

SLCGP
State and Local
Cybersecurity Grant Program

Washington State Plan
June 6, 2023



WaTech
Washington Technology Solutions



This Page Intentionally Left Blank



Promulgation and Signatories

This document is approved for implementation by the following authorities as of June 6, 2023:

William S Kehoe

William S Kehoe (Jun 7, 2023 18:06 PDT)

William Kehoe
State Chief Information Officer
Washington Technology Solutions

Robert Ezelle

Robert Ezelle (Jun 12, 2023 06:28 PDT)

Robert Ezelle
Director, Emergency Management Division
Washington Military Department



Contents

Promulgation and Signatories	2
Letter from Co-Chairs of the Washington SLCGP Planning Committee.	6
Introduction	7
Purpose	7
Project Scope	8
Strategic Objectives.....	8
Cybersecurity Program Goals, Objectives, and Potential Projects.....	9
Goal 1 - Improve the cybersecurity posture of all local governments.	9
Goal 2 - Increase cybersecurity and privacy capacity at the state and local level.....	10
Goal 3 - Develop enduring partnerships to support cyber resilience across the State of Washington.	10
Goal 4 - Effectively use existing funds and identify sustainable funding options.....	11
Cybersecurity Plan Elements.....	11
1. MANAGE, MONITOR, AND TRACK	11
2. MONITOR, AUDIT, AND TRACK	12
3. ENHANCE PREPAREDNESS.....	12
4. ASSESSMENT AND MITIGATION	13
5. BEST PRACTICES AND METHODOLOGIES	13
6. SAFE ONLINE SERVICES	14
7. CONTINUITY OF OPERATIONS.....	15
8. WORKFORCE	15
9. CONTINUITY OF COMMUNICATIONS AND DATA NETWORKS	16
10. ASSESS AND MITIGATE CYBERSECURITY RISKS AND THREATS TO CRITICAL INFRASTRUCTURE AND KEY RESOURCES.....	16
11. CYBER THREAT INDICATOR INFORMATION SHARING.....	17
12. LEVERAGE CISA SERVICES.....	19
13. INFORMATION TECHNOLOGY AND OPERATIONAL TECHNOLOGY MODERIZATION REVIEW	19
14. CYBERSECURITY RISK AND THREAT STRATEGIES	19
15. RURAL COMMUNITIES.....	20



16. DISTRIBUTION TO LOCAL GOVERNMENTS	20
Funding and Services	21
Funding Allocation.....	21
Distribution of Funds	21
Statewide Capability Overview	22
Mapping of SLCGP NOFO Required Plan Elements to the NIST Cybersecurity Framework	23
Implementation Plan.....	27
Organization Roles and Responsibilities	27
Notice of Intent (NOI)	30
Resource Overview and Timeline Summary.....	30
Applicant Requirements	31
Metrics.....	32
Appendix A: Cybersecurity Plan Capability Assessment.....	33
Appendix B: Project Summary Worksheet.....	42
Appendix C: Entity Metrics	46
Appendix D: Data Security Categorization and Critical Infrastructure.....	53
Protected Critical Infrastructure Information Program.....	53
Data Handling Practices	53
Washington State Information Classification Categories.....	53
Labeling Data for Secure Handling.....	53
Appendix E: Alignment with Equity and Inclusion Directives.....	55
Washington State Diversity, Equity and Inclusion Commitment.....	55
Washington State Pro-Equity and Anti-Racism (PEAR)	55
Federal Accessibility for Virtual Products	55
Appendix F: Acronyms.....	56
Appendix G: Glossary.....	59

List of Figures

Figure 1: Washington State Jurisdiction NCSR Functional Averages - 2021.....	22
--	----



List of Tables

Table 1: 2022 SLCGP Funding.....	21
Table 2: Grant Funds Distribution	21
Table 3: 2021 NCSR Response Averages by CSF Function.....	23
Table 4: SLCGP NOFO Element Mapping to NIST CSF Functions.	24
Table 5: SLCGP Planning Committee Members	27
Table 6: 2022 SLCGP Grant Cycle Timeline	30
Table 7: NCSR Maturity Levels Used to Define Capability Levels.....	33
Table 8: Cybersecurity Plan Capability Assessment.....	34
Table 9: Project Summary Worksheet	42
Table 10: Cybersecurity Plan Metrics.....	46
Table 11: List of Acronyms.....	56



Letter from Co-Chairs of the Washington SLCGP Planning Committee.

Greetings,

Washington Technology Solutions (WaTech), and the Washington Military Department's Emergency Management Division (EMD) have partnered to create and recruit members to represent various entities throughout Washington State to stand up the Cybersecurity Planning Committee. We are pleased to present the 2023 SLCGP Cybersecurity Plan, which represents the state's continuing commitment to improve cybersecurity, reinforce relationships across state agencies, and assist cybersecurity practitioners across our local jurisdictions and entities.

Representatives from many state agencies, local governments, and education and public health entities, collaborated to develop the Cybersecurity Plan with actionable and measurable goals and objectives that focus on strengthening our cybersecurity posture, creating sustainable and scalable solutions, increasing capacity, and leveraging other funding sources. The goals are designed to help our local jurisdictions plan for new technologies and navigate the rapidly changing cybersecurity landscape.

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

Sincerely,

William S Kehoe

[William S Kehoe \(Jun 7, 2023 18:06 PDT\)](#)

William Kehoe
State Chief Information Officer
Washington Technology Solutions

Robert Ezelle

[Robert Ezelle \(Jun 12, 2023 06:28 PDT\)](#)

Robert Ezelle
Director, Emergency Management Division
Washington Military Department



Introduction

Developing a state cybersecurity strategy is the first step in helping secure systems the public depends on. The purpose of this strategy is to create a clear vision for the State of Washington with goals and objectives that address gaps and lead to desired outcomes in cybersecurity. Each objective will be achieved through actionable items and deliverables that measure progress and maturity. This strategy is a living document which will be revisited and refined on a regular frequency based on the ever-evolving threat landscape, and emerging technologies and needs. This plan is meant to work with and build upon existing cybersecurity structures.

Cyber threats are an unpredictable, dangerous, and a proliferating hazard to state, local, and tribal governments (SLT), as well as private industry and operators of critical infrastructure systems. Every day, networks across the state face increasingly sophisticated cyberattacks. The State of Washington must be able to respond to the challenges of a significant cyber event. In a whole-of-state fashion, mitigation of cyber risks and improvements to response capabilities can be achieved through a coordinated, collaborative partnership between state agencies, local governments, and critical infrastructure partners. The Planning Committee is committed to continuing efforts already in process across all levels of government and state agencies, such as quarterly WaTech meetings with local government and monthly interagency cybersecurity coordinating committee meetings.

A whole-of-state approach supports rural and small local government entities and tribes by offering pre-approved tools, key threat intelligence and secure reporting, training, and generalized funding in the form of grants to help bolster cyber defenses across all levels of government. Washington's whole-of-state effort started as an organic, collaborative effort between local CIOs/CISOs, IT professionals, and state agency representatives to define cybersecurity-related challenges and create a plan of support for local governments across Washington – particularly for jurisdictions with the fewest available resources. This effort made progress in large part due to participation in a National Governor's Association policy academy that assisted in convening and focusing the work on recommendations.

Detailed operational plans support the SLCGP plan at the state agency, local government, tribal, and private sector levels.

Nothing in this plan restricts, supersedes, or otherwise replaces the legal authorities or regulatory responsibilities of any government agency or organization. All information will be handled, transmitted, distributed, released, and/or stored in accordance with applicable laws and policies.

WaTech is the primary technology provider of cybersecurity protection, detection and mitigation practices in defense of the state government network; EMD oversees initiatives that support local governments, tribal nations, and industry partners with critical infrastructure protection, including addressing cybersecurity planning and cyber incident response coordination. These two state agencies are working in collaboration to support the SLCGP.

Purpose

The SLCGP is intended to address gaps in readiness for local jurisdictions and entities. WaTech and EMD are committed to collaborating with sub-recipients (local jurisdictions receiving grants through the SLCGP) to improve the state's overall cybersecurity posture through stakeholder collaboration



and following best practices, standards and guidelines in cybersecurity governance, risk management, threat detection and resource allocation.

This strategy aims to establish a framework for preventing, responding to, and recovering from cyber incidents, as well as develop a clear vision for strengthening the State of Washington's cybersecurity posture through goals and objectives that address cybersecurity gaps at the local level. While this strategy is a multi-year plan, it is a living document that will be reevaluated regularly based on the ever-evolving threat landscape, emerging technologies, and current needs.

Project Scope

This strategy establishes a framework for a whole-of-state approach to cybersecurity. It is structured to provide clear guidance over the duration of the grant for identifying, managing risks and addressing cyber threats across the state. Partnerships with federal, state, local, tribal, and private sectors will be utilized and leveraged to accomplish the goals and objectives of the strategy.

Vision:

Implement a strong, secure, and resilient cybersecurity posture that facilitates and promotes best practices, reduces risks to critical services, and protects personal privacy and data at all levels of government within the State of Washington.

Mission:

Create a culture of information security excellence that empowers state and local jurisdictions throughout the State of Washington to deliver secure and reliable services to their citizens and stakeholders.

Strategic Objectives

The Cybersecurity Plan is a multi-year strategic planning document that applies a thorough priority-based approach to ensure SLCGP funding is used to improve cyber resilience and help protect critical infrastructure and information technology resources, secure critical data, and safeguard the privacy of Washington residents and those that interact with the state, municipalities, school districts, and other local government entities. The plan contains principles to:

- Manage, monitor, and track cyber incidents statewide.
- Enhance preparedness towards a secure cyberspace within local jurisdictions.
- Assess and mitigate infrastructure vulnerabilities to minimize exposure within local jurisdictions.
- Compile and share best practices and methodologies across jurisdictional boundaries.



Cybersecurity Program Goals, Objectives, and Potential Projects

Goal 1 - Improve the cybersecurity posture of all local governments.

