Washington State Cyber Incident Response Summit

September 7-8, 2022

Camp Murray, Washington

IN COORDINATION WITH:

The Adjutant General of Washington State – Major General Bret Daugherty, Washington Military Department

Cybersecurity and Infrastructure Security Agency Region 10

Pacific Northwest National Laboratory

with support from Department of Homeland Security Cybersecurity and Infrastructure Security Agency – National Risk Management Center

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor Battelle Memorial Institute, nor any of their employees, **makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights**. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof, or Battelle Memorial Institute. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

**Available to DOE and DOE contractors from
the Office of Scientific and Technical
Information,
P.O. Box 62, Oak Ridge, TN 37831-0062**
www.osti.gov
**ph: (865) 576-8401
fox: (865) 576-5728
email: reports@osti.gov**

**Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
or (703) 605-6000
email: info@ntis.gov
Online ordering: http://www.ntis.gov**

PNNL-33605

Washington State Cyber Incident Response Summit

Summary report from the September 7–8, 2022 workshop held at Camp Murray, Washington

In coordination with:
The Adjutant General of Washington State – Major General Bret Daugherty, Washington Military Department
Cybersecurity and Infrastructure Security Agency Region 10
Pacific Northwest National Laboratory
with support from Department of Homeland Security Cybersecurity and Infrastructure Security Agency – National Risk Management Center

Authored by: Ann Lesperance, Scott Godwin, Krystal Ayala, Maren Disney, Rich McLaughlin – Pacific Northwest National Laboratory

Summary

On September 7 and 8, 2022, Pacific Northwest National Laboratory and Washington State Adjutant General Major General Bret Daugherty, with support from the Department of Homeland Security Cybersecurity and Infrastructure Security Agency, hosted the Washington State Cyber Incident Response Summit at Camp Murray in Washington State. The invite-only summit convened 40 key decision makers and stakeholders from across the state to discuss strategies and pilot a collaborative approach to improve cyber incident response readiness within Washington. In small working groups, participants shared incident response lessons learned, best practices, and opportunities for improvement within the water and transportation sectors.

This report highlights the details of the workshop presentations and discussions. Key gaps identified during the event included a need for:

- Resources – staffing, funding, mutual aid, training, and subject matter expertise.
- Guidance – templates, standard operating procedures/conduct of operations, and legislature specific to each sector.
- Partnerships – public, private, industry, and across sectors.
- Information Sharing – templates, lessons learned, best practices, subject matter expertise, and easily accessible repositories.
- Training and Assessments – regularly scheduled execution of plans at various levels, including tabletop exercises and large-scale annual exercises across sectors.

Key takeaways from the summit highlighted both challenges and opportunities facing Washington State in the mission for effective cyber incident response:

- The threat is real, and the threat is growing. Cyber criminals are opportunistic, motivated by money and putting health and safety at risk.
- Misinformation can be as big of a concern as an actual cyberattack; this makes a communications plan essential.
- There is a desire for sector-specific Security Operations Centers with consistent conduct of operations, training, and reporting structures.
- Partnerships, communications plans, assessments/tabletop exercises, and structured information sharing with well-defined tiers/triggers are essential.
- Tools and resources are available to aid in response but need to be more effectively communicated. Additionally, some organizations have developed cyber incident response plans that may be used as templates for sectors in the future.

The summit emphasized a need for growing a network of partners and mutual aid to align sectors across Washington State. Recommended next steps include:

- Conduct a follow-on event and maintain communications among participants.
- Expand invitees to include other critical infrastructure sectors and organizations to provide heightened awareness of resources to fill any gaps agencies identified.
- Continue communication among sectors to help determine common areas of opportunity to provide state and federal leaders insight into high priorities for cyber incidents.

