Washington State Significant Cyber Incident Response Plan

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

Published December 16, 2024

Document History

	Editor	Date	Notes
1	Tristan Allen | WA Military Department, Emergency Management Division	12/16/2024	Initial document 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

In the rapidly evolving landscape of the digital age, organizations face an ever-growing threat landscape characterized by sophisticated cyber adversaries, advanced malware, and persistent cyber threats. The potential impact of a cyber incident underscores the critical need for a well-defined Significant Cyber Incident Response Plan as an appendix to the Response Plan Annex of the Washington State Comprehensive Emergency Management Plan (CEMP). This plan provides decision makers and emergency managers with specific considerations to structure a state response to a significant cyber incident.

Recognizing the need for an overarching policy and approach to cyber incidents occurring in or directly impacting Washington State, this plan was developed as a hazard specific plan—i.e., cyber incident—according to the principles outlined in the National Response Framework (NRF) to remain consistent with the state government's role in coordinating and supporting federal, tribal, and local governments during a response (i.e., a whole-of-government approach). Accepting the guidance provided by the state's CEMP, this plan considers the unique structures needed for the state to support impacted organizations through incident response and into recovery.

Purpose

The primary objective of this plan is to integrate cyber incident response considerations into existing emergency response coordination structures for a whole-of-government approach within the state of Washington. This includes leveraging established incident management structures, such as the National Incident Management System (NIMS), to ensure coordinated and efficient response to cyber incidents. This plan guides Washington State government agencies to an appropriate response structure in the event of a significant cyber incident. The plan details a concept of operations for the state, documents command, control, and coordination, and establishes state agency roles and responsibilities in the event of a significant cyber incident response. It aligns with roles, responsibilities, and response actions taken at the federal, tribal, and local levels of government.

Scope

The Significant Cyber Incident Response Plan applies to all cyber incidents that are deemed significant (as defined below), including those that impact critical infrastructure, compromise sensitive data, or threaten public safety. It provides guidance to state government entities for how the state enterprise will organize itself to respond to a significant cybersecurity incident. It does not provide incident response guidance or procedures for a specific network. Incident response plans that cover specific information technology or operational technologies are maintained by the entity that oversees their operation.

This plan does not provide any guidance regarding statewide cybersecurity prevention, protection, or mitigation activities; nor does it offer response guidance to state and local administrators of information technology systems or operators of operational technologies. To learn more about prevention, protection, and mitigation activities, see the Washington State Cybersecurity Prevention Framework.

Significant Cyber Incident Definition

As documented in Presidential Policy Directive 41, a **cyber incident** is defined as:

> "*An event occurring on or conducted through a computer network that actually or imminently jeopardizes the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon. For purposes of this directive, a cyber incident may include a vulnerability in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.*"

Cyber incidents occur at a near constant basis across organizations in both the public and private sectors. While these frequent attacks are regrettable, it is important to distinguish incidents according to the size and severity of impact they have. While a ransomware attack on a single organization may be catastrophic for that entity, it may not necessitate a coordinated state response unless it generates, or has the potential to generate, impacts to a level that require a Governor's Emergency Proclamation. It is therefore important to further define what constitutes a significant cyber incident.

A significant cyber incident is defined as:

> *An event that is likely to cause, or is causing, harm to critical functions and services across the public and private sectors by impairing the confidentiality, integrity, or availability of electronic information, information systems, services, or networks; and/or threaten public safety, undermine public confidence, or have a negative effect on the economy.*

State-level coordination of significant cyber incidents is triggered when the State Emergency Operations Center (SEOC) activates after receiving a request for assistance related to the incident, at the mandate of the governor's emergency proclamation, or based on other triggers as defined in the SEOC Standard Operating Procedures (SOP). At that point, the significant cyber incident will be monitored and coordinated through the SEOC under the guidance of the Unified Coordination Group (UCG). The governor may proclaim a state of emergency under RCW 43.06.010(12) and/or order the National Guard into active state service under RCW 38.08.040 in response to the incident.

Situation Overview

State government, public and private industries, and critical infrastructure sectors in Washington depend on information technology (IT) and operations technology (OT) systems to deliver an array of critical functions. IT systems process and store vast amounts of data, some of which contain confidential data or Personally Identifiable Information (PII). They are critical to our daily lives and facilitate almost all services and economic activity across the state's broad spectrum of industries and government functions. OT systems are the backbone of our state's critical infrastructure systems. They facilitate around-the-clock operations of facilities that provide power, water, communications, and transportation.

According to the Federal Bureau of Investigation (FBI), Internet Crime Report (2023), Washington State had 14,600 reported victims of cybercrime in 2023, which places Washington tenth in the United States for the number of victims of reported cybercrime with a total victim financial loss of $288,691,091.

Because cyber criminals have different preferences on the type of attack that best achieves their objectives, the nature of the impacts can vary widely to include destruction of physical infrastructure, disruption to critical services, economic harm, and loss of life. In addition, attackers sometimes adjust their plans before and even during an incident. The reciprocal feedback aspects of cyber incidents, in which the attackers learn and adapt to the defenses, present continuous challenges for prevention and protection activities.

The cyber threat landscape has continued to evolve with an increase in tracked threat groups, ransomware events, and other threat activities driven by global conflict. In addition to the proliferation of cyber criminals, the threat of state-sponsored attacks has increased. U.S. critical infrastructure, government functions, and elections' infrastructure remain a target for adversaries who wish to damage the economy, degrade or impair critical infrastructure function, and/or disrupt elections.

It is also possible that error or unintended action may result in significant cyber incidents.

Incident Types

The following is a non-exhaustive list of cyber incidents that could affect the above critical infrastructure systems within Washington State: hardware destruction or loss; network unavailability, compromise, degradation, or destruction; software malfunction, compromise, or exploitation. These can be further divided into non-malicious and malicious incidents as determined by the affected entity (see the Concept of Operations section for further information).

While this Significant Cyber Incident Response Plan is designed for significant cyber incidents or attacks, the same response measures can be applied in support of any cyber related incidents stemming from or occurring in concert with the 17 hazards outlined in the Washington State Enhanced Hazard Mitigation Plan (SEHMP), which include avalanche, drought, earthquake, extreme weather, flood, landslide, tsunami, volcano, wildfire, dam failures, disease outbreak (including pandemic and endemic), hazardous material, radiological incident, and terrorist attack.

