or acquisition of state systems or data. This team works with federal partners and the Ohio Cyber Integration Center.
- Identity and Access Governance – a team of cybersecurity experts who support identity and access management activities across state agencies and drive adherence to state policies and standards.
- Privacy team - responsible for evaluating agreements that pertain to utilization of data for their intended purpose, evaluating incidents from a breach and liability perspective, and performing agency-wide cyber training efforts.

Ohio Department of Higher Education (ODHE)

ODHE develops cybersecurity and information technology curriculum for adult education. It is also a partner in the Ohio Cyber Range Institute.

OARnet is a division of the ODHE's Ohio Technology Consortium that serves Ohio's education, health care, public broadcasting and government communities by centralizing technology hardware, software, and network requirements needed to support overall community connectivity.

Ohio Department of Public Safety (ODPS)

ODPS has four divisions with active roles in cybersecurity: Information Technology (IT), Homeland Security (OHS), State Highway Patrol (OSP), and the Ohio Emergency Management Agency.

- The IT department maintains the Security Operations Group (SOG) and provides Law Enforcement Automated Data System (LEADS) oversight. The SOG supports internal system security at DPS and assists in external cyber incidents as requested.
- OHS maintains cyber intel analysts in the OCIC and staff to support cybersecurity education and outreach activities and provide strategic, technical and tactical analysis. Utilizing Ohio’s state fusion center - the Statewide Terrorism Analysis & Crime Center (STACC) and the OCIC, OHS facilitates cyber incident reporting and information sharing, to include addressing cyber mis/dis-information, providing vulnerability notifications, and intelligence briefings.
- The OSP Computer Crimes Unit (CCU) provides training and support for the investigation of crimes involving computers or other digital devices. Investigators conduct forensic examinations of submitted evidence and occasionally conduct direct investigations of crimes involving computers or state databases.

- Ohio EMA provides expertise in planning, training and exercises to prepare for and respond to cyber incidents and maintains the Ohio Cyber Incident Plan. Ohio EMA is the current State Administrative Agency (SAA) for FEMA grants and manages and distributes the SLCGP grant funds.

Ohio Homeland Security Advisory Council (HSAC)

Established under ORC 5502, the HSAC operates under the direction of the Director of the Ohio Department of Public Safety to provide advice on homeland security issues, including funding efforts. The HSAC Cybersecurity workgroup undertakes various projects as needed. The Ohio Comprehensive Cyber Planning Committee (OCCPC) operations under the HSAC charter.

Ohio Statewide Interoperability Executive Committee (SIEC)

Originally established under Governor's Executive Order 2012-07K, the SIEC provides the strategic direction and alignment for those responsible for interoperable and emergency communications at the state, regional, and local levels. A cybersecurity committee was established in mid-2021 and is included as a goal in the Ohio Statewide Communication Interoperability Plan (SCIP). https://siec.ohio.gov/

Other Elected Office Holders

Ohio Secretary of State (SOS)

Currently, staffing for cybersecurity is:

- Chief Information Security Officer - Accountable for all cyber initiatives. Responsible for providing the strategic roadmap for the cyber program and responsible for governance programs.
- Cybersecurity Operations Manager - Accountable for all cyber operations. Responsible for the maturation of the cyber operations program.
- Cybersecurity Liaison (4) - Responsible for consulting with county boards of elections and county technical points of contacts and developing their assigned region's cyber posture. Responsible for responding to cyber alerts from counties in their regions.
- Cybersecurity Engineer (2) - Responsible for the implementation, operation, maintenance, and maturation of all cyber security tools.
- Cybersecurity Analyst (2) - Responsible for monitoring, responding to, and vetting alerts in the organization.

The Secretary of State's office assists county boards of elections and their information technology staff with cybersecurity support.

The Secretary of State's Cyber Defense Team serves as the primary point of contact for incident response for county boards of election, coordinates with OCIC, the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), and the CISA.