Acknowledgments

Pacific Northwest National Laboratory would like to acknowledge the people and organizations who joined in coordinating this event and helped facilitate the engagement and sharing of information, including:

- Major General Bret Daugherty, Robert Ezelle, and Alisha King from the Washington Military Department Emergency Management Division, for their support to coordinate, co-host, and facilitate this event.
- Kim Wyman, Senior Election Security Advisor from the Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA), for taking the time to attend and share valuable lessons learned and best practices with participants.
- Patrick Massey, Chris Callahan, Ian Moore, and Barrett Adams-Simmons from CISA Region 10, for their active engagement and participation on behalf of the CISA Region 10 office.
- Senior leaders from Washington State including Secretary of State Steve Hobbs, Matt Modarelli, Bill Kehoe, and Matt Boehnke, for sharing their perspectives on the need for further focus on cyber incident response in our state.
- The CISA National Risk Management Center, for their overall support of this event and this mission.
- All of the participants, for your engagement in the in-depth discussions and breakout groups, including sharing examples of cyber incident response plans and identifying gaps that need to be filled and opportunities for how we can work together in the future. Organizations are listed in Appendix A.

Acronyms and Abbreviations

CADDY	Cyber Asset Dependency Discovery
CISA	Cybersecurity and Infrastructure Security Agency
CIRCIA	Cyber Incident Reporting for Critical Infrastructure Act
DHS	Department of Homeland Security
FEMA	Federal Emergency Management Agency
ICS	Incident Command System
IT	information technology
MDM	mis-, dis-, and mal-information
NIST	National Institute of Standards and Technology
OT	operational technology
PCII	Protected Critical Infrastructure Information
PNNL	Pacific Northwest National Laboratory
SP	Special Publication
TAG	The Adjutant General

Contents

Introduction

On September 7 and 8, 2022, Pacific Northwest National Laboratory (PNNL) and The Adjutant General (TAG) for Washington State Major General Bret Daugherty, with support from the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA), hosted the Washington State Cyber Incident Response Summit at Camp Murray in Washington State. The invite-only summit convened key decision makers and stakeholders from across the state to discuss strategies and actions to improve cyber incident response readiness within Washington State, with a focus on election security, water, and transportation.

This report provides a summary of the event presentations and working group discussions followed by key takeaways and next steps for enabling more coordinated incident response to protect Washington State's critical infrastructure. The discussions outlined in this report are the opinions and perspectives of the speakers[1] as individuals and not an endorsement or representation of their organizations. The event agenda is available in Appendix B. Resources mentioned during the event are listed in Appendix C.

Objectives

- Convene key members of Washington's government leadership, emergency response managers, and private sector.
- Outline strategies and actions to improve the state's cybersecurity incident response readiness.
- Develop cyber incident response plans with state and county leaders with an initial focus on elections, transportation (rail/ports), and water.

Anticipated Outcomes

- Identification of assets and a strategy for how to work toward mutual aid and share assets.
- A standardized cyber incident response plan/template that provides a common framework, terms, and processes for states, cities, and counties.

The Washington State Cyber Incident Response Summit convened 40 decision makers and stakeholders from across the state.

Background

Across the nation, most states lack detailed cyber incident response planning at the sector-to-local county level. As a result, the few preparedness exercises performed somewhat regularly have lacked sufficient detail and role-based planning to be effective. Washington State aims to

[1] Speaker biographies

change that reality by leveraging researched international best practices to build a scalable cyber incident response template and apply it in several key sectors (elections, transportation, and water). Utilizing Washington State as a model to address cyber incident response from a holistic perspective—while aligning with the CISA's new and innovative approaches—can set an example for what could be done nationally. This will enable a model state-level program while supporting national and regional understanding of critical systems, assets, networks, and enabling technologies. Leveraging the prior activities, the summit proposed a collaborative approach between CISA Region 10, Washington State, and PNNL to create a model that can be piloted regionally then utilized by other regions to adapt and grow.

This project builds on current successes with strong potential for future integration and expansion to other states and collaborators. PNNL served as the lead and facilitator with Daugherty in developing and executing this project. This included:

- Working with Daugherty and his leadership team to scope, plan, and execute the summit to deliver actionable outcomes.
- Facilitating the identification of key infrastructures of focus, associated responsible organizations, and key participants.
- Engaging CISA Region 10 and others to leverage existing assets and prior efforts as appropriate.
- Conducting the summit and documenting discussions.
- Developing the cyber incident response documentation and this final report that summarizes the event.