Non-Malicious Incidents

Non-malicious cyber incidents happen for numerous reasons and can include the following:

- Human error
- Structural failures
- Natural disasters

Malicious Incidents

Malicious actors attempt to compromise the availability, integrity, or confidentiality of computers, networks, or information. These incidents can include, but are not limited to, the following types of attacks:

- Phishing campaigns
- Business email compromise
- Ransomware
- Denial-of-Service
- Man-in-the-Middle
- SQL injections
- Cross-site scripting
- Zero-day exploits
- DNS spoofing
- Supply chain attacks

Planning Assumptions

Emergency Management Planning Environment: This plan assumes the presence of a broader CEMP that provides a higher-level framework for response structures and priorities for the state.

Persistent Threat Landscape: This plan assumes a continuously evolving and persistent cyber threat landscape, with threat actors employing sophisticated tactics, techniques, and procedures (TTPs) to compromise systems, networks, and data.

Interconnected Dependencies: This plan assumes a high degree of interconnectedness among critical infrastructure sectors, government agencies, and private sector entities. A cyber incident affecting one sector may have cascading effects, necessitating a coordinated and collaborative response.

Public and Private Sector Collaboration Imperative: The planning assumes a critical need for collaboration and information sharing between public and private sectors. The plan recognizes the complementary roles of government agencies, industry partners, and critical infrastructure operators in a unified response effort.

Regulatory and Legal Considerations: The planning acknowledges the regulatory and legal landscape surrounding cyber incidents, including reporting requirements, data protection laws, and jurisdictional considerations. Response measures will align with applicable laws and regulations.

Vertical Integration

This plan is designed to align vertically with federal response structures at the national and regional level, and county and city plans at the local level.

Federal Integration

Per the National Response Framework, response coordination with the federal government will occur through the FEMA Region 10 Regional Response Coordination Center (RRCC). In addition to this coordination mechanism, the unique situation of a significant cyber incident may include coordination with the following federal response structures, as outlined in the National Cyber Incident Response Plan:

- National Cyber Investigative Joint Task Force (NCIJTF). The FBI serves as the lead federal entity for the NCIJTF that coordinates federal threat response to a significant cyber incident. Threat

response activities include resources and capabilities from across the law enforcement and defense communities to investigate, analyze, and interdict threat actors. Initial coordination with the NCIJTF would occur through the FBI field office in Seattle.

- Cybersecurity and Infrastructure Security Agency (CISA) Central Hub. As an operational element of the Department of Homeland Security (DHS), CISA Central is the primary platform to coordinate the federal government's asset response to cyber incidents. Asset response activities include providing technical assistance to affected entities and mitigating vulnerabilities. Initial coordination with CISA Central would occur through the CISA Region 10 Cyber Security Advisors who serve Washington State.

Local Integration

Local government cybersecurity incident response structures and capabilities vary. In general, the state will coordinate with county and city Emergency Operations Centers (EOC). Additional coordination may occur depending on the nature of the incident and the entities that have been compromised.

Horizontal Integration

This plan is a state-level, interagency plan that provides direction to state government entities responsible for responding to a significant cyber incident and its potential consequences to physical infrastructure following a disaster. Horizontal integration in the context of a cyber response plan for an emergency management agency refers to the coordination and collaboration among various state agencies at the same level of government to effectively respond to a cyber incident.

State Emergency Operations Center (SEOC)

The SEOC is the primary platform for coordinating operational response activities including incident prioritization, critical resource allocation, and situational awareness for issues arising due to a significant cyber incident. This coordination includes communicating significant cyber incident related situational awareness and activities to SEOC partners, the Governor's office, private sector partners, and local, tribal and federal coordination centers. The SEOC maintains the capability to physically or virtually add additional federal, state, local, tribal, territorial, and private sector partners, including international stakeholders as appropriate, to the coordinated SEOC effort. Affected partners, and those that can contribute to the response effort and risk mitigation activities, can be physically co-located and virtually connected to coordinate significant cyber incident response efforts with the SEOC.

Security Operations Center (SOC) Coordination and Data Sharing

Any organization affected by a cyber incident will coordinate their respective SOCs in response to said incident. Due to the sensitive and technical nature of networked systems, specific information that pertains to threat intelligence and/or impacts to critical systems may not be shared broadly with the overall state response structure—information security procedures such as Protected Critical Infrastructure Information (PCII) should be observed when communicating sensitive information during an incident that impacts critical infrastructure systems. (For further information see Information Security section below.) Representatives from SOCs that oversee response efforts to impacted systems should coordinate with each other to the maximum extent possible to share information about the threats

observed and actions being taken to contain and eradicate without further compromising their operations.

State Network Cyber Incident Response

As defined by RCW 43.105.450, the criteria for a state cyber incident also includes incidents that affect multiple agencies, impact over 10,000 citizens, involve a nation-state actor, or are likely to severely impact the public domain. The WaTech Office of Cybersecurity (OCS) will take responsibility for coordinating cyber incident response directly related to state and local network incidents that do not necessarily affect critical physical infrastructure that Washingtonians depend on (e.g., wastewater treatment).

OCS has established an Enterprise Incident Response Plan (EIRP) that provides a framework and procedures for state agencies to use to identify, respond to, and recover from cybersecurity threats and incidents.

Tribal Government Integration

Tribal government cybersecurity incident response structures and capabilities vary. If tribes choose, they can coordinate government-to-government with the state. The level of integration and coordination between the state and the involved tribe(s) depends on the nature of the incident, the entities compromised, and the level of support desired by the tribe(s). Tribal governments may also choose not to coordinate with the state in any capacity during a significant cyber incident.

Concept of Operations

As with any disaster, the SEOC provides a central point for managing the response, facilitating resource requests, coordinating with local, tribal, and federal governments, and coordinating a Joint Information System (JIS) to ensure unified messaging. Participation in SEOC operations can occur physically (on-site) and/or virtually, depending on the nature of the incident and the requirements to meet the response goals. During a significant cyber incident, the SEOC will coordinate the state's response efforts and act as a conduit between the affected entity or entities and the federal government. The SEOC will be primarily concerned with:

- Identifying and responding to any physical consequences resulting from the cyber incident;
- Coordinating information sharing and threat intelligence between impacted entities and the federal government;
- Facilitating resource requests and fulfillment to affected entities; and
- Centralizing and disseminating information through a JIS.