Objectives

- Enhance risk assessment and risk management capabilities within local jurisdictions by improving Nationwide Cybersecurity Review (NCSR) responses to level 5 ("Implementation in Process," see Table 7 on page 33 for a description of NCSR maturity level descriptions) per the [NIST CSF](#). (SLCGP NOFO elements 12, 14¹).
- Enhance business continuity (BC) and information technology disaster recovery (IT DR) capabilities within local jurisdictions by improving NCSR responses to level 5 (Implementation in Process) per the [NIST CSF](#). (SLCGP NOFO elements 1, 5, 9)
- Enhance incident response and recovery capabilities within local jurisdictions by improving NCSR responses to level 5 (Implementation in Process) per the [NIST CSF](#). (SLCGP NOFO elements 2, 3)
- Identify best practices for sharing threat intelligence, indicators of compromise and indicators of attack between victims and partner organizations. (SLCGP NOFO element 11)
- Promote industry standards for information security. (SLCGP NOFO element 6)

Suggested Potential Projects

- Jurisdictions or entities may implement Multi-Factor Authentication (MFA). (SLCGP NOFO element 5)
- Facilitate implementation of the .gov domain for all government jurisdictions. (SLCGP NOFO elements 5 and 6)
- Analyze and address state and local government entity risk management gaps. (SLCGP NOFO elements 12, 14)
- Analyze and address state and local government entity incident response plan gaps. (SLCGP NOFO elements 2, 3)
- Analyze and address state and local government entity gaps in threat information sharing. (SLCGP NOFO element 11)

¹ Combining the two assessment data sets and mapping across the required SLCGP elements (and NIST framework) will allow sub recipients to see where their individual project funding request fit within the broader goals of the Washington State Plan and the overall national objectives of the SLCGP. See Table 4: SLCGP NOFO Element Mapping to NIST CSF Functions.



Goal 2 - Increase cybersecurity and privacy capacity at the state and local level.

Objectives

- Implement redundant and resilient data storage and transmission systems. (SLCGP NOFO element 7)
- Develop a competent professional IT workforce using standardized curriculum. (SLCGP NOFO element 8)
- Promote a cyber aware culture within state and local jurisdictions and entities through accessible awareness content. (SLCGP NOFO element 8)

Suggested Potential Projects

- Provide financially accessible awareness programs on cybersecurity, privacy and protection of sensitive information and infrastructure systems for SLT employees. (SLCGP NOFO element 8)
- Increase the number of individuals with professional training and certification in cybersecurity, privacy and infrastructure protection within local jurisdictions and entities. (SLCGP NOFO element 8)
- Support participants in higher education programs (bachelor and masters programs) across the state. (SLCGP NOFO element 8)
- Identify opportunities for IT professionals to demonstrate skills and gain experience in real-world and simulated incident response and recovery operations (tabletop and cyber range exercises). (SLCGP NOFO element 3)
- Identify gaps in secure storage and transmission capabilities within state and local entities (SLCGP NOFO element 7)

Goal 3 - Develop enduring partnerships to support cyber resilience across the State of Washington.

Objectives

- Identify coalitions of local jurisdictions to support implementation of identified SLCGP projects. (SLCGP NOFO element 13)
- Work with SLT stakeholders to ensure compatibility of state and local cyber incident response plans. (SLCGP NOFO element 3, 14)
- Invest in the future cybersecurity workforce by conducting outreach on cybersecurity career pathways for K-12, and college and university students. (SLCGP NOFO elements 8, 13)

Suggested Potential Projects

- Partner with the Association of County and City Information Services (ACCIS) professionals, the Washington Coalition for Infrastructure Protection and Homeland Resilience (WA-CIPHR), and other organizations throughout the state to identify opportunities to improve cybersecurity statewide. (SLCGP NOFO element 14)



- Assist with the development and review of local jurisdictional cybersecurity programs and plans. (SLCGP NOFO element 14)
- Partner with national organizations and federal partners (including the FBI, Cybersecurity and Infrastructure Security Agency [CISA], Secret Service, Multi-State Information Sharing and Analysis Center [MS-ISAC], and the National Initiative for Cybersecurity Education [NICE]) to harness best-practices and information sharing.
- Work with state higher education institutions, and non-governmental organizations to improve workforce development and resources. (SLCGP NOFO element 8)

Goal 4 - Effectively use existing funds and identify sustainable funding options.

Objectives

- Demonstrate progress towards cyber risk reduction at the end of each funding cycle. (SLCGP NOFO element 10)
- Amplify the reach of projects by prioritizing those that can be extrapolated and shared with other jurisdictions. (SLCGP NOFO element 10)
- Leverage state master contracts to support accessible pricing for cyber resilience products, platforms, and solutions to all jurisdictions throughout Washington State. (SLCGP NOFO element 4)
- Apply values of equity when prioritizing proposed projects from local jurisdictions or entities. (Appendix E: Alignment with Equity and Inclusion Directives).

Suggested Potential Projects

- Develop outreach products for elected officials and executive personnel to clearly communicate funding needs for cyber related projects. (SLCGP NOFO element 10)
- Equitably distribute funds to areas of highest need and prioritize underserved jurisdictions. (SLCGP NOFO element 10, 15)

Cybersecurity Plan Elements

1. MANAGE, MONITOR, AND TRACK

MANAGE, MONITOR, AND TRACK INFORMATION SYSTEMS, APPLICATIONS, AND USER ACCOUNTS OWNED OR OPERATED BY, OR ON BEHALF OF, THE STATE OR LOCAL GOVERNMENTS WITHIN THE STATE, AND THE INFORMATION TECHNOLOGY DEPLOYED ON THOSE INFORMATION SYSTEMS, INCLUDING LEGACY INFORMATION SYSTEMS AND INFORMATION TECHNOLOGY THAT ARE NO LONGER SUPPORTED BY THE MANUFACTURER OF THE SYSTEMS OR TECHNOLOGY.

At the state and local levels, entities are encouraged to establish procedures to track information assets including proper asset management systems and practices, and controls to effectively restrict



and monitor access to agency information systems and data to authorized users based on defined business and legal requirements. Mechanisms will be implemented that provide for the control, administration, and tracking of access and use of information assets, as well as the protection of such assets from unauthorized or unapproved activity and/or destruction.

2. MONITOR, AUDIT, AND TRACK

MONITOR, AUDIT, AND TRACK NETWORK TRAFFIC AND ACTIVITY TRANSITING OR TRAVELING TO OR FROM INFORMATION SYSTEMS, APPLICATIONS, AND USER ACCOUNTS OWNED OR OPERATED BY, OR ON BEHALF OF, THE STATE OR LOCAL GOVERNMENTS WITHIN THE STATE.

Asset owners, asset custodians, and information security and privacy officers at the State and Local levels are encouraged to:

- Ensure the information assets under their purview are assessed for security and privacy risks; enable event logging to ensure potential threats to the confidentiality, integrity, availability, and privacy of agency information and information systems are identified and managed.
- Review and retain event logs in compliance with all applicable local, state, and federal laws, regulations, executive orders, circulars, directives, internal agency, and State of Washington policies, audit and contractual requirements.

3. ENHANCE PREPAREDNESS

Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.

The Cybersecurity and Critical Infrastructure Protection (CCIP) Unit was created within the EMD of the Washington State Military Department to enhance preparedness around concurrent incidents between cyber entities and municipalities with critical infrastructure. This unit specializes in educating SLT partners about the escalation process and providing awareness on preparing for a cyber or critical infrastructure incident at the following levels:

- **Federal Courses:** Identify and coordinate courses through the National Domestic Preparedness Consortium, FEMA, CISA, and other accredited sources.
- **Industry Courses:** With industry partners, to identify and coordinate highly specialized training in cybersecurity and infrastructure protection through SANS, Dragos, GIAC, and others.
- **Customized training:** Designed to meet unique needs not addressed by standardized courses. For example, Incident Command System 100/200/700 for Information Technology and Infrastructure Service Providers.



WaTech's Office of Cybersecurity (OCS) also coordinates and updates preparedness communication and training across state government agencies. Incident response plans are in place, and are currently being updated for use state-wide, state government wide, and agency wide.

SLTs are encouraged to participate with CCIP, EMD and WaTech to learn about preparedness, response, and resiliency. This can be accomplished through partnering with CCIP, engaging appropriate training partners, and through tabletop and cyber-range exercises and simulations.

4. ASSESSMENT AND MITIGATION

Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.

All major systems, applications, and general support systems operated by or on behalf of state and local government entities are encouraged to establish risk management processes to identify, assess, and address security and privacy risks throughout the cradle-to-grave lifecycle of a system. Assessments ensure adequate security and privacy controls and manage risks to acceptable levels throughout their lifecycles. The following sources can be used: continuous monitoring, audits and authorizations, and other system development life cycle activities.

CISA offers a suite of free tools and Washington will ensure local government agencies and organizations are aware of such tools and encourage their use. Assessing cybersecurity maturity begins with a comprehensive understanding of the available assessment tools. For example, CISA's Cybersecurity Evaluation Tool (CSET) allows all SLT partners, regardless of resource capability, to identify vulnerabilities of people, processes, and technology. Refer to the following links for further information:

[https://www.cisa.gov/sites/default/files/FactSheets/NCCIC ICS FactSheet CSET S508C.pdf](https://www.cisa.gov/sites/default/files/FactSheets/NCCIC%20ICS%20FactSheet%20CSET%20S508C.pdf)

<https://www.cisa.gov/downloading-and-installing-cset>.

Prior to receiving any reimbursements from grant funds, sub-recipients will be required to participate in CISA's Cyber Hygiene (CyHy) Vulnerability Scanning program which provides a report of identified vulnerabilities. At the time of this writing, 31 of Washington state's 39 counties have already subscribed to this service.

5. BEST PRACTICES AND METHODOLOGIES

Ensure that the state or local governments within the state adopt and use best practices and methodologies to enhance cybersecurity.

The following cybersecurity best practices (addressed in required element 5) will be considered in Washington's funded projects:

- Current use of multi-factor authentication.



- State of enhanced system and security logging and retention.
- Current implementation and use of encryption for data at rest and in transit.
- Planned end of use of unsupported/end of life software and hardware accessible from the internet.
- Plans to address exposed and required change of default system passwords and credentials.
- State of entity's ability to reconstitute systems (restore from backup).
- Plan or intent to migrate to the .gov domain.

Additional best practices that the sub-recipient's project plan can address include:

- Use of the National Institute of Standards and Technology (NIST) Cybersecurity Framework.
- NIST's cybersecurity supply chain risk management best practices.
- Current use of threat intelligence resources (tools, services, or platforms).

In order to provide a uniform baseline across state entities subject to these levels of compliance, all state-owned, leased, licensed, or managed information systems, system components, and system services subject to the above should implement moderate level controls as outlined in the [CIS Critical Security Controls, version 8.0](#). SLT organizations are encouraged to follow OCIO 141.10 policies.

6. SAFE ONLINE SERVICES

Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.

Under this program, all state agencies, counties, and cities using domains other than .GOV will be encouraged to migrate to the .GOV domain. Doing so will signal trust and credibility of the governmental entity.

