Washington State Cybersecurity Prevention Framework

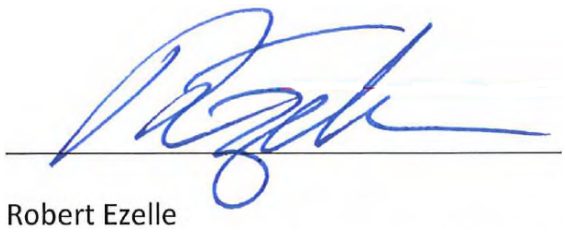
Annex to the Washington State Comprehensive Emergency Management Plan (CEMP)

Document History

	Editor	Date	Notes
1	Tristan Allen | WA Military Department, Emergency Management Division	12/16/24	Initial version promulgated.
2			
3			
4			
5			

Promulgation & Signatories

This document is approved for implementation by the following authorities as of December 16, 2024. This plan supersedes all previous plans and directives.



Robert Ezelle
Director, Emergency Management Division
Washington Military Department

Contents

Introduction, Purpose & Scope

Cybersecurity threats against sensitive technological systems, especially networked systems, are increasing in severity and frequency. This is compounded by the complexity of our built environment, where critical infrastructure and essential community services are increasingly reliant on networked systems and dependent on each other for day-to-day operations. To address this hazard, the state of Washington must prepare for and seek to prevent and protect against the cybersecurity threats through a "whole-of-government, whole-of-community" approach.

A unified, coordinated approach to cybersecurity prevention and protection activities is needed to reduce the risk of cyber incidents across our state's communities and critical infrastructure. No one level of government or private sector entity owns the problem. This framework provides a broad structure for state agencies to align efforts to improve cybersecurity resilience through shared goals and a common understanding of roles and responsibilities across accountable entities.

Purpose

This document is a framework for prevention and protection activities designed to reduce the risk of cybersecurity incidents that impact the security or wellbeing of Washington residents.

Vision

Alignment across state and federal government cybersecurity prevention and protection activities to maximize positive effect and identify cybersecurity preparedness gaps across government and industry.

Scope

This framework applies to all state agencies involved in cybersecurity prevention, protection, and mitigation activities in Washington State. It guides an overall approach for supporting cybersecurity resilience at a statewide level. It encourages collaboration and shared approaches across agencies but recognizes the administration of these programs is the responsibility of individual organizations.

This framework also references prevention and protection actions taken by federal agencies. This plan does not direct federal agencies toward specific actions but lists their activities to synchronize state-led efforts towards a common goal of cyber preparedness across the state.

This document does not provide planning considerations for cyber incident response. Guidance for the state's approach to responding to a significant cyber incident can be found in the Comprehensive Emergency Management Plan (CEMP) Significant Cyber Incident Response Annex.

Situation Overview

Information technology has grown to provide both government and the private sector with an efficient and timely means of delivering essential services throughout the United States. Critical systems are at an increased risk due to this connectivity. The state of Washington seeks to lower the risks present in computer applications, information technology networks, and operational technology that enable the facilitation of critical infrastructure operations.

Securing infrastructure and government services from cyberattacks requires a concerted effort blending federal and state resources into a cohesive strategy. At its core, this mission hinges on collaboration, information sharing, and a reliance on shared best practices. Federal agencies play a critical role in setting overarching cybersecurity standards, and providing threat intelligence and resources. They establish frameworks, guidelines, and best practices, ensuring that states have a foundation for safeguarding their virtual and physical infrastructure. Meanwhile, state governments bring localized insights, agility, and hands-on approaches to addressing cyber threats specific to their jurisdictions. Collaboratively, they cultivate a culture of preparedness, invest in technology, and prioritize cyber-resilience across all levels of government. This shared mission fosters a unified front against cyber adversaries, where expertise and resources are pooled to fortify the nation's digital defenses, ensuring the integrity and reliability of essential services to all residents.

A whole-of-government approach in tandem with private sector partnerships is required to secure critical infrastructure systems and networks. This includes, but is not limited to, such measures as incident response planning, education and awareness, grant funding, and training and exercise.