This plan provides specific considerations for coordinating a state response to cyber threats and incidents affecting organizations, infrastructure, and individuals within the state of Washington. It does not replace, replicate, or supersede the broader all-hazards approach to structuring a state response but does provide state leadership and responding organizations with hazard-specific information to effectively respond to cyber incidents within the emergency management context.

Governor's Emergency Proclamation

Cybersecurity incidents that necessitate a governor's proclamation will follow the applicable processes, policies, and laws governing an emergency proclamation, as detailed in the Washington State Response Plan. Initial activation and the organizational structure for the SEOC will follow the guidance provided by the state's Response Plan.

Requesting a Presidential Disaster Declaration and Damage Assessments

Consistent with other hazards, the process for requesting a Presidential Disaster Declaration and supporting damage assessments follows the process outlined in the Washington State Response Plan. While the impacts from a significant cyber incident may produce unique damages, including reputational, financial, physical, and supply chain disruption, the damage assessment process remains consistent with all hazards.

Cyber Incident Severity Schema and SEOC Activation

Examples of significant cyber incidents that may trigger state-level coordination are those that pose an imminent threat to the provision of wide-scale critical infrastructure services, government stability, or lives of residents; or those that are likely to create significant impacts to public health or safety, national security, economic security, foreign relations, or civil liberties. The severity of an incident may depend largely on scope and scale of the incident and the potential for cascading impacts into other infrastructure sectors or government functions. While there isn't an absolute definition for when an emergency proclamation should be issued or when the SEOC should be activated, the following table provides decision makers with considerations for the state's initial response level. This severity schema was adopted from the National Cyber Incident Response Plan. Note that the SEOC may move to a different activation level due to complexity and other effects depending on the needs necessitated by the situation, especially if the cyber incident is occurring simultaneously to, as a result of, or in concert with another incident.

Description	SEOC Activation Level	Cyber Incident Severity	General Definition
Due to its severity, size, location, actual or potential impact on public health, welfare, and infrastructure, it requires an extreme amount of federal and state assistance for response and recovery efforts for which the capabilities to support do not exist at any level of government.	Level 1	Level 5 – Emergency	*Poses an imminent threat* to the provision of wide-scale critical infrastructure services, government stability, or lives of residents.
Requires elevated coordination among federal, state, local and tribal governments due to	Level 2	Level 4 – Severe	*Likely to result in a significant impact* to public health or safety, national security, economic

moderate levels and breadth of damage. Significant involvement of state agencies.			security, foreign relations, or civil liberties.
		Level 3 – High	*Likely to result in a demonstrable impact* to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Requires coordination among federal, state, local and tribal governments due to minor to average levels and breadth of damage. Typically, this is primarily a recovery effort with minimal response requirements.	Level 3	Level 2 – Medium	*May impact* public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
		Level 1 – Low	*Unlikely to impact* public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
No event or incident anticipated. This includes routine watch and warning activities.		Level 0 - Baseline	Unsubstantiated or inconsequential event.

Organization During a Significant Cyber Incident

Given the unique nature of cyber incidents, the SEOC should consider which organizations and individuals that would not normally participate in SEOC activations for other hazards need to participate in the response to a cyber incident. These considerations include:

Policy Group and Unified Coordination Group (UCG)

The Emergency Management Division will establish a Policy Group and a Unified Coordination Group (UCG) following the guidelines outlined in the Washington State Response Plan. In the case of a significant cyber incident, additional entities may need to be included in these groups. This may involve representation from state agencies affected by the incident, especially those responsible for critical infrastructure or maintaining separate network infrastructures. Furthermore, agencies leading coordination efforts with critical infrastructure sectors should have representation in the UCG when incidents affect organizations within those sectors. The expertise and coordination role of these agencies may be integrated at all appropriate levels of SEOC operation to ensure the utilization of pertinent subject matter expertise. (Refer to the CEMP and associated annexes, including the Washington State Response Plan, for authorities governing the UCG.)

Sector-Specific Agencies for Coordinating Response Activities by Critical Infrastructure Sector

A significant cyber incident can impact a wide range of critical infrastructure and government functions. Given the breadth of the potential impacted parties, several state agencies are identified as sector-specific lead agencies for critical infrastructure sectors. These agencies will provide a leading role in the state's response structure based on which sectors are experiencing impacts from the incident.

State Agency	Sector Coordination
Department of Agriculture	Agriculture and Food Production
Department of Commerce	Energy
Department of Health	Water/Wastewater
Department of Health	Healthcare and Public Health
Office of the Superintendent of Public Instruction	K-12 Schools
Washington Secretary of State's Office	Elections
Washington State Patrol	Law Enforcement Agencies
WaTech	State Agency Information Technology Networks

SEOC Command and General Staff

Staffing at the command and general staff level will follow standard SEOC procedures. If the conditions of the cyber incident require expertise from different government functions not normally represented in the SEOC (e.g., information technology or operational technology specialists), then state agencies should consider staffing the SEOC accordingly.

Direction, Control, and Coordination

Responding to a significant cyber incident involves a timely, coordinated effort across state government to contain and eradicate the threat, prioritize resources and assistance, minimize the impacts, and ensure a swift recovery. Following a Governor's Emergency Proclamation, the Emergency Management Division will partially or fully activate the SEOC to coordinate and manage the response efforts. The SEOC provides a central location for state agencies to coordinate the state's response with federal, tribal, local, and private sector organizations that may be impacted by the incident or are contributing to response operations.

Lines of Authority

Lines of authority for the SEOC remain consistent with the state's CEMP, however the unique circumstances of a significant cyber incident will necessitate coordination across concurrent lines of authority. SEOC lines of authority will apply to the overall state response, working to organize information and activities across jurisdictions in the public sector and with private sector partners. But this authority may not apply to the individual actions taken by impacted organizations that are working to contain and eradicate threats to their respective networks and infrastructure.