Additional security benefits would include:

- Use of a two-step verification method for all users and enhance password security.
- Preloaded HTTPS protocols that alter web browsers to use HTTPS over any other website on that domain.
- The namespace is continually monitored by CISA, GSA and NIST for cybersecurity issues.

Entities not eligible for, or not wishing to migrate to the .GOV domain, will be encouraged to force the use of HTTPS encryption on all websites, thus ensuring encryption of communication in transit and authenticity of the website through digital certificate ownership.



7. CONTINUITY OF OPERATIONS

Ensure continuity of operations of the state or local governments within the state, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident.

Contingency planning is an important aspect of risk management. Ensuring availability for critical and essential systems and components allows agencies to meet mandates dictated by statute, executive order, policy, or contract, and ensure delivery of vital government services.

EMD's mission is to minimize the impact of disasters and emergencies on the people, property, environment, and economy of Washington. To accomplish this mission, the EMD must ensure its operations are performed efficiently with minimal disruption, especially during an emergency. EMD provides planning and program guidance for implementing the EMD's Continuity Plan and programs to ensure the organization can conduct its mission essential functions under all threats and conditions, including cybersecurity incidents.

State and local government entities will be encouraged to apply for projects to develop, implement, test, and maintain contingency plans to ensure continuity of operations for all information systems that deliver or support essential or critical functions.

8. WORKFORCE

Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the cybersecurity workforces of the state or local governments within the state enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of personnel of the state or local governments within the state, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training.

Washington State has begun initial work and discussions to use the National Initiative for Cybersecurity Education (NICE) Workforce Framework to identify and mitigate gaps in the state cybersecurity workforce. The state continues to collaborate across public and private sectors to develop solutions to a widespread challenge facing both public and private sectors.

A major challenge with maintaining a stable cybersecurity workforce is twofold; the first is recruiting qualified personnel. The State of Washington employs various programs to develop future cybersecurity experts. For example:

- The Public Infrastructure Security Cyber Education System (PISCES) is a program developed and adopted in Washington and subsequently launched in Alabama, Colorado, and Kentucky. Through its training program, PISCES equips students from middle school to higher education institutions to become entry-level cyber analysts and gives them a head start when entering the work force.



- The Air Force Association's CyberPatriot program is a national program that has expanded internationally. Over 100 teams from 49 schools and organizations in Washington State participate in the program and competed in the 2022-2023 CyberPatriot XV exercise. Spokane Public Schools is rated as one of the eighteen Centers of Excellence,

A second workforce challenge is keeping up with rapidly evolving cybersecurity technology, and the skills and experience required to maintain a strong cybersecurity posture. Washington State capitalizes on the presence of the large technology companies to employ various programs to grow its cyber workforce, in a future focused way:

- Career Connect Washington (CCW) is an example of an initiative that continues the cyber development pipeline from education into the workforce. CCW selected the non-profit sector leader, Computing for All, to take the strategic lead for Information Technology and Cybersecurity in collaborating with potential employers to create equitable opportunities for students.

Washington State is also committed to tapping into unmet potential within the workforce by cultivating a more diverse cybersecurity workforce. Apprenti is a coding apprenticeship program sponsored by the Washington Technology Industry Association (WTIA) that creates alternative pathways to access diverse tech talent. Ada Developers is another program committed to diversifying the tech industry and has expanded to the State of Georgia.

9. CONTINUITY OF COMMUNICATIONS AND DATA NETWORKS

Ensures continuity of communication and data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident involving those communications or data networks.

The State Interoperability Executive Committee (SIEC) works to ensure that all emergency responders, across all levels of government and across all jurisdictions can communicate with each other and share data. The committee recently updated its State Communications Interoperability Plan with the help of CISA. The updated plan is focused on assessing and improving emergency communications interoperability in the state. Many local jurisdictions throughout the state participate in the SIEC. Also, several members of the SLCGP Planning Committee also participate in the SIEC.

10. ASSESS AND MITIGATE CYBERSECURITY RISKS AND THREATS TO CRITICAL INFRASTRUCTURE AND KEY RESOURCES

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 state.

EMD annually conducts a federally mandated Stakeholder Preparedness Review (SPR) and a Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR) every three years with all 39 counties. EMD utilizes the Comprehensive Preparedness Guide (CPG) 201, Third Edition, which provides guidance for conducting a THIRA and SPR. The THIRA/SPR



assesses Washington's capabilities across five mission areas (Prevention, Protection, Mitigation, Response, Recovery) in 32 core capabilities, one of which is Cybersecurity. This assessment process is used to identify cybersecurity risks and threats relating to critical infrastructure and key resources (such as power grids and telecommunications) that may impact the performance of systems statewide. Understanding the risks supports setting the level of capability needed for response, identifying gaps, and aligning federal and state funding to mitigate those gaps.

Response Coordination: Governance for cross-organizational cyber incident response is shared. Domestic cyber incident response still largely depends on voluntary coordination and cooperation between the public and private sectors.

State Emergency Operations Center (SEOC) Units:

Intelligence Section: Performs critical analysis and data brokerage during cyberattacks and critical infrastructure incidents.

Intake and Analysis Unit: Sorts and labels incoming data for secure handling and shares it with other entities for further analysis and distribution, if needed and appropriate.

Infrastructure Impacts Unit: Future casts cascading issues resulting from the initial incident. This unit coordinates closely with the Situation Unit and Advanced Planning Unit.

Investigations Unit: Routes necessary information to law enforcement and other forensics entities.

Threat Monitoring Unit: Assesses a broad range of open-source and sensitive intelligence products to identify connections to human-caused harm to infrastructure and socio-political systems.

Escalation Process for Cyber Incidents: Following a significant cyber incident, the SEOC Supervisor or EMD Response Section Manager and the State Coordinating Officer (SCO) will activate the state emergency operations center utilizing the standard incident command system (ICS) structure to respond to the incident. Specific considerations for the coordination between the private sector, contractors, and other entities responding to the cyber incident will be made by the SEOC Supervisor and the Cybersecurity and Critical Infrastructure Protection Program Manager.

11. CYBER THREAT INDICATOR INFORMATION SHARING

Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.

Effective response requires close coordination across traditional boundaries and requires the development of a robust Common Operating Picture (COP) during significant cyber incidents as a foundational element.

Information sharing is a foundation for cyber incident response activities. Sub-recipients will be expected to develop and share tips, indicators, warnings, information, and mitigation recommendations using established communication channels.

While Washington state does not currently have a centralized security operations center that supports the whole-of-state vision, access to resources and initial discussions are underway to build out that



support for partners within the state. The state also encourages jurisdictions and entities to join both formal information sharing networks such as MS-ISAC, state organizations like ACCIS, and informal networks of professionals.

The Washington State Fusion Center collaborates across federal, state, local and tribal agencies to detect, deter and prevent cybercrime. WaTech's state OCS also works in collaboration with various federal state, local and tribal governments to assist with a similar mission focused on state government agencies. Sub-recipients of the SLCGP will also share information through their respective MS-ISAC indicator sharing efforts.

Additional organizations that currently assist with information sharing on cybersecurity issues include:

The Washington Coalition for Infrastructure Protection and Homeland Resilience (WA-CIPHR): WA-CIPHR is a cross-disciplinary initiative with representation from all 16 critical infrastructure sectors, all levels of government, and tribal nations. WA-CIPHR provides coaching to localities on their cyber posture and vets cyber plans towards their organizations' maturity standards. WA-CIPHR also provides specialized training courses to support stakeholders with planning, threat identification, vulnerability analysis, and infrastructure protection.

Washington Technology Solutions (WaTech): For incidents impacting the state government network (SGN), WaTech's OCS is the central point of contact for state government agencies to report suspicious activity and security incidents. OCS also provides guidance and assistance to local entities on incident response and recovery activities.

Department of Commerce (WA Energy Office): The mission of the Energy Resilience and Emergency Management Office within the Department of Commerce is to provide comprehensive and sustainable emergency management, resilience development, cybersecurity services for the energy sector. Commerce coordinates with stakeholders at all levels of government and with electric, natural gas utilities, the petroleum industry, and renewable sectors statewide to develop planning documents and standards, trainings, and operational support during emergencies.

Washington State Auditor's Office (SAO): The SAO provides citizens with independent and transparent examinations of how state and local governments use public funds and develops strategies to make government more efficient and effective. The SAO conducts IT assessments, provides cybersecurity guidance, and supports the State Interagency Cybersecurity Coordinating Committee.

Washington Secretary of State (WA SOS): The Office of the Secretary of State promotes public trust by safeguarding vital government records, documents, publications and process, preserving the integrity of elections in Washington State, providing the business community and public with easy access to information about corporations and charities, performing public outreach to improve civic knowledge and participation, and leveraging technology to improve efficiency and enhance customer service. The WA SOS assists local elections officials with securing elections infrastructure from cyber-attack.

Washington State Fusion Center (WSFC): The WSFC is Washington State's single fusion center and supports federal, state, and tribal agencies, regional and local law enforcement, public safety and homeland security by providing timely, relevant and high-quality information and intelligence services.



Washington Attorney General Office (WA AGO): The WA AGO tracks breaches within the state and issues an annual report. The AGO also assists with legal guidance for cybersecurity incidents.

12. LEVERAGE CISA SERVICES

Leverage cybersecurity services offered by the Department.

Washington State is committed to increasing awareness of CISA's services and free tools they provide and will use the WaTech website, newsletters, and network of cybersecurity professionals to do so.

Prior to receiving any grant fund reimbursements entities will be required to participate in CISA's CyHy vulnerability scanning program and Cyber Infrastructure Survey.

In addition to support and services from CISA, the MS-ISAC provides numerous free and low-cost services, such as incident response and forensics analysis, as well as platforms to SLT members. Currently, there are 364 MS-ISAC member entities within the State of Washington, representing all 39 counties and their election agencies, along with 81 cities and 95 educational institutions.

13. INFORMATION TECHNOLOGY AND OPERATIONAL TECHNOLOGY MODERNIZATION REVIEW

Implement a modernization review process that ensures alignment between information technology and operational technology cybersecurity objectives.

Washington State has a legacy replacement strategic plan, and the Legislature established an innovation and legacy modernization fund to support modernization efforts through addressing cybersecurity needs of legacy systems.

In keeping with modernization efforts, WaTech's OCS advocates a practice of holistic information security, which is a comprehensive approach to safeguarding data, systems, and people from cyber threats. Holistic information security considers not only technical solutions, but also human, organizational, and environmental factors that influence security. It aligns security goals and strategies with the organization's business objectives and culture and promotes security-conscious practices among all stakeholders.