Opening Remarks

Daugherty welcomed participants by sharing the vision for the two days that lay ahead. Cyber criminals are growing increasingly more advanced and are targeting critical infrastructure and other systems essential to keeping America safe. In the face of this challenge, the summit's intent was twofold: to elicit a broader understanding of the tools and resources available within Washington State and to create a better plan for how entities will work together to protect from and respond to a cyberattack against critical infrastructure.

To set the stage for discussions, Daugherty invited representatives present from across the state to share brief words of welcome. Speakers and key points included:

- Washington State Chief Information Officer Bill Kehoe noted that staying ahead of these things is very difficult—it requires daily diligence because the sophistication and the volume are extraordinary. The criticality posed by cyberattacks and the need for a proactive approach are essential to assessing and closing gaps at the state and local government levels.
- Washington State Department of Transportation Chief Information Officer Matt Modarelli underpinned the value of a whole-of-community approach to address emerging threats and shared his leadership's strategic goals based on diversity/equity/inclusion, workforce development, and practical solutions and resilience.
- Washington State Representative and Columbia Basin College Associate Professor of Computer Science Matt Boehnke emphasized the need to get back to fundamentals to build effective plans that prioritize cyber. He noted the importance of workforce development,

building future cyber professionals who understand emerging technologies and how they can make a difference, particularly for a leading technology state like Washington.

- Director of the Washington Military Department Emergency Management Division Robert Ezelle shared his perspective on how global events demonstrate the importance of planning and preparedness and of building overarching policy with key stakeholders, bringing together the right people to focus on policy direction and resources. He highlighted recent initiatives building on principles of emergency management to coordinate response plans that prioritize resources, establish policies and direction, and facilitate communication and information sharing. The result has been a reliable structure to enable practical solutions during an incident, putting essentials together in a toolkit to better respond in the future.
- CISA Region 10 Regional Director Patrick Massey returned to the cause of the summit: the threat is real and continuously evolving. Cyber incident planning is imperative.

Building on this current state of cyber affairs, Daugherty emphasized the importance of the National Incident Management System[1] and the Incident Command System (ICS)—they are the state's road map to emergency response for all types of disasters, including a cyberattack. The summit was proposed as an added layer of defense to build on these structures and help the state plan for a major cyber event. To that end, he encouraged participants to:

- Be transparent about what resources already exist in the state.
- Discuss how to work together to increase resilience and strengthen response capabilities.
- Identify ways to build on existing public–private partnerships.
- Collaborate across disciplines.

He closed by noting that in a typical emergency, like a fire or winter storm, federal resources are spread thin and counties and states often rely on mutual aid. That is when state entities can share resources to enable speedy, effective response—the Washington State Cyber Incident Response Summit sought to apply that notion to cyber incidents.

> "I hope at the end of these two days we can come away with a broader understanding of the tools and resources that are in our state already to protect us from and respond to a cyberattack against our critical infrastructure. It is critical we develop strategies not only to protect and detect but also to quickly respond and recover so when our castle wall is compromised, our work will continue."
>
> Major General Bret Daugherty

Summit Overview

To prepare participants for the day's activities, Director for PNNL's Northwest Regional Technology Center[2] Ann Lesperance provided an overview of the agenda (see Appendix B), the summit's history, and expectations for discussions and outcomes.

[1] https://www.fema.gov/emergency-managers/nims

[2] http://www.pnnl.gov/projects/nwrtc

Lesperance shared the current summit would focus on specific sectors that participants highlighted in a pre-event survey: elections, water, and transportation. The goal is to establish the building blocks necessary to create useful and consistent incident response plans at the state level, with a focus on:

- What should go in a cyber incident response plan for each sector?
- What in that plan should be unique to a specific sector?
- What can we apply across sectors?