Affected Entity Authority

When a specific organization is directly impacted by a cyber incident, that organization will have primary responsibility for their response activities. This is true when considering all levels of government and private sector entities. While this responsibility is absolute, affected entities should work to coordinate their respective response activities collectively, sharing information and coordinating actions to the maximum extent possible. This is especially true following significant incidents where numerous systems and organizations may be impacted. Reporting requirements for affected entities are crucial in this regard, as they vary depending on the nature of the incident, the sector, and the regulatory environment. Each entity must understand its unique obligations and procedures, ensuring timely and

accurate information dissemination to relevant stakeholders, regulatory bodies, and other affected parties.

Coordinating with the Private Sector

Depending on the impacts of a significant cyber incident, private sector organizations may be directly impacted. Private corporations that own/operate critical infrastructure, employ a significant number of Washington residents, and/or are important contributors to the state's economy are recognized as crucial partners during any emergency response. In the event these organizations are directly impacted by a significant cyber incident, the state will coordinate response activities with impacted private sector entities to:

- Coordinate efforts to contain and eradicate threats;
- Align response priorities; and
- Share information and resources.

This coordination may occur either virtually or physically at the UCG level, through the relevant Emergency Support Function (ESF), within the state's Business Emergency Operations Center (BEOC), or through a partner state or federal agency with a direct relationship with the affected business.

Threat Intelligence

This plan emphasizes a proactive approach to cybersecurity which includes identifying potential cyber threats, vulnerabilities, and the possible impact on emergency management functions. Regular updates to these assessments will inform ongoing improvements to cyber response strategies. Additionally, the Cyber Intelligence Network (CIN), Washington State Fusion Center (WSFC), and Multi-State Information Sharing and Analysis Center (MS-ISAC) will be used to coordinate and share intelligence on potential cyber threats and vulnerabilities through various ESFs and SEOC positions that are actively engaged in and receiving updates from these entities at all times.

Cyber Intelligence Network (CIN)

The CIN is an association of cyber analysts across the country dedicated to responding to cyber incidents, sharing cyber intelligence, and producing analytic products on cyber threats. CIN's mission is to support the free and rapid exchange of cyber intelligence. Through the CIN, cyber analysts at various state agencies and organizations: (1) share information rapidly, (2) coordinate and prevent the duplication of efforts, and (3) connect with each other, so analysts know who their counterparts are nationwide and can rely on them when needed.

Washington State Fusion Center (WSFC)

The fusion centers are owned and operated by state and local entities with support from federal partners in the form of deployed personnel, training, technical assistance, exercise support, security clearances, and connectivity to federal systems. A fusion center plays a crucial role in cyber threat and risk assessment by serving as a centralized hub for collecting, analyzing, and disseminating information related to cybersecurity. These centers are typically collaborative efforts that bring together experts from various government agencies, law enforcement, and private sector organizations. The primary goal is to enhance situational awareness, facilitate information sharing, and improve the overall

cybersecurity posture of organizations. The WSFC provides information and updates on cybersecurity and potential threats through ESF 13 – Public Safety, Law Enforcement, and Security.

Multi-State Information Sharing and Analysis Center (MS-ISAC)

The MS-ISAC is a voluntary and collaborative effort designated by DHS as the key resource for cyber threat prevention, protection, response, and recovery for the nation's state, local, tribal, and territorial (SLTT) governments. ESF 14 – Cross-Sector Business and Infrastructure and the SEOC Situation Unit Leader monitor information shared through MS-ISAC.

Information Security

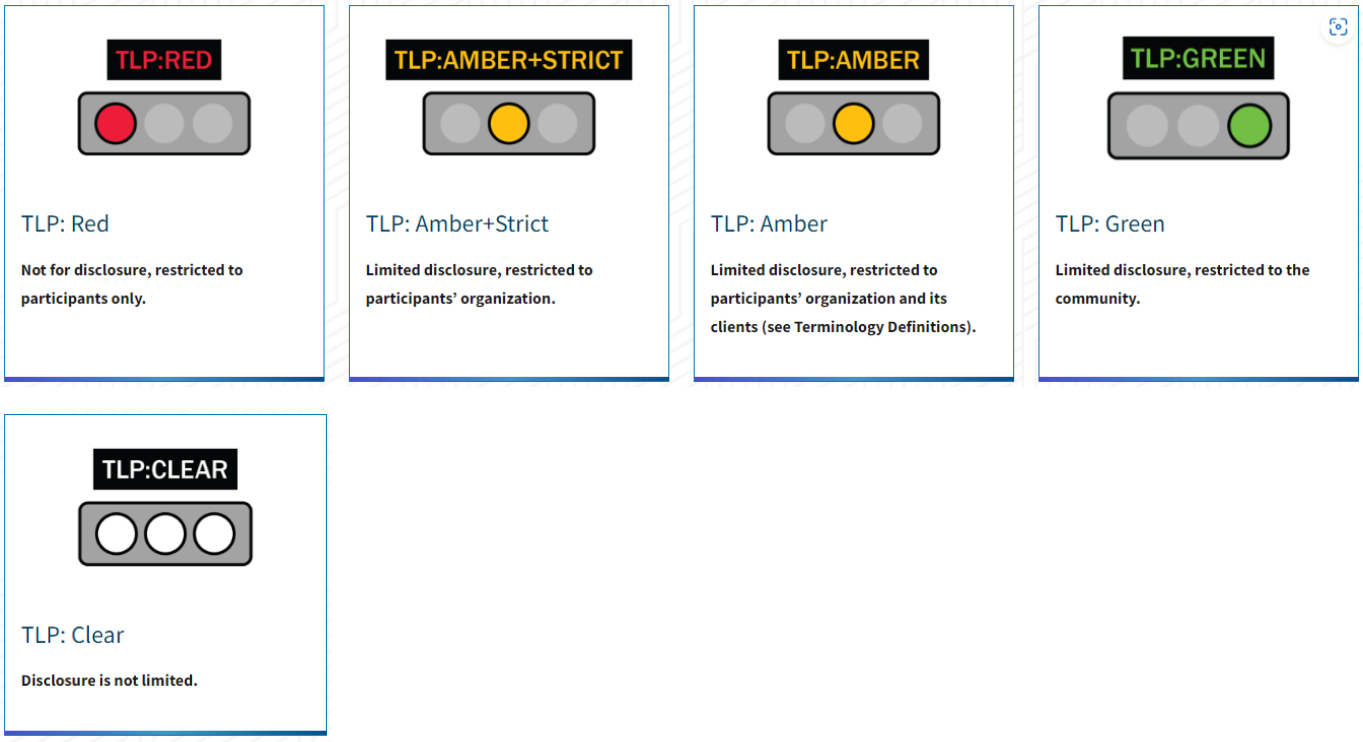
Given the complex nature of cybersecurity incidents, the handling of sensitive information will follow standards and protocols that indicate when and how sensitive information can be shared. To ensure information security before, during, and after a significant cyber incident, all individuals and organizations involved in a state response will adhere to the security guidance set forth by the EOC Supervisor, sector-specific agency leading a response, or the incident commander of an affected entity. The SEOC SOPs contain general guidance for marking, storing, and transmitting information during a response. Information security precautions that are event specific will be captured in the Incident Action Plan (IAP). This guidance may vary based on the nature of the incident, but the following categories serve as guiding principles for securing information and communications during a significant cyber incident.