Holistic information security requires continuous evaluation and improvement of the security posture, and proactive incident response and recovery. Following this approach, combines information technology and operations functions rather than seeing them as distinct functions. Opportunities will be made to train local entities in this approach and its methodologies.

14. CYBERSECURITY RISK AND THREAT STRATEGIES

Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats. Local governments and associations of local governments within the state should be



consulted. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.

Over the funded years of this grant, the Washington SLCGP Planning Committee will operate under their approved charter and develop, prioritize, and coordinate strategies and projects to address cybersecurity risks and threats with other organizations, including consultation with local governments and associations of local governments. The Planning Committee includes representatives from the Association of Washington Cities and the Washington State Association of Counties to continuously solicit and receive input and feedback from their respective members. The SLCGP has been an opportunity to continue to build the relationship between the state, local, tribal, and private sector which face similar challenges.

15. RURAL COMMUNITIES

Ensure adequate access to, and participation in, the services and programs described in this subparagraph by rural areas within the state.

The NOFO references 49 U.S.C. § 5302 which provides the following definition of a rural area as:

"... an area encompassing a population of less than 50,000 people that has not been designated in the most recent decennial census as an "urbanized area" by the Secretary of Commerce."

Due to the requirement to direct 25% of funds towards rural communities, the Planning Committee members are tasked with querying rural representatives about resources and suggestions on how to assist small, rural, or under-resourced communities to ensure their participation in the SLCGP.

Rural communities are assured access to funding under the SLCGP through outreach activities supported by the Planning Committee.

16. DISTRIBUTION TO LOCAL GOVERNMENTS

Distribute funds, items, services, capabilities, or activities to local governments.

The SLCGP and Infrastructure Investment and Jobs Act (IIJA), as approved by Congress, set the standards for equitable distribution of funding and services to local governments. EMD will oversee the grant administration of the SLCGP. The Planning Committee will select the projects based on agreed upon selection criteria in alignment with the NOFO.

The State of Washington will allocate at least 80% of the funds it receives from SLCGP to provide services and capabilities to local government entities as part of its strategy to enhance cybersecurity and resilience across the state. The remaining 20% of the funds may be used for state-level initiatives and administration costs.



Funding and Services

Funding Allocation

Washington State has been awarded \$4,073,923 for FY 2022 as displayed in the following table:

Table 1: 2022 SLCGP Funding

Anticipated Funding Release	Federal Allocation	Washington State Match	Total Award
Sept. 2023	\$ 3,666,530	\$ 407,393	\$ 4,073,923

Distribution of Funds

SLCGP grant funds will be distributed as follows.

Table 2: Grant Funds Distribution

Allocation	Percentage	Available Funds
FY22 Award		\$ 4,073,923
State Retention ²	20%	\$ 814,784
Subtotal		\$ 3,259,139
Earmarked for Rural Communities	25%	\$ 1,018,481
General passthrough ³ (remainder to all jurisdictions)		\$ 2,240,658

Funding is passed through by the Washington Military Department as the State Administrative Agency. Award funding is expected annually in the Federal Fiscal Years 2022-2025. The total amount anticipated to be awarded to the state during the grant cycle is approximately \$14,000,000. Based on the FY22 NOFO, it is expected each grant period of performance will be four years.

² The grant permits the state to retain 20% of the allocation for grant management and administration (M&A) and state level projects. Washington State may choose to not retain funding beyond the 5% allowable M&A based on overall needs of the SLTs. Additionally, the state may retain over the 20% for passthrough of items, services, capabilities, or activities in lieu of funding but must have the consent of the benefiting local jurisdictions.

³ While the NOFO requires that 25% of the award be passed through to rural communities based on proposals submitted by SLTs more than the required 25% may actually be allocated to rural communities.



SLT jurisdictions will apply to fund projects under the SLCGP grant. SLTs may submit multiple projects that strengthen their cybersecurity practices and programs. Projects will then be ranked by an oversight committee and selected projects will be funded by the SLCGP grant. For examples see Appendix B: Project Summary Worksheet.

Statewide Capability Overview

Washington State utilized the following information to compile the analysis for the table in Appendix A: Cybersecurity Plan Capability Assessment.

Two sources of data were used in this assessment of the cybersecurity needs within local jurisdictions. The combined assessment of the NCSR data for 2021 and a series of IT findings from audits conducted by the SAO. These two data sets informed our discussion of expected local cybersecurity needs and gaps. With over 2,500 local jurisdictions and entities across Washington state, these data sets are not comprehensive, yet illuminate specific needs and risk profiles. This information assisted in setting goals, objectives and leading discussion within the Planning Committee.

In 2021, 52 Washington state jurisdictions, the majority of which were counties, participated in the NCSR. The NCSR is a cybersecurity self-assessment that measures maturity in five functional areas: Identify, Protect, Detect, Respond and Recover, and is based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF).

The NCSR ranks agency responses on a seven-point maturity scale. (See Table 7 for the NCSR Maturity Levels and their definitions.) Jurisdictions scoring between 3 and 5 are either in the process of developing their policies/standards or implementing the controls required by those documents.

Figure 1 below displays the functional average of the 52 Washington State jurisdictions that reported in 2021.

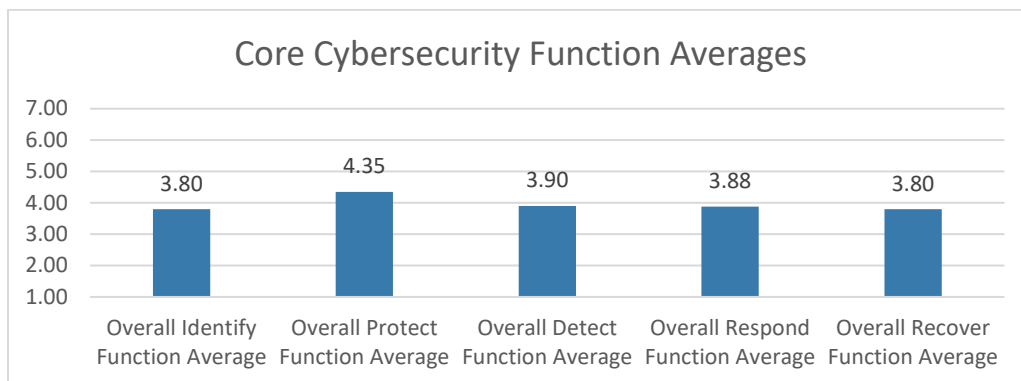


Figure 1: Washington State Jurisdiction NCSR Functional Averages - 2021



The following shows a breakdown of these overall averages by responding entity category:

Table 3: 2021 NCSR Response Averages by CSF Function

Entity Category ⁴	Number of Responses ⁵	NIST CSF Function (average by entity category)				
		Identify	Protect	Detect	Respond	Recover
Washington State (67 agencies aggregated to one report)	1 ⁶	4.6	4.8	4.6	4.7	4.6
Counties	21	3.5	4.4	3.8	3.7	3.6
Cities	11	4.0	4.5	4.0	4.0	4.0
K-12	5	4.3	4.2	3.6	3.7	4.0
Fire Districts/EMS	7	2.7	4.0	3.5	3.4	2.9

These results indicate that assistance is needed in all functional areas of the NIST CSF in jurisdictions across the State. The Planning Committee expects proposals from all entity categories in all functional areas. However, certain foundational activities should be considered a priority. For example, the functional area of Identify - which includes asset management, development of policies, risk management strategies and assessments, information security and incident response plans - shows some of the lowest averages and should be considered a priority.

Mapping of SLCGP NOFO Required Plan Elements to the NIST Cybersecurity Framework

To identify gaps in information security environments across the state, WaTech’s OCS used the NCSR as a baseline. The required elements of the SLCGP NOFO were mapped to the NIST CSF framework (see Table 4). For SLCGP NOFO elements not easily or directly mappable to the NIST CSF (specifically elements 6 and 13), a capability analysis was performed using SAO cybersecurity IT audit findings.

SAO cybersecurity audits which examine information technology systems used in government operations were also used to augment the NCSR analysis. They look for weaknesses in that technology and propose solutions to help strengthen those systems.

⁴ No Tribal Nations within the state of Washington submitted the NCSR in 2021.

⁵ The number of responses in Table 3 totals 45 responses. As discussed, 52 jurisdictions reported the NCSR in 2021. The difference is accounted for in that the other 8 NCSR submissions are sub-agencies of a parent agency.

⁶ 67 state agencies provide responses to the 2021 NCSR. These have been aggregated to a single State-wide response.



Combining the two assessment data sets, and mapping across the required SLCGP elements (and NIST framework) will allow sub-recipients to see where their individual project funding requests fit within the broader goals of the Washington State plan and overall national objectives of the SLCGP.

Table 4: SLCGP NOFO Element Mapping to NIST CSF Functions.

SLCGP NOFO Required Elements	NIST CSF Function				
	Identify	Protect	Detect	Respond	Recover
1. Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.	X		X		
2. Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.	X	X	X		
3. Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.		X		X	
4. Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.	X	X	X		
5. Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity, discussed further below.		X	X		X





SLCGP NOFO Required Elements	NIST CSF Function				
	Identify	Protect	Detect	Respond	Recover
6. Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.					
7. Ensure continuity of operations of the state or local governments within the state, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident.				X	
8. Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the cybersecurity workforces of the state or local governments within the state, enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of personnel of the state or local governments within the state, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training.		X			
9. Ensures continuity of communication and data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident involving those communications or data networks.				X	
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 state.	X	X	X	X	
11. Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.		X		X	
12. Leverage cybersecurity services offered by the Department.	X		X		



SLCGP NOFO Required Elements	NIST CSF Function				
	Identify	Protect	Detect	Respond	Recover
13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives.					
14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats. Local governments and associations of local governments within the state should be consulted. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.	X	X	X	X	X
15. Ensure adequate access to, and participation in, the services and programs described in this subparagraph by rural areas within the state.					
16. Distribute funds, items, services, capabilities, or activities to local governments.					

KEY

-  Partially Documented Standards and/or Procedures
-  Documented Policy

Note: Grayed-out rows indicate no direct mapping to NIST CSF functions.



Implementation Plan

Organization Roles and Responsibilities

This section provides insight into the strategic partnerships that support the planning process, identification of potential projects, and allocation of funding. These partnerships will provide ongoing resources and guidance throughout the course of the SLCGP grant process over the next four years.

Strategic Partnerships

This section provides insight into the strategic partnerships that support the planning process, identification of potential projects, and allocation of funding.