Other Contributing Collaborative Entities

InfraGard

InfraGard is a partnership between the Federal Bureau of Investigation (FBI) and members of the private sector for the protection of U.S. Critical Infrastructure. https://www.infragard.org/

Law Enforcement Roles

The investigation of cyber-related crimes is very complex with no one agency having full jurisdiction or authority in the state of Ohio. In Ohio the following organizations would be involved in an investigation:

Local Police Department

Record and report initial details of cyber-crimes, preserve evidence, and inform the appropriate state or federal law enforcement agencies and cyber response partners. Respond to cybercrime on a very localized level but many lack the resources to investigate complex cyber cases.

County Sheriff's Office

Record and report initial details and preserve evidence of cyber-crime that crosses city jurisdictions and within a given county but many lack the resources to investigate complex cyber cases. Inform the appropriate state or federal law enforcement agencies and cyber response partners.

State

OSP Computer Crimes Unit: Investigates all cyber-crime related to state owned or leased property. Provides augmentation to local, state and federal organizations who do not have cybercrime investigatory capabilities.

OAG – Bureau of Criminal Investigations Cyber Crimes Unit: Provides augmentation to both local and state-level law enforcement organizations who do not have cybercrime investigatory capabilities.

Federal

FBI: Focuses on all cybercrime that rises to the level in which they will investigate, including foreign threat actors, large-scale RICO cases against large cybercrime syndicates or APTs, or if the case has multiple victims across state lines.

Secret Service: Focuses on cybercrime from a financial perspective.

Homeland Security Investigations: Involved as needed for terrorist activity related to cybercrimes; provides augmentation as needed.

Other Supporting Government Resources for Law Enforcement

DHS CISA https://www.cisa.gov/

The Law Enforcement Cyber Center (LECC) https://www.iacpcybercenter.org/

Cybercrime Support Network (CSN) https://cybercrimesupport.org/

Resource Overview and Timeline Summary

The teams responsible for leading and implementing the Cybersecurity Program Goals and meet Program Objectives is listed in the Cybersecurity Program Goals and Objectives.

Each goal and its associated objectives have a timeline with a target completion date, and one or more owners that are responsible for overseeing and coordinating its completion. Accomplishing goals and objectives requires support and cooperation from numerous individuals, groups, or agencies, and are added as formal agenda items for review during regular governance body meetings. The Cybersecurity and Infrastructure Security Agency's (CISA) Service Catalog[1] of technical assistance is available to assist with the implementation of the OCCP. Technical assistance (TA) requests are to be coordinated through the CISA Stakeholder Engagement Branch.

Based on the discussions during the OCCP Workshop, CISA recommends the following TAs to support State of Ohio OCCP goals:

- CISA led a Tabletop Exercise in 2024 to test the Ohio Cyber Incident Plan.
- A Tabletop Exercise is planned for 2025.

[1] CISA Services Catalog | CISA

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

APPENDIX C: PROJECT SUMMARY WORKSHEET

Purpose: The Project Summary Worksheet is a list of cybersecurity projects that the OCCPC expects to complete to develop or improve any needed cybersecurity capabilities identified in Appendix A: Sample Cybersecurity Plan Capabilities Assessment – Ohio Counties, and Appendix B: Sample Cybersecurity Plan Capabilities Assessment – State of Ohio Agencies. The Comprehensive Cybersecurity Plan is a 2-year plan. Projects funded or intended to be funded under SLCGP have start and end dates consistent with the grant period of performance. Projects intended to be funded through state funds have start and end dates consistent with the implementation of the 2-year OCCP. Project types are in line with Planning, Organization, Equipment, Training and Exercise (POETE) elements.