Washington State Information Sharing Data Categories

Under the WaTech policy SEC-01 – Securing Information Technology Assets (formerly OCIO 141.10), state agencies must classify data into categories based on the sensitivity of the data. During a response to a significant cyber incident, responding state agencies must ensure that storing and sharing data complies with this policy, and when sharing Category 3 or higher data outside an agency, an agreement must be in place. To review these categories, visit the WaTech website.

Traffic Light Protocol (TLP)

The TLP was created to designate sensitive information and facilitate appropriate sharing and dissemination of information. The TLP designations indicate when and how sensitive information can be shared. TLP designations do not have any effect on freedom of information or the Washington State Public Records Act (RCW 42.56). Therefore, additional data classification will be necessary for PCII and other sensitive data. To review TLP guidance, visit the TLP website.



Protected Critical Infrastructure Information (PCII) Program

The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) administer the PCII Program. The PCII Program allows for secure sharing of sensitive infrastructure data and prohibits the unauthorized sharing of that data by requiring the redaction of PCII-designated information from public records requests. The program requires training by all individuals who handle and transmit information and documents marked as PCII. To review PCII program requirements and guidance, visit the CISA PCII website.

Federally Classified Information

Federally classified information will be handled in accordance with their security requirements. State agency employees who have obtained a federal security clearance from a sponsoring federal entity will be vetted through existing federal processes. It is recommended that anyone who maintains a federal security clearance that originates from a federal department other than the Department of Defense seek reciprocity with the Department of Defense's security clearance system. The SEOC maintains a facility for storing classified information up to SECRET. National Guard facilities located on Camp Murray, adjacent to the SEOC, are available for accommodating access to classified networks, discussions at the classified level, and Secure Video Teleconferencing.

Procedures for Using Non-Sensitive Information in Coordinating Cyber Incident Response Operations

It is crucial to establish clear procedures for how the SEOC, UCG, and Policy Group should utilize non-sensitive information to manage the consequences of a significant cyber incident. This includes:

1. Information Sharing: Ensure timely dissemination of non-sensitive information to all relevant stakeholders, including public and private sector partners, to facilitate coordinate response efforts.

2. Operational Coordination: Use non-sensitive information to align and synchronize the action of the SEOC, UCG, and Policy Group with on-the-ground response activities, ensuring a unified approach to incident management.
3. Situational Awareness: Maintain a common operating picture by continuously updating all groups with the latest non-sensitive information about the incident's status, impacts, and response progress.
4. Emergency Public Information: Develop and distribute clear, accurate, and consistent public messages using non-sensitive information to inform and guide the public, helping to mitigate panic, and provide instructions for safety.
5. Resource Allocation: Utilize non-sensitive information to prioritize and allocate resources effectively, ensuring that the most critical needs are addressed promptly.
6. Interagency Collaboration: Foster partnerships among various agencies by sharing non-sensitive information that can help identify collaborative opportunities and avoid duplication of efforts.

By following these procedures, the SEOC, UCG, and Policy Group can ensure an effective and coordinated response to significant cyber incidents, enhancing overall incident management and public communication.

Alignment with the National Preparedness Goal

In the National Preparedness Goal, FEMA lays out 32 core capabilities that constitute a comprehensive emergency management capability. Given the specific focus of responding to a significant cyber incident, the following list of core capabilities are addressed by this plan.

Cybersecurity

Description: Protect (and, if needed, restore) electronic communications systems, information, and services from damage, unauthorized use, and exploitation.

In the context of this response plan, this capability encompasses the overall goal of responding to a significant cyber incident by restoring key information technology systems and coordinating across local, tribal, state, and federal governments to avoid cascading impacts from an incident.

Planning

Description: Conduct a systematic process engaging the whole community as appropriate in the development of executable strategic, operational, and/or tactical-level approaches to meet defined objectives.

This plan serves as the roadmap for state activation to a significant cyber incident. Following the general structures and processes documented in the CEMP, the Planning core capability facilitates a coordinated and effective response to cyber incidents of significance. It encompasses the strategic orchestration of resources, personnel, and strategies aimed at restoring critical information technology systems while mitigating potential cascading impacts. Through meticulous planning and coordination efforts across various levels of government—local, tribal, state, and federal—this capability ensures a unified response framework capable of addressing the evolving challenges posed by cyber threats.

Operational Coordination

Description: Establish and maintain a unified and coordinated operational structure and process that appropriately integrates all critical stakeholders and supports the execution of Core Capabilities.

In the context of this plan, the Operational Coordination core capability focuses on orchestrating a cohesive and efficient response to significant cyber incidents. Its primary objective is to swiftly restore critical information technology systems and operational technology networks while facilitating seamless coordination among local, tribal, state, and federal entities. This capability aims to mitigate the potential cascading impacts of cyber incidents, ensuring unified and effective response to emerging threats in the digital landscape.

Infrastructure Systems

Description: Stabilize critical infrastructure functions, minimize health and safety threats, and efficiently restore and revitalize systems and services to support a viable, resilient community.