This framework integrates the domains of emergency management and information technology management. It is therefore important to acknowledge the integration of Information Technology (IT) and Operational Technology (OT) organizations utilizing the National Institute of Standards and Technology (NIST) Cybersecurity Framework. The NIST framework provides a standard, structured approach to cybersecurity and risk management, and is the recommended methodology for individual organizations to use when developing and maintaining a comprehensive cybersecurity capability.

Organization & Coordination of Efforts

Government support for cyber prevention activities has seen notable proliferation across various agencies in recent years. Recognizing the criticality of cybersecurity in today's digital landscape, governmental bodies have allocated significant resources to bolster defenses against cyber threats. However, amidst this surge in initiatives, there arises a pressing need to unify these efforts into a cohesive strategy. At times, the endeavors of different agencies may appear disjointed or duplicative, which can undermine the overall effectiveness of our collective cyber defense posture. Therefore, integrating disparate cyber prevention activities under a comprehensive framework is imperative to streamline operations, enhance coordination, and maximize resources for a more robust defense against evolving cyber threats. Centralizing strategies and fostering collaboration among agencies can lead to greater cooperation, efficiency, and ultimately, better protection of critical digital infrastructure and sensitive information.

Risk Assessment

Risk assessments serve as the cornerstone for identifying, prioritizing, and mitigating potential cyber threats and weaknesses within an organization's digital infrastructure. By conducting thorough risk assessments, organizations gain a clear understanding of their unique threat landscape, including vulnerabilities that adversaries may exploit to compromise systems or steal sensitive data. Through vulnerability assessments, specific weaknesses in software, hardware, system configurations, and

operational processes are identified, allowing for proactive remediation before these vulnerabilities can be exploited. By regularly performing these assessments, organizations can stay ahead of emerging threats, allocate resources effectively, and implement targeted security measures to reduce the likelihood and impact of cyber incidents. In essence, risk and vulnerability assessments provide the foundational insights necessary to develop and maintain a robust cybersecurity posture tailored to the evolving threat landscape.

Third-Party Security Assessments

Third-party security assessments provide an external view of a government's security environment and can highlight vulnerabilities and risks the government was not fully aware of. Depending on the scope, third-party assessments can provide the following insights:

- Help identifying current vulnerabilities due to gaps in patching and network configurations, among other areas;
- Providing recommendations for improving the control environment through stronger policies, procedures, and technical controls; and
- Assessing compliance with relevant state, federal, or industry security standards.

The results of third-party assessments should feed into a government's risk assessment process. They can also be used to identify and help prioritize the need for additional security resources.

Incident Response Planning

Incident response planning serves as a critical link between government agency preventative efforts and cyber resiliency. While preventative measures aim to minimize the occurrence of cyber incidents, the reality is that no system can be entirely immune to attacks. Therefore, having a well-defined incident response plan is essential for efficiently and effectively addressing and mitigating the impact of cyber incidents when they occur. By connecting incident response planning to preventative efforts, government agencies can establish a comprehensive approach to cyber resiliency.

Incident response planning provides a structured framework for how agencies should respond to cyber incidents, ensuring a coordinated and timely response across all levels of the organization. This alignment helps minimize confusion and delays in addressing cyber threats, enabling agencies to contain and mitigate the impact of incidents more swiftly.

Incident response planning allows agencies to leverage insights gained from past incidents to strengthen preventative measures. By analyzing the root cause and tactics employed by adversaries during cyber incidents, agencies can identify weaknesses in their defenses and proactively enhance security controls to prevent similar incidents in the future.

Incident response planning fosters a culture of continuous improvement and learning within government agencies. Through post-incident reviews and evaluations, agencies can identify areas for improvement in their preventative measures, response procedures, and overall cybersecurity posture. This iterative process enables agencies to adapt and evolve their strategies in response to emerging threats and changing risk landscapes, thereby enhancing their overall cyber resiliency.

The connection between incident response planning and agency preventative efforts for cyber resiliency is crucial for building a holistic approach to cybersecurity.