	Project Name	Project Summary	Target start and end dates	Cost	Status	Priority	Project Type
1.	Sustain Ohio Cyber Integration Center (OCIC)	Build and maintain current capabilities in strategic analysis, incident reporting, secure information sharing, and outreach activities. Build capabilities in technical and tactical analysis, alerts and warnings, suspicious activity reporting, risk assessment, and information linking. Support OhCR missions and assist with prioritizing critical infrastructure sectors. Expand partnerships and build relationships with key cyber partners, stakeholders, and the broader cyber community.	12/1/2023 – 11/30/2027	$2.5M (SLCGP funded)	Ongoing	High	Plan, Organize, Exercise
2.	Support Local Government Entities	Expand Ohio Persistent Cyber Improvement Ecosystem Leverage Internet Service Provider Capabilities Provide Affordable Access to Cybersecurity Services Grant Funding for .Gov Migrations and Cybersecurity Software Services	12/01/2022-11/30/2028 12/01/2022 – 11/30/2027	$7,680,979 (SLCGP funded) Funded by State of Ohio Funded by State of Ohio $10,553,905 (SLCGP funded)	Ongoing	High	Plan, Organize, Equip, Train, Exercise
3.	Strengthen Cybersecurity Practices for	Provide specific cyber training and awareness for small businesses	1/1/2023 – 12/31/2027	SBA and State of Ohio funded	Ongoing	High	Plan, Organize

	Small Businesses						
4.	Expand and Evolve Cybersecurity Practices Across State Agencies	Conduct Cybersecurity Risk Assessments Enhance Incident Response Practices	9/1/2022 – 12/31/2027	Funded by State of Ohio	Ongoing	High	Assess, Implement
5.	Strengthen Cybersecurity Practices at Water and Waste-Water Treatment Facilities	Provide funding for cybersecurity enhancements at water facilities Provide cyber training and awareness for water facilities	1/1/2023 – 12/31/2027	Funded by State of Ohio	Ongoing	High	Plan, Organize
6.	Planning and Grant Management Contractor Services	Contractor services are needed to support Ohio Homeland Security in the execution of the statewide Comprehensive Cybersecurity Plan, as required by the SLCGP.	12/1/2022-6/30/2026	$500,000 (SLCGP funded)	Ongoing	High	Plan, Organize

APPENDIX D: OHIO METRICS

The Appendix D Table documents performance measures and metrics for the 5 Goals included in Comprehensive Cybersecurity Plan. The lead for each Goal provides regular reporting to the OCCPC and OCCEC.

Goal	Description	Step	Performance Measure(s)
1.	Improve and enhance cybersecurity intelligence and information sharing across local, regional, state, and federal organizations	Sustain Ohio Cyber Integration Center (OCIC)	Build and maintain current capabilities in strategic analysis, incident reporting, secure information sharing, and outreach activities. Build capabilities in technical and tactical analysis, alerts and warnings, suspicious activity reporting, risk assessment, and information linking. Support OhCR missions and assist with prioritizing critical infrastructure sectors. Expand partnerships and build relationships with key cyber partners, stakeholders, and the broader cyber community.
		Identify partner equipment needs to engage remotely and securely with cyber operations center.	Secure funding to acquire and sustain necessary equipment for cyber operations center. Assess equipment needs annually for sustainment and/or gaps.
		Establish, continue to develop, and/or enhance partnerships with local, state and federal agencies and private businesses via the cyber operations center.	Maintain and build appropriate cyber partnerships for sharing cyber related information through trusted partner engagement processes (i.e., CyberOhio, O-PCI, Ohio Public Private Partnerships (OP3), Intelligence Liaison Officer (ILO).)
	1.2 Implement appropriate methods to improve secure information	Establish methods and policies to anonymize shared data to improve detection and protection.	Identify priority data sets and develop a process to anonymize incident response data to allow sharing with statewide stakeholders. Annually, provide analysis of cyber products posted to CIMS, OCIC Tip data, DAS incident data, elections-related cyber incident data, and