Modern critical infrastructure systems are reliant upon IT and OT systems and assets to function. In the context of a significant cyber incident, these IT and OT assets must be secured and recovered rapidly to ensure the threat is eradicated and normal operations resume. The primary objective is to prevent the escalation of disruptions and avert the cascading impacts that could reverberate across interconnected systems.

Washington State Agency Roles and Responsibilities

The possibility of a significant cyber incident occurring within the state of Washington is an ever-present threat, and effective planning and coordination activities that support unity of effort across the whole state government are essential. Cybersecurity and the ability to respond to cyber incidents are not the responsibility of any single office and require collaboration across multiple state agencies.

Office of the Governor (GOV)

In accordance with RCW 38.52.030(2) and (3) and RCW 38.52.050, the governor provides overall direction and control for the preparation and carrying out of all emergency actions authorized under chapter 38.52 RCW, the Emergency Management Act, including development and carrying out of the state's comprehensive emergency management program. This includes preparation for and carrying out all emergency functions to mitigate, prepare for, respond to, and recover from emergencies and disasters from all hazards, whether natural, technological, or human caused, resulting from an event or set of circumstances that either (1) demand immediate action to preserve public health, protect life and public property, or to provide relief to any stricken community overtaken by such occurrences, or (2) have resulted in the governor proclaiming a state of emergency pursuant to RCW 43.06.010(12).

Under RCW 38.08.040, the governor is also authorized to activate the National Guard to perform such duty as deemed proper in the event of a public disaster; when required for public health, safety or welfare; or to prepare for or recover from such events.

Washington Military Department (MIL)

Homeland Security Advisor (HSA)

The Adjutant General (TAG) of the Washington Military Department serves on the governor's cabinet and is the governor's Homeland Security Advisor (HSA). The HSA has responsibility for coordinating significant cyber incident related activities for the state of Washington.

Emergency Management Division (EMD)

The Director of EMD ensures the state is prepared to deal with any disaster or emergency by administering the program for emergency management delineated by the HSA. The EMD Director is also responsible for coordinating the state's response in any disaster or emergency.

EMD has established the Emergency Communications Unit, which includes both the Enhanced 9-1-1 (E911) section and the Infrastructure & Industry section (I&I). These sections and their functions are described below.

The E911 Program facilitates local planning and installation of cyber systems to ensure the E911 system is operational and available. The State E911 Coordination Office maintains an overarching enterprise Incident Response Plan (IRP) for working with and supporting public safety answering points (PSAP) experiencing E911 outages. All jurisdictions and PSAPs must also create and maintain local IRPs for this unique system.

The I&I section is tasked with maintaining the state's cybersecurity response plans and facilitating the state's response to a significant cyber incident by providing the SEOC with subject matter expertise.

Joint Staff, Cyber Plans and Operations (J36)

In the event of a significant cyber incident, the governor may direct the National Guard into state active service under RCW 38.08.040 to perform incident response actions to support the defense of both public and/or private state entities' cyber infrastructure. An entity may also request support without an emergency proclamation. This support is most likely to be met through a Mission Element (ME) which is a joint team composed of cybersecurity experts from within the 252nd Cyber Operations Group of the Washington Air National Guard, the Army Defensive Cyber Operations Element (DCOE) and/or the Washington State Guard (WSG) when availability allows. More details about these forces are captured in the Washington National Guard Joint Contingency Plan 23-01, Defensive Cyber Operations.

Washington Technology Solutions (WaTech)

WaTech is Washington State's information technology agency. It is led by the state's Chief Information Officer who is part of the governor's cabinet. Located within WaTech, OCS has the responsibility to respond to any cyber incident that impacts the information systems, data, and assets attached to networks within Washington State, owned or operated by state agencies or by third parties on behalf of the state of Washington. This authority applies to employees, contractors, and third-party partners who have access to department IT systems, data, equipment, or infrastructure. These responsibilities and the procedures for responding are captured in the Enterprise IRP.

In accordance with this plan, OCS operates the Washington SOC which leads the coordination and response efforts in assessing and managing cyber incidents affecting the state government networks. The SOC determines the level of response required to respond to incidents and directs the utilization of agency resources to minimize incident exposure. The SOC team is comprised of certified experts in incident handling, forensics, and penetration testing. The SOC ensures appropriate enterprise protection controls are deployed; communicates information regarding the incident to organizational partners; and keeps executive leadership informed. If a state entity does not have internal resources to respond to an incident, the SOC will handle the incident on behalf of the entity.

Washington State Fusion Center (WSFC)

During a significant cyber incident, the WSFC is in a unique position to facilitate information sharing using Homeland Security Information Network (HSIN) cyber security alerts. HSIN is a national secure and trusted web-based portal for information sharing and collaboration. During the incident, the WSFC will generate cyber alerts to notify federal, state, regional, local, tribal, and private sector partners with early warning indicators and potential actionable intelligence measures. Further, the WSFC is positioned to complement the notifications and updates coming out of the SEOC's UCG, CISA Central, and Seattle FBI Joint Cyber Task Force, as well as to communicate and collaborate with the SEOC and WSFC cyber stakeholders. In addition, the WSFC engages with other national homeland security fusion center cyber programs through the CIN (an outreach network of public security, information security and intelligence community professionals) to augment the SEOC common situational awareness of a significant cyber incident.

Washington State Patrol (WSP)

The WSP routinely partners with other law enforcement, traffic safety, and criminal justice agencies to provide public safety services to the citizens of Washington State. WSP has the responsibility to investigate cybercrimes committed on state property, against state agencies, and against state assets. The High-Tech Crimes Unit (HTCU) is a full-time computer forensics team within the WSP responsible for the investigation of these crimes. The unit may also investigate cybercrimes in local jurisdictions at the request of a local law enforcement agency.

Due to the pervasive nature of cyberspace, criminal activities can cross multiple law enforcement jurisdictions complicating efforts to investigate and prosecute cybercrimes. During a significant cyber incident, WSP will coordinate the initiation of cybercrime investigations with appropriate state and local law enforcement agencies and support from our federal partners. HTCU will ensure the UCG and SEOC are aware of which law enforcement agencies are engaged.

Attorney General's Office (AGO)

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. The AGO has limited jurisdiction to prosecute internet crime and defers to the FBI's Internet Crime Complaint Center (IC3) as a central reception for reporting cybercrime. Through RCW 19.255 and RCW 42.56.590, the AGO requires

businesses and public agencies to report data breaches that impact the personal information of Washington residents.