Education and Awareness

Education and awareness training are crucial components that connect to Washington State's preventative efforts for cyber resiliency. These initiatives play a pivotal role in fostering a culture of cybersecurity awareness among government employees, contractors, stakeholders, and the public. Through education programs, workshops, and awareness campaigns individuals are better equipped with the knowledge and skills needed to recognize, prevent, and respond to cyber threats effectively. By instilling a sense of responsibility and vigilance regarding cybersecurity best practices, education and awareness efforts empower individuals to become proactive participants in safeguarding sensitive information, critical infrastructure, and national security interests. As cyber threats continue to evolve and become increasingly sophisticated, ongoing education and awareness initiatives help ensure that government personnel remain informed about emerging risks, new attack vectors, and evolving trends in cybercrime.

Training and Exercise

Training and exercise are pivotal in connecting Washington State's preventative efforts for cyber resiliency within its agencies, stakeholders, political subdivisions, and citizenry. Training equips personnel with knowledge, skills, and awareness needed to recognize and respond effectively to cyber threats. It ensures that its audience understands cybersecurity best practices, policies, and procedures, enabling them to implement preventive measures and mitigate risks proactively. Additionally, training fosters a culture of cybersecurity awareness and responsibility across all levels of the organization, empowering individuals to play an active role in safeguarding digital assets and sensitive information.

Exercises simulate real-world cyber incidents and test the efficacy of response plans, procedures, and coordination mechanisms. By conducting regular drills and tabletop exercises, government agencies can identify gaps, refine incident response protocols, and enhance coordination among stakeholders, including internal teams, external partners, and relevant authorities. These exercises provide invaluable opportunities for personnel to practice their roles and responsibilities in a controlled environment, improving readiness and resilience in the face of actual cyber threats.

The integration of training and exercises in Washington State's preventative effort fosters a culture of continuous improvement and adaptation to evolving cyber threats, allowing organizations to stay ahead of emerging challenges. These efforts enhance interagency collaboration and coordination, facilitating a cohesive and unified response to cyber threats that may transcend organizational boundaries.

Grant Funding

Grant funding provides important and crucial financial support for the development, implementation, and enhancement of cybersecurity measures. Washington State's passthrough agencies allocate grant funds to support initiatives aimed at improving cyber resiliency across various sectors, including critical infrastructure, healthcare, education, political subdivisions, and small businesses. These funds also support state agency initiatives to become more cyber resilient by implementing preventative measures.

These funds may be used to establish cybersecurity awareness and training programs, deploy advanced security technologies, conduct risk assessments, and facilitate information sharing and collaboration among stakeholders. Importantly, grant funding enables agencies to address cybersecurity challenges that may exceed their existing budgets or expertise, fostering a more proactive and coordinated approach to cyber defense. Grant funding supports innovation and research in cybersecurity, driving the development of new technologies and strategies to address emerging threats and vulnerabilities. Grant funding, specifically the State and Local Cybersecurity Grant Program (SLCGP), is a critical enabler of agency preventative efforts for cyber resiliency, ensuring that resources are allocated effectively to safeguard critical assets and infrastructure against evolving cyber threats.

Washinton State Agencies' Division of Responsibilities

Agency	Activity	Description
State Auditor's Office	State & Local Security Audits	• Performs independent cybersecurity audits under its performance audit authority. Testing may include internal and external vulnerability assessment and penetration testing of networks, systems, and applications, as well as testing of IT security controls and policies. • Contracts with state agencies and local governments to conduct agreed-upon procedures and engagements to help assess compliance with WaTech and Department of Licensing security requirements. • Coordinates with WaTech on state agency IT security audits, including planning, audit results, remediation of deficiencies, and reporting. • Coordinates with the Military Department when tested applications include critical infrastructure.
State Auditor's Office	Government Consultation Services	• Conducts basic cybersecurity reviews of local governments, small state agencies, and higher education institutions to identify key gaps in security controls that can be addressed easily. • Develops, curates, and promotes cybersecurity resources designed for governments in Washington based on best practices and common issues highlighted in audits. • Provides cybersecurity training, presentations, and consultations.
Secretary of State's Office	Election Security	• Supervises and certifies the Washington State elections. • Secures, operates, and maintains the statewide Election Management System and Voter Registration Database. • Serves as elections' security central point-of-contact for county elections' officers. • Serves as an executive board member of the Elections Infrastructure ISAC (EI-ISAC).