	sharing between local, state, and federal public and private partners to include predictive and anticipatory cybersecurity activities as well as response and investigatory activities.		any other relevant stakeholder data sets to develop visual analytic products to support an assessment of state cyber posture.
		Ensure the OCIC has the capability to rapidly and effectively analyze cyber information through training and partnerships.	Participate in fusion center cyber analyst training sponsored by the US Department of Homeland Security and/or provided by the Multi State Information Sharing and Analysis Center (MS-ISAC), FBI, and other partners. OCIC collaborates with partners to develop effective cyber intelligence processes, to be reviewed annually.
		Identify and utilize methods to improve federal information sharing flow.	Engage federal stakeholders to explore usage of information sharing tools within the cyber operations center (i.e., ThreatConnect, WISP, HiveIQ, the Cyber 9 Line, etc.).
		Coordinate information sharing and collaborative engagement opportunities to promote individual and community preparedness as it relates to cybersecurity best practices.	Annual Cyber assessment conducted by Ohio EMA as part of annual County Emergency Management Agencies Stakeholder Preparedness Review report. Includes questions that address history of any cyber incidents in the last year, and development history of jurisdiction's cybersecurity resiliency capabilities. Conduct annual Tabletop Exercise (TTX) to validate the Ohio Cyber Incident Plan reporting and response processes. TTX's involve key personnel/agencies from the emergency management community and stakeholder agencies. The exercise evaluation assesses the ability to meet objectives and capabilities of the Ohio Cyber Incident Plan by documenting strengths, areas of improvements, capability performance, and any corrective actions that need to be made for the plan.
2.	Support Local Government Entities		
	2.1 Expand a statewide Ohio Persistent Cyber Improvement ecosystem to scale cybersecurity	Expand and scale Ohio Cyber Range Institute capabilities to provide ongoing and persistent cybersecurity capabilities for Ohio LGE general employees, IT/cyber specialists and	Continue expanding number of local government entities in Gateway 1, 2, and 3. Provide OCCEC with reporting and utilization metrics.

	practices and exercises across Ohio for local government entities and critical infrastructure	executives/managers on cybersecurity skills.	
		Expand and scale Ohio Cyber Reserve to provide ongoing and persistent evaluation and testing of cybersecurity skills for Ohio LGEs.	Provide OCCEC with utilization metrics of Ohio Cyber Reserve.
	2.2 Leverage Internet Service Provider Capabilities	Expand adoption of OARnet broadband and security services to provide defense in depth protections for Ohio LGEs.	Increase LGE subscription to OARnet. Leverage OARnet provided pre-configured volumetric DDoS filters. Leverage OARnet provided DNS management.
	2.3 Provide Affordable Access to Cybersecurity Services	Increase access to affordable security services (including cloud-based services). Reduce the cost of security services and technologies through aggregate purchasing, and maximize shared services opportunities for OARnet members, partners and customers as required, in order to assist organizations with the Cyber Security Framework (CSF) functions to identify, protect, detect, respond, and recover their information systems and data.	Deployment/adoption of offered services. Number of new security services added Price reduction based on aggregation purchase (percentage reduction in TCO) Increase in adoption on a year-to-year basis
	2.4 Grant funding for .Gov Migrations and Cybersecurity	Develop metrics for grant program	Number of applications received Number of applications recommended for approval

	Software and Services		Funding Requests Rural LGEs supported Ohio Counties supported Types of projects supported
3.	Strengthen Cybersecurity Practices for Small Businesses	Develop and report metrics for small business cybersecurity training program	Provide OCCEC with reporting and utilization metrics.
4.	Expand and Evolve Cybersecurity Practices Across State Agencies		
	4.1 Conduct Cybersecurity Risk Assessments	Regularly assess state agencies to the NIST CSF and work to address identified gaps. Evaluate state agency IT suppliers and the risk they introduce to the state.	Agency cybersecurity maturity assessments Project status reports Cybersecurity governance reports showing adherence to NIST CSF Re-assessment of state agency cybersecurity program Supplier Risk Assessments
	4.2 Enhance Incident Response Practices	Enhance Cyber and Privacy Incident Response Practices. Formalize, test, and improve processes throughout the full lifecycle of cyber incidents.	After-Action Reports Plans and Playbooks

5.	Strengthen Cybersecurity Practices at Water and Waste-Water Treatment Facilities	Identify the current level of cybersecurity maturity at water and waste-water treatment facilities and match appropriate resources to effectively strengthen cybersecurity practices.	Track the number of facilities engaged. Identify the current level of need either through assessments, a grant application process, or a similar process. Monitor cybersecurity uplift as measured by either assessment, grant monitoring, or a similar process.
6.	Planning and Grant Management Contractor Services	Schedule and support OCCPC and OCCEC meetings, subcommittee meetings, and workgroup meetings	Meeting agendas, minutes and notes Project plans Weekly status reports Support annual FEMA reporting Coordinate OCCP updates Coordinate with vendors