Washington State Secretary of State's Office (S0S)

As the government agency tasked with administering elections in the state of Washington, the Secretary of State's Office is the lead agency for securing election networks and responding to cybersecurity incidents that impact election infrastructure.

Washington State Department of Commerce (COM)

The Department of Commerce's Energy Resilience and Emergency Management Office (EREMO) is committed to providing comprehensive emergency management, resilience development, and cybersecurity services for the energy sector and residents of Washington State. EREMO's mission is to coordinate with stakeholders at all levels of government, as well as with electric, natural gas, petroleum, and renewable energy industries statewide, to develop planning documents, standards, trainings, and operational support during emergencies. As leaders in energy resilience and emergency management, EREMO envisions supporting communities' capacity to adapt to hazards, including cyber incidents, and climate change through whole community planning, mitigation, and resilience initiatives.

Washington State Department of Health (DOH)

The Washington State Department of Health (DOH) plays a crucial role in safeguarding public health by focusing on water safety and cybersecurity in the water sector. Owned by DOH, the water considerations involve addressing larger scale issues that require state resources, including the involvement of criminal elements. In such instances, DOH provides technical assistance to ensure the continued provision of safe drinking water, coordinating with federal partners as necessary. When alternative water supplies are needed, DOH assists and takes responsibility for communicating the status of the water systems to EMD, considering regional impacts like firefighting needs and requirements. Additionally, the department addresses health and safety issues related to other critical water-dependent infrastructures such as nuclear cooling at Hanford and dams for irrigation and electricity, which are managed by local utilities and cities. Moreover, cybersecurity concerns encompass not just operational technology but also secondary considerations like breaches of customer or employer data, requiring proper notifications and ensuring health advisories are effectively communicated.

In the healthcare sector, DOH emphasizes the importance of cybersecurity across various facets to enhance patient safety and healthcare service integrity. Priorities include maintaining the operational integrity of telemetry and transport systems, ensuring air traffic coordination for patient transfer, monitoring hospital bed status, and managing automated medical processes including charting and pharmacy operations. The DOH also takes the lead in helping hospitals prioritize needs in surgical suites and ICUs, which are susceptible to cybersecurity risks due to their automated nature. Furthermore, the cleaning of medical supplies, billing, and coding processes, particularly in smaller critical access hospitals, are areas where DOH is developing programs to enhance cyber resilience. The department also focuses on ensuring the integrity of electronic medical records, pharmaceutical data protection, and effective response to ransomware attacks. By collaborating with healthcare facilities, DOH aims to get a clear

status of the industry's needs and help in developing robust cyber defenses, ensuring that transfer points, critical access hospitals, and patient transport are secure and efficient.

Roles & Responsibilities by Core Capability

Core Capability	Activity/Action	Organization(s) Name
Cybersecurity	Lead response to cybersecurity incident impacting state networks, applications, and assets.	WaTech
Cybersecurity	Lead response to cybersecurity incident impacting election infrastructure.	SOS
Cybersecurity	Activate and coordinate State Guard and National Guard cybersecurity response resources to conduct technical and investigative countermeasures, mitigations, and operations against cyber threats.	MIL
Cybersecurity	Facilitate information sharing during a significant cyber incident through cyber alerts to the appropriate federal, state, regional, tribal, local, and private sector partners.	WSFC
Cybersecurity	Coordinate the investigation of cybercrimes committed on state property and/or against state agencies and assets with the appropriate state and local law enforcement.	WSP
Planning	Coordinating state planning for significant cyber incidents, including maintaining the response and prevention annexes for the state CEMP that encompass state agency activities and programs related to cybersecurity.	MIL
Planning	Develop and maintain an Incident Response Plan for state network infrastructure and enterprise applications.	WaTech
Planning	Produce Incident Response Plan templates for local governments to bolster their cybersecurity posture.	MIL
Planning	Maintain and execute the state's Energy Emergency Plan and Fuel Action Plan.	COM
Operational Coordination	Provide overall direction and control for emergency actions carried out by the state.	GOV
Infrastructure Systems	Maintain integrity of state networks, applications, and assets.	WaTech
Infrastructure Systems	Maintain integrity of election networks, applications, and assets.	SOS
Infrastructure Systems	Lead response to cybersecurity incident impacting state highways and the ferry system through ESF 1.	WSDOT
Infrastructure Systems	Lead response to cybersecurity incident impacting communications infrastructure through ESF 2.	MIL
Infrastructure Systems	Coordinate state response efforts to cybersecurity incidents impacting state energy systems through the ESF 12.	COM
Infrastructure Systems	Coordinate state response efforts to cybersecurity incidents impacting K-20 education infrastructure.	OSPI

Infrastructure Systems	Coordinate state response efforts to cybersecurity incidents impacting election infrastructure.	SOS
Infrastructure Systems	Coordinate state response efforts to cybersecurity incidents impacting water/wastewater infrastructure through ESF 3.	DOH
Infrastructure Systems	Coordinate state response efforts to cybersecurity incidents impacting healthcare infrastructure through ESF 8.	DOH

Attachment 1: Authorities and Policies

State

RCW 43.105.450: WaTech & OCIO

Establishes Chief Information Security Officer and Consolidates Services Agency, which serves Washington State agencies by providing information technology services such as protecting and managing sensitive data, and ensuring all agencies have dependable technology resources. Mandates the responsibility to detect and respond to security incidents consistent with information security standards and policies.

RCW 38.52: Emergency Management

Authorizes the state military department to administer an emergency management program through the promulgation of written plans and the staffing of the State Emergency Operations Center in coordination with primary responding state agencies involved in an incident.

RCW 43.21F.045: State Energy Office

Authorizes the State Energy Office to prepare and update contingency plans for securing energy infrastructure against all physical and cybersecurity threats, and for implementation in the event of energy shortages or emergencies.

RCW 43.21F.060: State Energy Office

Establishes the ability to obtain necessary information from energy suppliers and ensure confidentiality and protection from public disclosure.