SLCGP Planning Committee Composition

The SLCGP Planning Committee was built around existing collaborations - the Technology Services Board Cybersecurity subcommittee; the State Interoperability Executive Committee; the Interagency Cybersecurity Coordinating Committee; and the Washington State Fusion Center. Each member of the Planning Committee was invited to participate based on the following criteria:

- Personal responsibility within their organization (i.e., assigned specifically to a cybersecurity role within their organization) or their organizational responsibility for cybersecurity.
- Personal or organizational Statewide focus.
- Awareness of local governments concerns and ongoing relationships with local governments.

The membership of the Planning Committee recognized the complexity and diversity of the many jurisdictions or entities that may apply and committed themselves to think broadly and with a focus on the smallest or least-resourced jurisdictions.

Below is a table showing all Planning Committee members and supporting staff.

Table 5: SLCGP Planning Committee Members

Name	Title	Organization	SLCGP Role
Robert Ezelle	Director of Emergency Management	Washington Emergency Management Division	Co-Chair
Bill Kehoe	Chief Information Officer	WaTech	Co-Chair
Craig Adams	Chief Information Officer	Washington State Association of Counties + Kitsap County	Member
Samuel Anderson	Chief Information Security Officer	Office of the Secretary of State	Member



State and Local Cybersecurity Grant Program
Washington State Cybersecurity Plan
Published: June 2023

Name	Title	Organization	SLCGP Role
John Batiste	Chief of the Washington State Patrol	Washington State Patrol	Member
Nick Benfield	Sr Security Specialist	Office of the State Auditor	Member
Eli King	Director of Energy Emergency Management	Department of Commerce	Member
Grant Rodeheaver	Deputy Executive Director–Information Technology	Washington State Board for Community and Technical Colleges	Member
Ralph Johnson	State Chief Information Security Officer	WaTech	Member
Katy Ruckle	Chief Privacy Officer	WaTech	Member
Sheri Sawyer	Senior Policy Advisor	Governor’s Office	Member
Jie Tang	Budget Advisor	Office of Financial Management	Member
Bre Urness-Straight	Director of Educational Technology	Office of Superintendent of Public School Instruction	Member
John Weeks	Chief Information Security Officer	Washington Department of Health	Member
Dan Wordell	Chief Information Officer	Association of WA Cities + City of Spokane	Member
Tanya Kumar	Senior Compliance Manager, National Security Cloud Compliance	Oracle	Member
Zack Hudgins	Privacy Manager	WaTech Office of Privacy and Data Protection	Meeting Facilitator



Name	Title	Organization	SLCGP Role
Stevens Fox	Deputy CISO - Policy and Program Management	WaTech Office of Cybersecurity	Subject Matter Expert
Ariah Olsen	Infrastructure and Industry Manager	Washington Emergency Management Division	Support
Adam Wasserman	E911 and OneNet Unit Manager	Washington Emergency Management Division	Support
Josh Castillo	Cyber Resilience Specialist	Washington Emergency Management Division	Lead Local Coordinator
Sierra Wardell	Financial Operations Section Manager	Washington Emergency Management Division	Lead Grant Manager
Jackie Chang	Grants Program Manager	Washington Emergency Management Division	Support Grant Manager
Allen Avery	Lead Cyber Intelligence Analyst	Washington State Fusion Center	Subject Matter Expert
Ian Moore	Cybersecurity Advisor	Cybersecurity and Infrastructure Security Agency - Region 10	Subject Matter Expert (non-voting)

Affiliation with Association of County and City Information Systems

The Association of County and City Information Systems (ACCIS) is an organization of the Chief Information Systems Office of Counties and Cities within Washington that promotes a communication link between the information systems functions of member agencies, represents county and city information systems’ interests to state officials, calls attention to legislation affecting data processing operations and technology, and provides education to county and city officers on roles and responsibilities of information systems departments.

Affiliation with Association of Washington Cities

The Association of Washington Cities (AWC) is a private, nonprofit, nonpartisan corporation that represents Washington’s cities and towns before the state legislature, the state executive branch and with regulatory agencies. A wide array of programs and services are offered to its members.

Affiliation with Washington State Association of Counties

The Washington State Association of Counties (WSAC) serves the counties of Washington State and includes elected county commissioners, councilmembers, and executives from all of Washington’s 39



counties. The organization provides a variety of services to its member counties, including advocacy, professional development, public-private business partnerships, and a forum to network and share best practices.

Affiliation with the Washington Coalition for Infrastructure Protection and Homeland Resilience

The Washington Coalition for Infrastructure Protection and Homeland Resilience (CIPHR) is a cross-disciplinary initiative with representation from all 16 critical infrastructure sectors, all levels of government, and Tribal nations. WA-CIPHR will review and provide feedback on proposed planning and application processes for all external-facing cybersecurity plans for Washington State, including SLCGP and the Significant Cyber Incident Annex.

Tribal Government Partnerships

While Tribal governments are eligible to apply and receive grants under SLCGP, the Federal government has also created a Tribal Cybersecurity Grant Program (TCGP), which allows Tribal governments to apply for grant funding specific to their needs.

No matter which Federal program Tribal governments choose to pursue, the state is committed to the continued pursuit of mutual cybersecurity goals through the established relationships between sovereign governments. Examples of this work include WaTech's provision of technology access to the Intergovernmental Network (IGN) for tribes requesting support for services maintained by state government agencies, such as law enforcement systems. EMD also provides comprehensive emergency management planning, exercise, education, and training for tribal, state, and local jurisdictions. EMD facilitates other grant programs where Tribes have the option of working directly with FEMA as a recipient or working through EMD.

WaTech, EMD, and staffing support for the Planning Committee welcome all state, local, and tribal participation in the SLCGP to strengthen relationships, build confidence in cybersecurity postures, and improve the services delivered by government. Successfully addressing cybersecurity issues of mutual concern, through either the TCGP or the SLCGP with clear, direct communication, and robust collaboration is beneficial to all residents within Washington.

Notice of Intent (NOI)

The Planning Committee has chosen to distribute a NOI to SLTs. The NOI is intended to inform and refine the planning process to identify statewide projects, assist in determining collaboration efforts and provide advance notice of intent to apply for grant funding. The Planning Committee distributed an NOI in May 2023 to inform the application process for the first year and may distribute an NOI for each subsequent funding year.

Resource Overview and Timeline Summary

WaTech and EMD will provide the necessary resources to oversee grant administration and performance oversight.

The anticipated timeline for the 2022 funding cycle is as follows:

Table 6: 2022 SLCGP Grant Cycle Timeline



Activity	Date
NOI distributed to SLTs.	May 2023
Grant applications available.	June 2023
Submission of the SLCGP Cybersecurity Plan.	July 1, 2023
Grant application submissions due.	July 2023
Applications evaluated and grant sub-recipients notified.	July 2023
Submission of projects and revised Investment Justifications to FEMA.	August 2023
CISA approval of Washington State Cybersecurity Plan.	August 2023
FEMA releases funds.	September 2023
Grant agreements executed/projects funded - 45 days after release of funds.	September/ October 2023

Applicant Requirements

To receive grant funding from the State of Washington through the SLCGP program, each sub-recipient must meet the following requirements⁷:

- **Rural communities** must meet the 49 U.S.C. § 5302 definition of a rural area stated in the NOFO.
- Must be a member of the MS-ISAC, MS-ISAC membership is free.
- Complete CISA's Cyber Infrastructure Survey (CIS) (see information on the CISA Cyber Resource Hub page) The CIS is a free service provided by CISA that evaluates the effectiveness of organizational security controls, cybersecurity preparedness, and the overall resilience of an organization's cybersecurity ecosystem. This can be done through a self-assessment or with CISA's assistance. The CIS will provide a baseline that will later be used to show improvement in the information security maturity of the organization based on the proposed project. Results of the CIS must be submitted to WaTech's OCS.
- Unless already receiving the service, sign up for CISA's CyHy Vulnerability scanning program (a free service provided by CISA).
- All FY22 SLCGP sub-recipients must complete the NCSR by 12/1/2023. Failure to complete the NCSR will result in future funds being withheld. Completion of the NCSR on an annual basis is required to receive SLCGP funds in subsequent years. NCSR responses must be forwarded to WaTech's OCS for comparison to show improvement in cybersecurity posture and provide an aggregated picture of the state's posture as a whole.
 - NCSR is open October 1-February 28 annually.
 - If the applicant SLT submitted an NCSR for 2022 the detailed report should be forwarded to OCS to assist in establishing a baseline cybersecurity posture.

⁷ These requirements can be met at any time during the application process but must be achieved before any grant funds are distributed.



- Prior to submitting a grant application SLTs are encouraged to investigate free services provided by CISA and MS-ISAC. If CISA or MS-ISAC provides a free service that will meet the needs of the SLT noted in the proposed application, an application to purchase these same service should not be submitted.

For assistance with any of these requirements, contact WaTech OCS.

Metrics

Success for each recipient and sub-recipient of grant funding will be measured by comparing the "before," "during," and "after" states of their cybersecurity posture against the goals and objectives of the grant and their specific project scope during the period of performance. Grant sub-recipients will be required to report progress on their project. The specifics will be based on their project and will be included in the individual grant agreement timeline. Project progress will be shared with the Planning Committee and consolidated into the annual required Performance Progress Reports (PPR) submitted by the State Administrative Agency (SAA). Details may include project status, summary of expenditures, and any potential issues affecting project completion. Please see Appendix C: Entity Metrics on page 46 for details on reporting program metrics.

All subgrantees must meet certain requirements to qualify to receive funds. (See Applicant Requirements in the previous section).

As grants are approved for funding, OCS will develop a series of metrics specifically targeted to monitor progress for the sub-recipient's specific project. Report templates will be provided to allow roll up in a standard way for reporting to the Planning Committee and CISA.

Projects will be measured against traditional project controls (scope, schedule, and budget).



Appendix A: Cybersecurity Plan Capability Assessment

Reviewing the SLCGP Required Elements against capability data collected through NCSR responses and SAO audit findings reveals great diversity across local jurisdictions within the State of Washington. Larger entities are, as expected, more mature than smaller entities. Larger entities have more resources (e.g., funding, people, etc.) not to mention larger data sets to protect. Smaller entities are less well-resourced and funded, providing easier targets for threat actors, but potentially less lucrative as smaller jurisdictions have smaller data sets. In determining the “Capability Level” in Table 8 the planning committee chose to use the NCSR Maturity Scale. The NCSR utilizes a seven (7) step maturity rating. The seven steps are shown in Table 7 below.