APPENDIX E: MAPPING OF THE CIS CONTROLS AND SAFEGUARDS TO NIST CSF

The Ohio Department of Administrative Services Office of Information Security and Privacy (OISP) maintains a crosswalk mapping of the CIS Controls and NIST CSF. The NIST CSF 2.0 forms the foundation of the State of Ohio Cybersecurity Program, and the Office of Information Security and Privacy uses CIS to controls to validate a state agency's compliance with NIST CSF 2.0.

The OCCPC and OCCEC promote the use of the CIS Controls and NIST CSF to local entities and critical infrastructure.

APPENDIX F: FACILITATING AND SUPPORTING AGENCIES

FACILITATING AGENCY: Ohio Department of Public Safety (ODPS), Division of Homeland Security (OHS)

SUPPORT AGENCIES: Governor Mike DeWine's office

City of Dayton

City of Hilliard

Columbus City Schools

Erie County

Franklin County

Greater Cincinnati Waterworks

Henry County

Hocking County

Perry County

Management Council

Northeast Ohio Regional Fusion Center (NEORFC)

Ohio Academic Resources Network (OARnet)

Ohio Adjutant General's Department (ADJ), Ohio National Guard (OHNG)

Ohio Association of Chiefs of Police (OACP)

Ohio Cyber Range Institute (OCRI)

Ohio Department of Administrative Services (DAS)

Ohio Department of Education and Workforce (ODEW)

Ohio Department of Higher Education (ODHE)

Ohio Department of Health (ODH)

Ohio Emergency Management Agency (Ohio EMA)

Ohio Hospital Association

Ohio Office of Budget and Management (OBM)

Ohio Public Library Information Network (OPLIN)

Ohio State Highway Patrol (OSHP)

Ohio Secretary of State's Office (SOS)

Ohio Technology Consortium

Ohio Water/Wastewater Agency Response Network (OH WARN)

Orange City School District

Shaker Heights City Schools

Innovate Ohio

APPENDIX G: ACRONYMS

Acronym	Definition
AAR	After Action Reports
BCI	Bureau of Criminal Investigation
CI	Critical Infrastructure
CIMS	Communication and Information Management System
CIO	Chief Information Officer
CIS	Center for Internet Security
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
COOP	Continuity of Operations Planning
CSA	Cybersecurity Strategic Advisor
C-SCRM	Cyber Supply Chain Risk Management
DHS	U.S. Department of Homeland Security
EI-ISAC	Elections Infrastructure Information Sharing and Analysis Center
EOP	Emergency Operations Plan
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
HSAC	State of Ohio Homeland Security Advisory Council
ILO	Intelligence Liaison Officer Program
IOC	Initial Operating Capacity
LG	Local Government

LE	Law Enforcement
MS-ISAC	Multi State Information Sharing and Analysis Center
NICE	National Initiative for Cybersecurity Education Workforce Framework
NIST CSF	National Institute of Standards and Technology, Cybersecurity Framework
OARnet	Ohio Academic Resources Network
OCCEC	Ohio Comprehensive Cyber Executive Committee
OCCPC	Ohio Comprehensive Cyber Planning Committee
OIT	Office of Information Technology, DAS
OP3	Ohio Public Private Partnership Program
POETE	Planning, Organization, Equipment, Training and Exercise elements
SAA	State Administering Agency
SIEC	Statewide Interoperability Executive Committee
SIEM	Security Information and Event Management
SCIP	Statewide Communications Interoperability Plan
SLCGP	State and Local Cybersecurity Grant Program
SPR	Stakeholder Preparedness Review
STACC	Statewide Terrorism Analysis and Crime Center
THIRA	Threat and Hazard Identification and Risk Assessment
TLP	Traffic Light Protocol
TTX	Tabletop Exercise

CyberOhio