RCW 43.21G: Energy Supply Emergencies, Alerts

Defines Energy Supply Alert and Energy Emergencies. Establishes Governor's Energy Emergency Powers. Provides priority guidance for the allocation of energy during an energy emergency.

WAC 118-30: Local Emergency Management Organizations, Plans, and Programs

Establishes criteria for evaluating local emergency management organizations, plans, and programs to ensure consistency with the state comprehensive emergency management plans and programs.

WAC 182-70-430: Data Retention

Ensures a clear date retention policy that protects infrastructure assets by allowing periodic penetration tests to identify vulnerabilities and align with industry cybersecurity standards.

WAC 194-14: Emergency Petroleum Allocation Act Rules

Establishes administrative procedures with respect to state orders issued under the authority granted by the Emergency Petroleum Allocation Act and appeals from such orders.

WAC 194-22: Washington State Curtailment Plan for Electric Energy

Establishes the process by which the state of Washington utilities will initiate and implement statewide electric load curtailment when there is an insufficient supply of electric energy.

WAC 480-100-505: Energy Sector

Identifies energy sector responsibilities to submit periodic reports granting the ability to send information about energy services, costs, etc.; information about energy equipment to improve the flexibility, functionality,

interoperability, cybersecurity, situational awareness, and operational efficiency of the energy transmission and distribution system.

WaTech SEC-01 (Formerly OCIO Policy 141)
Sets requirements for maintain system and network security, data integrity, and confidentiality.

WaTech SEC-12 (Formerly OCIO Policy 151)
Within Washington State government, the Military Department has overall responsibility for emergency management activities. Included as part of emergency management is the requirement that state agencies develop a Continuity of Operations Plan (COOP). It is through the COOP that agencies identify mission essential functions in order to develop disaster recovery plans for the technology necessary to deliver agency essential functions. Once developed, the disaster recovery plan(s) becomes part of the COOP. While the COOP speaks to emergencies and crisis management, routine business continuity planning ensures that essential functions are identified and can be recovered and restored in the event of service disruptions.

Federal

Homeland Security Presidential Directive 7: National Infrastructure Protection Plan
Establishes policy for federal departments and agencies to identify and protect critical infrastructure.

Infrastructure Investment and Jobs Act
Creates new authorities for the energy/nuclear, communications, transportation, drinking water/wastewater sectors.

Cyber Incident Reporting for Critical Infrastructure Act
Grants regulatory authority to the Department of Homeland Security (DHS) Cybersecurity and Critical Infrastructure Security Agency (CISA) to enforce reporting of ransomware payments during cyber incidents.

National Cyber Incident Response Plan
Provides a national framework for significant cyber incident coordination.

42 U.S.C 6323(e)(1). Energy Policy and Conservation Act of 1975
Each state is required to submit an energy emergency plan that it will utilize in the case of an energy supply disruption.

Energy Infrastructure Act of 2021
Updates the requirements for each state to develop and submit State Energy Security Plans for natural, physical (human-caused), equipment failure, and cybersecurity incidents.

Presidential Policy Directive 7
Establishes a national policy to identify and prioritize critical infrastructure and to protect them from terrorist attacks.

Presidential Policy Directive 8
National preparedness strengthens the security and resilience of the U.S. through systemic preparation for high-risk threats.

Presidential Policy Directive 9

Unifies the national effort to strengthen and maintain critical infrastructure.

Attachment 2: Plan Development and Maintenance

This plan was developed through planning workshops with the Interagency Cybersecurity Coordination Group:

- Washington Military Department
- Utilities and Transportation Commission
- State Auditor's Office
- Washington Technology Solutions
- The Governor's Office
- Washington State Fusion Center
- Secretary of State's Office
- Washington Office of Superintendent of Public Instruction
- Department of Financial Institutions
- Department of Commerce
- Attorney General's Office

This plan adheres to the planning maintenance schedule put forth by the CEMP. Per the CEMP, this plan will be exercised and updated at a minimum of every five years from the date of last publication.

Attachment 3: Glossary

- AGO – Attorney General's Office
- BEOC – Business Emergency Operations Center
- CEMP – Comprehensive Emergency Management Plan
- CIN – Cyber Intelligence Network
- CISA – Cybersecurity and Infrastructure Security Agency
- COM – Washington State Department of Commerce
- COOP – Continuity of Operations Plan
- DCOE – Army Defensive Cyber Operations Element
- DHS – Department of Homeland Security
- DOH – Washington State Department of Health
- E911 – Enhanced 9-1-1
- EIRP – Enterprise Incident Response Plan
- EMD – Washington State Emergency Management Division
- EOC – Emergency Operations Center
- EREMO – Energy Resilience and Emergency Management Office
- ESF – Emergency Support Function
- FBI – Federal Bureau of Investigation
- GOV – Office of the Governor
- HSA – Homeland Security Advisor
- HSIN – Homeland Security Information Network
- HTCU – High-Tech Crimes Unit
- IAP – Incident Action Plan
- IRP – Incident Response Plan
- IT – Information Technology
- J36 – Joint Staff, Cyber Plans, and Operations
- JIS – Joint Information System
- ME – Mission Element
- MIL – Washington Military Department
- MS-ISAC – Multi-State Information Sharing and Analysis Center
- NCIJTF – National Cyber Investigative Joint Task Force
- NIMS – National Incident Management System
- NRF – National Response Framework
- OCS – Office of Cybersecurity
- OSPI – Washington State Office of Superintendent of Public Instruction
- OT – Operations Technology
- PCII – Protected Critical Infrastructure Information
- PII – Personally Identifiable Information
- PSAP – Public Safety Answering Points

- RRCC – Regional Response Coordination Center
- SEHMP – State Enhanced Hazard Mitigation Plan
- SEOC – State Emergency Operations Center
- SLTT – State, Local, Tribal, and Territorial
- SOC – Security Operations Center
- SOP – Standard Operating Procedures
- SOS – Washington State Secretary of State's Office
- TAG – The Adjutant General
- TLP – Traffic Light Protocol
- TTP – Tactics, Techniques, and Procedures
- UCG – Unified Coordination Group
- WaTech – Washington Technology Solutions
- WSDOT – Washington State Department of Transportation
- WSFC – Washington State Fusion Center
- WSG – Washington State Guard
- WSP – Washington State Patrol