Table 7: NCSR Maturity Levels Used to Define Capability Levels

Maturity Level (Capability Level)	Definition
1. Not Performed	Activities, processes, and technologies are not in place to achieve referenced objectives.
2. Informally Done	Activities and processes may be substantially performed, and technologies may be available to achieve the objective. They are undocumented and/or not formally approved by senior management.
3. Documented Policy	The organization has a formal policy in place that has been approved by senior management.
4. Partially Documented Standards and/or Procedures	The organization has a formal policy in place and has begun the process of developing documented standards and/or procedures to support the policy.
5. Implementation in Progress	The organization has an activity in process defined within documented policies, standards and/or procedures. The organization is in the process of implementing and aligning the documentation to a formal security framework and methodology.



Maturity Level (Capability Level)	Definition
6. Tested and Verified	The organization is executing the activity or process and has formally documented policies, standards and procedures. Implementation is tested and verified.
7. Optimized	The organization is executing the activity or process and has formally documented policies, standards and procedures. Implementation is tested, verified, and reviewed regularly to ensure continued effectiveness.

A review of the available NCSR responses for 2021 and SAO audit findings shows that the majority of the state is at the Documented Policy level for most required elements. This is an aggregated state-level assessment and not representative of any individual jurisdiction.

Table 8: Cybersecurity Plan Capability Assessment

Completed by WaTech’s Office of Cybersecurity (OCS)			
Cybersecurity Plan Required Elements	Description of Current Capabilities	Capability Level <small>(See Table 7 for capability level designations)</small>	Project # #(s)
1. Manage, monitor, and track information systems, applications, and user accounts.	Incomplete implementation of management, monitoring, and system tracking - the State and Local Government (SLG) entities have partially documented policies and standards. Identity and access management controls are in the implementation phase within counties and cities.	3. Documented Policy	1, 2, 3



Completed by WaTech’s Office of Cybersecurity (OCS)			
Cybersecurity Plan Required Elements	Description of Current Capabilities	Capability Level <small>(See Table 7 for capability level designations)</small>	Project # #(s)
2. Monitor, audit, and track network traffic and activity.	Incomplete implementation - the SLG entities have partially documented policies and standards.	4. Partially Documented Standards and Procedures	1, 2
3. Enhance the preparation, response, and resiliency of information systems, applications, and user accounts.	Incomplete implementation - the SLG entities have partially documented policies and standards.	4. Partially Documented Standards and Procedures	1, 2
4. Implement a process of continuous cybersecurity risk factors and threat mitigation practices prioritized by degree of risk.	Incomplete implementation - the SLG entities have partially documented policies and standards.	4. Partially Documented Standards and Procedures	1, 2
5. Adopt and use best practices and methodologies to enhance cybersecurity (references NIST).			
a. Implement multi-factor authentication.	Incomplete - the majority of SLG entities are in the implementation phase.	3. Documented Policy	2, 3



Completed by WaTech's Office of Cybersecurity (OCS)			
Cybersecurity Plan Required Elements	Description of Current Capabilities	Capability Level <small>(See Table 7 for capability level designations)</small>	Project # <small>(s)</small>
b. Implement enhanced logging.	Most SLG entities only have default logging in place. Very rarely do we find that they have engaged a managed detection and response vendor. Also, they very rarely have an internally or externally managed SIEM. None of this is typically well documented as procedures or standards.	3. Documented Policy	2
c. Data encryption for data at rest and in transit.	Incomplete - the majority of SLG entities are in the implementation phase.	5. Implementation in Progress	2
d. End use of unsupported/end of life software and hardware that are accessible from the internet.	Incomplete - the majority of SLG entities are in the implementation phase. Documentation/policy around this is extremely rare.	3. Documented Policy	1, 2
e. Prohibit use of known/fixed/default passwords and credentials.	Different processes are used across the SLG entities. Very rarely do SLGs have documented standards for this; usually it is just IT people doing it because they know they need to.	4. Partially Documented Standards and Procedures	1, 2



Completed by WaTech’s Office of Cybersecurity (OCS)			
Cybersecurity Plan Required Elements	Description of Current Capabilities	Capability Level <small>(See Table 7 for capability level designations)</small>	Project # <small>(s)</small>
f. Ensure the ability to reconstitute systems (backups).	Most SLG entities do not have such devices/software facing the internet, though of course some very rarely slip through. Internal facing only outdated systems are uncommon, but not rare. Documentation/policy around this is extremely rare.	4. Partially Documented Standards and Procedures	2
g. Migration to the .gov internet domain.	Incomplete across the eligible entities.	4. Partially Documented Standards and Procedures	1, 2
6. Promote the delivery of safe, recognizable, and trustworthy online services, including using the .gov internet domain.	A myriad of domains are used throughout the state. Many municipal governments are using the .gov domain. There are a substantial number of entities such as water and sewer districts and utilities that use .org and .com and are unlikely to change to .gov for perceptual reasons. Educational institutions generally use the .edu domain.	4. Partially Documented Standards and Procedures	1, 2
7. Ensure continuity of operations including by conducting exercises.	Different processes are used across the various SLG entities.	3. Documented Policy	1, 4



Completed by WaTech’s Office of Cybersecurity (OCS)			
Cybersecurity Plan Required Elements	Description of Current Capabilities	Capability Level <small>(See Table 7 for capability level designations)</small>	Project # <small>(s)</small>
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).	No documented implementation of the NIST NICE Workforce Framework was found in its audits of SLG entities.	2. Informally Done	4
9. Ensure continuity of communications and data networks in the event of an incident involving communications or data networks.	The State is developing, improving and updating incident response plans which include processes for post-incident communications. Many of the larger jurisdictions also have incident response plans in varying stages of development. Little is known of the smaller local entities, it is assumed, based on what is known that most are at the foundational level. Washington updated and adopted a new State Communications Interoperability Plan (SCIP) through the State Interoperability Executive Committee (SIEC) with the assistance of CISA.	3. Documented Policy	1



Completed by WaTech’s Office of Cybersecurity (OCS)			
Cybersecurity Plan Required Elements	Description of Current Capabilities	Capability Level <small>(See Table 7 for capability level designations)</small>	Project # <small>(s)</small>
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 - The State and Local Government entities have partially documented policies and standards.	4. Partially Documented Standards and Procedures	1
11. Enhance capabilities to share cyber threat indicators and related information between the eligible entity and the Department.	Most SLG entities do not share cyber threat indicators with other local municipalities.	4. Partially Documented Standards and Procedures	1, 2
12. Leverage cybersecurity services offered by the Department.	The NOFO requires organizations receiving funding from the SLCGP to complete the NCSR and engage with CISA vulnerabilities and web application scanning. It is unknown to what extent this is occurring. In 2021, the state and 52 cities and counties completed the NCSR.	3. Documented Policy	1



Completed by WaTech’s Office of Cybersecurity (OCS)			
Cybersecurity Plan Required Elements	Description of Current Capabilities	Capability Level <small>(See Table 7 for capability level designations)</small>	Project # <small>(s)</small>
13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives.	It is anticipated that SLG entities rarely engage in such alignment. Review of processes are uncommon, and only a few formally consider security as part of the process. At the strategic/larger objectives level even fewer coordinate IT operations and cybersecurity. Documentation of this at the strategic level does not seem to be occurring.	2. Informally Done	2
14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats.	Different processes are used across the various SLG entities. Some SLG entities take part in industry specific groups that share information. Most counties and cities are members of ACCIS. There are 364 MS-ISAC members within the state of Washington. The extent of their individual participation is unknown..	2. Informally Done	1, 2
15. Ensure rural communities have adequate access to, and participation in plan activities.	Inherent in the program administration.	N/A	N/A



Completed by WaTech's Office of Cybersecurity (OCS)			
Cybersecurity Plan Required Elements	Description of Current Capabilities	Capability Level <small>(See Table 7 for capability level designations)</small>	Project # #(s)
16. Distribute funds, items, services, capabilities, or activities to local governments.	EMD has experience managing FEMA/DHS Grant programs. The experience with this department will be leveraged to support this grant program.	N/A	N/A



Appendix B: Project Summary Worksheet

Table 9 shows four categories of potential projects based on the local government capability assessment. Projects proposed outside of these categories will also be considered for funding.

Table 9: Project Summary Worksheet

Project Name	Project Description	Related Required Element #	Cost ⁸	Status	Priority	Project Type
1 Cybersecurity Assessment Program	Assess and document a jurisdiction’s security posture and recommend areas for improvement.	1, 2, 3, 4, 5, 6, 7, 9, 10, 11, 12, 14	\$ 1,750,000	Future	High	Plan
	Leverage CISA and/or MS-ISAC-provided web application and network vulnerability scanning services.					
	Utilize state negotiated contracts with qualified consulting firms to conduct security assessments to objectively assess the security posture of the municipality. Each grant application would be preceded by a					

⁸ The total estimated cost of the identified projects only equals \$4,000,000. These are only estimates, actual budgets are not available since no projects have yet been selected for funding.



Project Name	Project Description	Related Required Element #	Cost ⁸	Status	Priority	Project Type
	Statement of Work and bid from the contractor for the assessment.					
2 Endpoint Management Software	Endpoint Management Software enables local agencies to automate their endpoint inventory and management workflows. This deployment will track endpoint activity, allowing administrators to isolate individual endpoints in response to a threat.	1, 2, 3, 4, 5, 6, 11, 13, 14	\$ 1,000,000	Future	High	Platform
	The state may negotiate a master agreement with endpoint security solution providers, enabling volume discount prices for entities.					
3 Multi-Factor Authentication	Software tokens are a cost-effective and flexible option for deploying MFA. The state may negotiate volume discounts with an MFA solution provider.	1, 5	\$ 500,000	Future	High	Platform
	State-wide MFA deployment is an initial step towards deploying identity and access management across the local entities.					



Project Name	Project Description	Related Required Element #	Cost ⁸	Status	Priority	Project Type
4 Security and Privacy Training	Deliver a security and privacy curriculum to bolster the knowledge, skills, and abilities that local municipalities bring to bear against cyber criminals.	7, 8	\$ 750,000	Ongoing	High	Training
	Utilize a state-negotiated master contract with vendor(s) to provide information security and privacy awareness content for jurisdictional employees.					
	Utilize a state-negotiated master contract with vendor(s) to provide a phishing simulation platform.					
	Identify and provide professional cybersecurity training to cyber practitioners. Examples of such training may include but not be limited to:					
	<table border="1"> <tr> <td>CISSP</td> <td>HISP</td> </tr> <tr> <td>CISM</td> <td>Privacy (IAPP)</td> </tr> <tr> <td>CISA</td> <td></td> </tr> </table>					
CISSP	HISP					
CISM	Privacy (IAPP)					
CISA						



Project Name	Project Description		Related Required Element #	Cost ⁸	Status	Priority	Project Type
	SANS GIAC	Technical platform trainings (Cisco, CrowdStrike, Fortinet, Microsoft, etc.)					