		• Maintains the Washington State Archives, Digital Archives, and State Records Centers.
WA Military Department, Cyber Operations & Planning (J36)	Cyber Security Assessments (CSAs)	When availability allows, conducts cyber security assessments (CSAs) for local government and critical infrastructure organizations. These assessments generally include the following activities: • Network Infrastructure & Traffic Analysis • End-Point Analysis • Enterprise System Analysis • Web-Application Security Analysis • Root-Cause Analysis of Observed Indicators • Network Monitoring • Recommended improvements to continuous monitoring capability • Recommended network hardening actions • Validation of hardening actions • Penetration testing of networks
WA Military Department, Emergency Management Division	Emergency Management	• Responsible for the strategy, policy, and integration of statewide cybersecurity activities through all phases of emergency management. • Develops and maintains the state's Cybersecurity Prevention Framework and the state's Significant Cyber Incident Response Plan. • Ensures statewide cybersecurity training and exercise needs are included in the state's Integrated Preparedness Plan. • Engages critical infrastructure providers to further statewide cybersecurity posture and emergency management preparedness. • The primary state agency to interface with the Department of Homeland Security (DHS) for cybersecurity and critical infrastructure protection activities. • Advises the state legislature and Governor's Office on evolving cybersecurity matters affecting critical infrastructure. • Coordinates and prioritizes National Guard's security assessments of critical infrastructures for public, private, and/or tribal sector agencies and providers upon request.
Department of Commerce (COM) – Energy and Resilience Emergency Management Office (EREMO)	Energy Critical Infrastructure Resilience	• Provides comprehensive emergency management services for the energy sector. • Cybersecurity resilience development for the energy sector. • Coordinates with stakeholders at all levels of government. • Coordinates with electric, natural gas, petroleum, and renewable energy industries statewide.

		• Develops planning documents, standards, training, and operation support during emergencies.
Washington Technology Solutions (WaTech)	Government IT Structure – State Networks	The state's chief information officer serves as a member of the governor's executive cabinet and advises the governor on cybersecurity and technology issues. The chief information officer appoints the state chief information security officer (CISO), who serves as the director of the state Office of Cybersecurity (OCS). Responsibilities of the OCS include: • The CISO is charged with the authority for ensuring the security of all networks and applications administered on the Washington State network. The CISO serves as a senior advisor to state executive branch leadership and the legislature on cybersecurity issues, decisions, and legislation. • OCS is responsible for developing statewide information technology security policies and standards, and ensuring that security is an enabler for the safe delivery of government services to citizens and businesses. • OCS provides enterprise information security services, platforms, technologies, and strategic direction for cybersecurity for Washington State agencies. • OCS is responsible for ensuring the security of information technology infrastructure and data owned, operated, and managed by or on behalf of the state of Washington. • In the event of a cybersecurity incident that affects state government infrastructure or systems, OCS is responsible for determining the scope and severity of the incident, activating an incident response team, and leading the statewide communications response in coordination with the Governor's Office and other appropriate stakeholders. • Provides statewide strategic direction for cybersecurity, including plans and procedures to ensure the continuity of commerce and government in the event of a cybersecurity incident that affects state government. • Reviews the design of new computer systems before they are put in place to help ensure they are secure. • Conducts comprehensive security evaluations and coordinates with state agencies to find and address vulnerabilities in the state networked systems. • Serves as a liaison between the state government and federal cybersecurity resources, including DHS CISA, National Security Agency, FBI, Multi-State Information Sharing and Analysis Center, etc. • Works with stakeholders, including the Department of Commerce and key local, state, and federal partners, to

		maintain the state's status as a national leader in cybersecurity. • Serves as a cybersecurity resource for local governments in Washington.
Washington State Office of the Attorney General	Legal Authority	The Attorney General of Washington is the chief legal officer of the U.S. state of Washington and head of the Washington State Office of the Attorney General. The attorney general represents clients of the state and defends the public interest in accordance with state law.