Appendix C: Entity Metrics

Table 10: Cybersecurity Plan Metrics

Program Goal	Program Objectives	Associated Metrics	Metric Description (details, source, frequency)
Goal 1 - Improve the cybersecurity posture of all local governments and entities.	Enhance risk assessment and risk management capabilities within local jurisdictions by improving NCSR responses to level 5 (Implementation in Process) per the NIST CSF . (SLCGP NOFO elements 12, 14)	Number of local jurisdictions that have a final cybersecurity plan.	Reported by sub recipient. Reporting: Annually.
		Number of local jurisdictions that are participating in CISA's CyHy program.	Reported by sub recipient. Reporting: Annually.
	Enhance business continuity (BC) and information technology disaster recovery (IT DR) capabilities within local jurisdictions by improving NCSR responses to level 5 (Implementation in Process) per the NIST CSF . (SLCGP NOFO elements 1, 5, 9)	Number of local jurisdictions that have a final Cybersecurity/IT Incident Response Plan.	Reported by sub recipient. Reporting: Annually.
		Number of local jurisdictions that have a robust IT/Cybersecurity backup plan or program.	Reported by sub recipient. Reporting: Annually.



Program Goal	Program Objectives	Associated Metrics	Metric Description (details, source, frequency)
		Number of local jurisdictions that have an alternate site for operations.	Reported by sub recipient. Reporting: Annually.
	Enhance incident response and recovery capabilities within local jurisdictions by improving NCSR responses to level 5 (Implementation in Process per the NIST CSF . (SLCGP NOFO elements 2, 3))	Number of local jurisdictions that have a final Cybersecurity/IT Incident Response Plan.	Reported by sub recipient. Reporting: Annually.
		Number of local jurisdictions that have a executed an incident response tabletop.	Reported by sub recipient. Reporting: Annually.
	Identify best practices for sharing threat intelligence, indicators of compromise and indicators of attack between victims and partner organizations. (SLCGP NOFO element 11)	Number of local jurisdictions that are participating in CISA's CyHy Program.	Reported by sub recipient. Reporting: Annually.
		Number of local jurisdictions that are receiving WA State Fusion Center alerts.	Reported by sub recipient. Washington State Fusion Center. Reporting: Annually.



Program Goal	Program Objectives	Associated Metrics	Metric Description (details, source, frequency)
		Number of local jurisdictions that are members of the Multi-State Information Sharing and Analysis Center (MS-ISAC).	Reported by sub recipient. MS-ISAC. Reporting: Annually.
	Promote industry standards for information security. (SLCGP NOFO element 6)	Number of local jurisdictions that have had a CISA Cybersecurity assessment.	Reported by sub recipient. Reporting: Annually.
Goal 2 - Increase cybersecurity and privacy capacity at the state and local level.	Implement redundant and resilient data storage and transmission systems. (SLCGP NOFO element 7)	Number of local jurisdictions that have a robust IT/Cybersecurity backup plan or program.	Reported by sub recipient. Reporting: Annually
		Number of local jurisdictions that have an alternate site for operations.	Reported by sub recipient. Reporting: Annually.



Program Goal	Program Objectives	Associated Metrics	Metric Description (details, source, frequency)
	Develop a competent professional IT workforce using standardized curricula. (SLCGP NOFO element 8)	Number of local jurisdictions that have created a training program for their information technology and security professionals.	Reported by sub recipient. Reporting: Annually.
	Promote a cyber aware culture within state and local jurisdictions and entities through accessible awareness content (SLCGP NOFO element 8)	Number of local jurisdictions that have created an employee cyber awareness program or are using an employee awareness program.	Reported by sub recipient. Alternatively, Washington State may leverage master contract purchasing power to obtain an awareness platform for use by the SLTs. In such a case, OCS would have access to the information. Reporting: Annually.



Program Goal	Program Objectives	Associated Metrics	Metric Description (details, source, frequency)
		Number of local jurisdictions that have implemented a phishing simulation platform or are using a phishing simulation platform.	Reported by sub recipient. Alternatively, Washington State may leverage master contract purchasing power to obtain a phishing simulation platform for use by the SLTs. In such a case, OCS would have access to the information. Reporting: Annually.
Goal 3 - Develop enduring partnerships to support cyber resilience across the State of Washington.	Identify coalitions of local jurisdictions to support implementation of identified SLCGP projects. (SLCGP NOFO element 13)	Count of groups and local jurisdictions that are partnering together to meet project goals.	Grant application submissions. Reported by sub recipient. Reporting: Annually.
	Work with SLT stakeholders to ensure compatibility of state and local cyber incident response plans. (SLCGP NOFO element 3, 14)	Number of local jurisdictions that have attended the CISA-sponsored Incident Response Training Workshops/Exercises throughout the state.	Reported by sub recipient. Reporting: Annually.



Program Goal	Program Objectives	Associated Metrics	Metric Description (details, source, frequency)
		Number of local jurisdictions that have a final Incident Response plan.	Reported by sub recipient. Reporting: Annually.
	Invest in the future cybersecurity workforce by conducting outreach on cybersecurity career pathways for K-20 students. (SLCGP NOFO elements 8, 13)	Number of local jurisdictions that have actively performed outreach to local community colleges or universities.	Reported by sub recipient. Reporting: Annually.
		Number of local jurisdictions that have connected with the PISCES program.	Reported by sub recipient. PISCES Management. Reporting: Annually.
Goal 4 - Effectively use existing funds and	Demonstrate progress towards cyber risk reduction at the end of	Number of local jurisdictions that have an active risk registry.	Reported by sub recipient. Reporting: Annually.



Program Goal	Program Objectives	Associated Metrics	Metric Description (details, source, frequency)
identify sustainable funding options.	each funding cycle. (SLCGP NOFO element 10)	For the jurisdictions that have a risk registry, how many have spent money to implement projects that remove risk from the registry?	Reported by sub recipient. Reporting: Annually.
	Amplify the reach of projects by prioritizing those that can be extrapolated and shared with other jurisdictions. (SLCGP NOFO element 10)	Identify the number of projects that have multiple local jurisdictions attached and track the progress of those orgs.	Grant application submissions. Reported by sub recipient. Reporting: Annually.
	Leverage state master contracts to support accessible pricing for cyber resilience products, platforms and solutions to all jurisdictions throughout Washington State. (SLCGP NOFO element 4)	Number of contracts and the number of SLTs associated with each contract.	Grant application submissions. Reported by sub recipient. Contract managers. Reporting: Annually.
	Apply values of equity when prioritizing proposed projects from local jurisdictions or entities. (Appendix E: Alignment with Equity and Inclusion Directives)	Track number of rural, urban, suburban projects and evaluate them with an equity lens.	



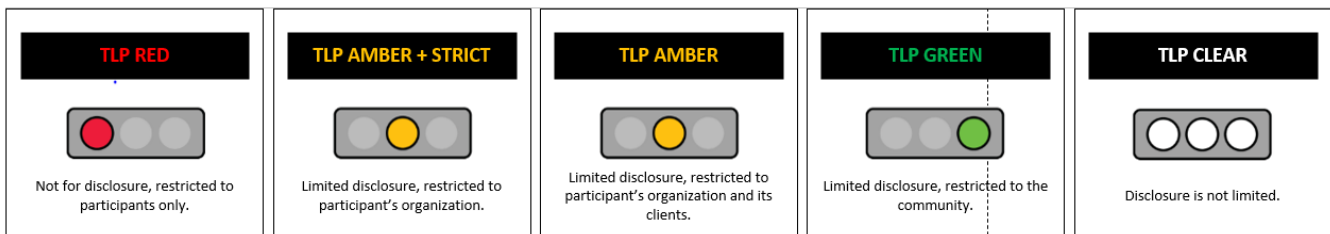
Appendix D: Data Security Categorization and Critical Infrastructure

Protected Critical Infrastructure Information Program

Safe data handling is critical to ensure that sensitive systems are protected from exploitation of vulnerabilities. The CCIP manages the Washington State [Protected Critical Infrastructure Information Program \(PCII\)](#) in partnership with the Cybersecurity and Critical Infrastructure Security Agency (CISA). All CCIP Personnel and WA-CIPHR members are required to undergo [PCII Authorized User training](#) to ensure safe handling of sensitive data.

Data Handling Practices

CCIP utilizes [DHS CISA’s Traffic Light Protocol](#) for civilian data, and the [Department of Defense classification system](#) for all data requiring a security clearance.



Washington State Information Classification Categories

Under WaTech’s OCS [Data Classification Standard](#), state agencies must classify data and information into categories based on sensitivity. When sharing, transferring or otherwise disclosing information and during a response to a cyber incident, responding state agencies must ensure that sharing data and information with the public or other entities complies with this policy. When sharing Category 3 or higher data outside an agency, a Data Sharing Agreement (DSA) must be in place as prescribed in the Office of Cybersecurity’s [Data Sharing Policy](#).

Labeling Data for Secure Handling

Per DHS-CISA: “Only the PCII Program Office or the PCII Program Manager Designees may mark information as PCII and assign a submission identification number. To ensure proper handling and safeguarding from disclosure:

- PCII documents include a PCII Program Green Cover Sheet outlining protection requirements.
- PCII is marked with “PROTECTED CRITICAL INFRASTRUCTURE INFORMATION” in the headers and footers to alert users of the information’s status and protection requirements.
- PCII is labeled with a unique identification number.

The PCII marking remains until either the PCII Program Office determines the information no longer qualifies for PCII protection or the submitter requests the removal of protections. PCII is normally



labeled with the following statement by the PClI Program Office to ensure the material is safeguarded and handled appropriately.

“This document contains Protected Critical Infrastructure Information. In accordance with the provisions of the Critical Infrastructure Information Act, 6 U.S.C. §§ 131 et seq., it is exempt from release under the Freedom of Information Act (5 U.S.C. § 552) and similar state and local disclosure laws. Unauthorized release may result in criminal and administrative penalties. PClI must be safeguarded and shared in accordance with the Critical Infrastructure Information Act, 6 U.S.C. §§ 131 et seq., the implementing regulation, 6 CFR part 29 and PClI Program requirements.”



Appendix E: Alignment with Equity and Inclusion Directives

Washington State Diversity, Equity and Inclusion Commitment

On February 1, 2023, Governor Jay Inslee issued a [state proclamation](#) to expand the efforts for Diversity, Equity, and Inclusion (DEI) awareness and training for all government employees. The proclamation identifies ways to enhance the overall approach to DEI initiatives. This enhanced awareness will include incorporating these values into assessing sub-recipient proposals.

Washington State Pro-Equity and Anti-Racism (PEAR)

In [2018](#), Governor Jay Inslee called on state agencies to take action to create an inclusive and respectful workplace and in 2022 issued [Executive Order 22-02](#) "Achieving Equity in Washington State Government." The goal of this directive is to create a starting point for a shared foundation of critical knowledge and to promote DEI in the administration of an agency's policies, practices, and procedures.

The goals and objectives of this plan recognize the differences of resources and capabilities between each population. The Cybersecurity Plan and SLCGP support and aims towards an equitable distribution of assets utilizing the critical knowledge DEI provides.

The Washington State PEAR initiative, managed through the Office of Equity for Washington State, has been implemented in all state agencies. The SLCGP Planning Committee adopts these concepts as core tenants of our inclusion strategy.

Federal Accessibility for Virtual Products

Information and communications technology (ICT) accessibility refers to ensuring the ability of everyone, regardless of disability, to access, use and benefit from information technology and systems. In accordance with [Section 508](#), which requires federal agencies to ensure the accessibility of their ICT, the SLCGP as a federal grant also requires the passthrough agency and recipient of the grant to ensure the funded program do not discriminate against qualified individuals with disabilities. SLCGP will be administered to ensure compliance with Section 508 through the integration of the needs of people with disabilities at all levels of the program that utilizes ICT.



Appendix F: Acronyms

Table 11: List of Acronyms

Acronym	Definition
ACCIS	Association of County and City Information Services
AWC	Association of Washington Cities
CCIP	Cybersecurity and Critical Infrastructure Protection
CCW	Career Connect Washington
CISA	Cybersecurity and Infrastructure Security Agency
CISA	Certified Information Security Auditor
CISM	Certified Information Security Manager
CISSP	Certified Information Systems Security Professional
COP	Common Operating Picture
CPG	Comprehensive Preparedness Guide
CSET	Cybersecurity Evaluation Tool
CSF	Cybersecurity Framework
CTS	Consolidated Technology Solutions (aka WaTech)
CyHy	CISA's Cyber Hygiene Program
DEI	Diversity, Equity, and Inclusion
DHS	Department of Homeland Security
DSA	Data Sharing Agreement
EMD	Emergency Management Division
FEMA	Federal Emergency Management Agency
FBI	Federal Bureau of Investigation



Acronym	Definition
GIAC	Global Information Assurance Certification
HISP	Holistic Information Security Practitioner Certification
IAPP	International Association of Privacy Professionals
ICT	Information and Communications Technology
IGN	Intergovernmental Network
IIJA	Infrastructure Investment and Jobs Act
MFA	Multi-Factor Authentication
MS-ISAC	Multi-State Information Sharing and Analysis Center
NCSR	Nationwide Cybersecurity Review
NICC	National Infrastructure Coordinating Center
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
NOFO	Notice of Funding Opportunity
NOI	Notice of Intent
OCIO	Washington State Office of the Chief Information Officer
OCS	Washington State Office of Cybersecurity
PCII	Protected Critical Infrastructure Information Program
PEAR	Pro-Equity and Anti-Racism
PISCES	Public Infrastructure Security Cyber Education System
PPR	Performance Progress Report
SANS	Escal Institute of Advanced Technologies
SAO	State Auditor's Office



Acronym	Definition
SCIP	State Communications Interoperability Plan
SGN	State Government Network
SIEC	State Interoperability Executive Committee
SLCGP	State and Local Cybersecurity Grant Program
SLG	State and Local Government Entities
SLT	State, Local and Tribal Governments
SPR	Stakeholder Preparedness Review
TCGP	Tribal Cybersecurity Grant Program
THIRA	Threat and Hazard Identification and Risk Assessment
WA-CIPHR	Washington Coalition for Infrastructure Protection and Homeland Resilience
WaTech	Washington Technology Solutions (aka CTS)
WSAC	Washington State Association of Counties
WSFC	Washington State Fusion Center
WTIA	Washington Technology Industry Association



Appendix G: Glossary

Availability: The property of information being accessible and usable upon demand by an authorized entity (Workforce Member or process).

Continuity of Operations (COOP): A predetermined set of instructions or procedures that describe how an organization's mission essential functions will be sustained within 12 hours and for up to 30 days as a result of a disaster event before returning to normal operations.

Confidentiality: The property that data or information is not made available or disclosed to unauthorized persons or processes.

Critical Infrastructure: Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination thereof.

Data: Representation of facts, concepts, or instructions in a manner suitable for communication, interpretation, or processing by humans or by automatic means.

Department of Homeland Security (DHS): The United States Department of Homeland Security (DHS) is the U.S. federal executive department responsible for public security, comparable to the interior or home ministries of other countries. Its stated missions involves anti-terrorism, border security, immigration and customs, cybersecurity, and disaster prevention and management.

Disaster Recovery (DR): Disaster recovery is the process of maintaining or reestablishing vital infrastructure and systems following a natural or human-induced disaster, such as a storm or battle. It employs policies, tools, and procedures. Disaster recovery focuses on the information technology (IT) or technology systems supporting critical business functions as opposed to business continuity. This involves keeping all essential aspects of a business functioning despite significant disruptive events; it can therefore be considered a subset of business continuity.

Disaster: A disruption of services, community capital, or assets beyond the ability to cope with local resources.

Emergency Management (EM): Emergency management or disaster management is the managerial function charged with creating the framework within which communities reduce vulnerability to hazards and cope with disasters.

Emergency Management Accreditation Program (EMAP): Created by a group of national organizations to foster continuous improvement in emergency management capabilities, the standard, assessment, and accreditation process provides emergency management programs the opportunity to be recognized for compliance with industry standards, to demonstrate accountability, and to focus attention on areas and issues where resources are needed.

Emergency: Any incident that requires responsive action to protect life or property.

Event: any observable occurrence in a system and/or network. Events sometimes provide an indication that an incident is occurring.

Exercise: A simulation of an emergency designed to validate the viability of one or more aspects of an IT plan.



Incident: An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Industry: To include private sector and special municipalities (e.g., ports and public utility districts).

Information Technology: Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

Integrity: The condition whereby data or information has not been improperly modified or destroyed and authenticity of the data or information can be ensured.

Multifactor Authentication (Two-Factor Authentication, MFA or 2FA): Authentication method using different types of factors to gain access to a resource. Factors include: (i) something you know (e.g., password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric).

Policy: High level statements of intention and direction of an organization as formally expressed by its top management.

Risk: A measure of the extent to which the entity is threatened by a potential circumstance or event, Risk is typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

Risk Assessment: The process of identifying, prioritizing, identifying potential threats and estimating risks. This includes determining the extent to which adverse circumstances or events could impact the company. Uses the results of threat and vulnerability assessments to identify risk to organizational operations and evaluates those risks in terms of likelihood of occurrence and impacts if they occur. The product of a risk assessment is a list of estimated potential impacts and unmitigated vulnerabilities. Risk assessment is part of risk management.

Risk Management: The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations resulting from the operation or use of an information system, and includes: (1) the conduct of a risk assessment; (2) the implementation of a risk mitigation strategy; (3) employment of documented techniques and procedures for the continuous monitoring of the security state of the Information system; and (4) documenting the overall risk management program.

Risk Mitigation: Prioritizing, evaluating, and implementing the appropriate risk-reducing safeguards and countermeasures recommended from the risk management process.

Standards: Documents that support policies and indicate how and what kind of technology and business processes must be implemented, used and maintained to meet policy objectives.

State Administrative Agency (SAA): Entity designated by the Governor that applies for SLCGP to DHS/FEMA on behalf of the state. For Washington, the responsibility rests with the Washington Military Department Emergency Management Division. The SAA is responsible for administration of the grant to include management of passthrough grant agreements.



State Interoperability Executive Committee (SIEC) Advisory Workgroup (SAW): Our emergency responders cannot always talk to each other during crisis situations. The State Interoperability Executive Committee (SIEC) works to ensure that all emergency responders, across all levels of government and across all jurisdictions can talk to each other and share data.

Threat: Any circumstance or event with the potential to adversely impact operations (including mission, functions, image, or reputation), organizational assets, individuals, or other organizations through an information system via unauthorized access, destruction, disclosure, modification of Information, and/or denial of service.

Vulnerability: A weakness in a system, application, data, network or process that is subject to exploitation or misuse.











Adopted SLCGP WA Cybersecurity Plan - June 6, 2023

Final Audit Report

2023-06-12

Created:	2023-06-06
By:	Rhonda Mendel (rhonda.mendel@watech.wa.gov)
Status:	Signed
Transaction ID:	CBJCHBCAABAALok74tPhGKYJDTHx5rAjqIYXXORT_55w

"Adopted SLCGP WA Cybersecurity Plan - June 6, 2023" History

-  Document created by Rhonda Mendel (rhonda.mendel@watech.wa.gov)
2023-06-06 - 11:40:28 PM GMT
-  Document emailed to bill.kehoe@watech.wa.gov for signature
2023-06-06 - 11:49:00 PM GMT
-  Email viewed by bill.kehoe@watech.wa.gov
2023-06-07 - 1:40:30 AM GMT
-  Email viewed by bill.kehoe@watech.wa.gov
2023-06-08 - 1:06:27 AM GMT
-  Signer bill.kehoe@watech.wa.gov entered name at signing as William S Kehoe
2023-06-08 - 1:06:51 AM GMT
-  Document e-signed by William S Kehoe (bill.kehoe@watech.wa.gov)
Signature Date: 2023-06-08 - 1:06:53 AM GMT - Time Source: server
-  Document emailed to Robert Ezelle (robert.ezelle@mil.wa.gov) for signature
2023-06-08 - 1:06:56 AM GMT
-  Email viewed by Robert Ezelle (robert.ezelle@mil.wa.gov)
2023-06-12 - 1:27:12 PM GMT
-  Document e-signed by Robert Ezelle (robert.ezelle@mil.wa.gov)
Signature Date: 2023-06-12 - 1:28:10 PM GMT - Time Source: server
-  Agreement completed.
2023-06-12 - 1:28:10 PM GMT