Ultimately, feedback and lessons learned from this workshop will be used to shape similar opportunities for collaboration with other partners and states.

> “In Washington State, we know response takes a whole-of-community approach. Utilizing our state as a model to address cyber incident response from a holistic perspective—while aligning with the CISA’s new and innovative approaches—we can set an example for a state-level program while supporting national and regional understanding of critical systems, assets, networks, and enabling technologies.
>
> Ann Lesperance, PNNL

Day 1: September 7, 2022

Election Security: Approaches to Cyber Incident Response

CISA Senior Election Security Advisor and former Washington Secretary of State Kim Wyman and Washington’s 16th Secretary of State Steven Hobbs began the day’s information sessions with a focus on election security.

Wyman presented on a 2014–2019 modernization effort (VoteWA),[1] showcasing the challenges posed by aging election equipment, systems, and operations. The efforts resulted in numerous technology, policy, and partnership improvements, including those among the Washington State Chief Information Security Office and Chief Information Officer, DHS, FBI, the Washington National Guard, Information Sharing and Analysis Centers, and private security vendors. Wyman emphasized partnerships’ value in improving communication, coordination, and collaboration—and ultimately solutions and mitigation strategies. The effort resulted in the VoteWA platform, but also in resources such as an Elections Cyber Unit with a Security Operations Center, a Memorandum of Understanding with the National Guard, an Election Infrastructure Information Sharing and Analysis Center, and more.

> “We could not have succeeded without our planning. What you’re doing today will serve you well. It is accomplishable, and it is a good investment.”
>
> Kim Wyman, CISA

[1] https://voter.votewa.gov/WhereToVote.aspx

Hobbs shared an overview of the state's collaborative approach to cybersecurity, with values of confidentiality, integrity, and availability spanning from the Washington Secretary of State and counties to the Center for Internet Security and CISA. He provided an overview of the state's Information Security and Response Division, initiated by Wyman and designed to provide cybersecurity, information, technology, and a messaging capability to support the integrity of the election process throughout the state of Washington. He underpinned Wyman's points that partnerships—particularly those with the National Guard and broader military—and tabletop exercises are essential to a robust cybersecurity capability.

In addition to partnerships, Hobbs noted that the challenge of mis-, dis-, and mal-information (MDM) is a growing threat in concert with cyber. He cited the importance of staying proactive and strategic, emphasizing the value of transparency, information sharing (i.e., letting the public know what processes exist and what systems are in place to protect them), and social reminders (i.e., encouraging others to research their information). Where the goal of the adversary is to penetrate trust, educational campaigns can help build it.

> "We cannot sit down—we have to stay active. We deal with a lot of mis-, dis-, and mal-information. We need to let the public know how processes are done and that there are systems in place to protect these processes."
>
> Steven Hobbs, Secretary of State

A participant posed a question regarding elected officials and upcoming elections. Wyman shared three threats focused on in 2022: physical security, cybersecurity, and MDM. They work in concert and weaken people's confidence. This calls for a focus on insider threat, incident response, and access controls.

When asked to pick one thing for sectors less mature in cyber incident response planning to prioritize, the speakers chose communications and MDM. They noted a communications plan is as important as knowing whom to call. Also, preparing for MDM is critical because the perception of an attack is as damaging as a real one.

From left, Hobbs, Daugherty, and Wyman kicked off the summit with a focus on election security.

Federal Perspective: Cyber Incident Response and Activities

CISA Region 10 Chief of Cybersecurity Chris Callahan shared an overview of whole-of-government incident response and coordination, with a focus on federal perspective regarding the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) at CISA.[1] CIRCIA is intended to provide the federal government with a better understanding of the nation's cyber threats and facilitate a coordinated national response to ransomware attacks. CIRCIA went into effect in March 2022, requiring critical infrastructure companies in the 16 industry sectors to report to CISA within 72 hours if they are experiencing a cyberattack and within 24 hours of making a ransomware payment. Callahan outlined the act's key elements, including regulatory reporting requirements and information sharing and coordination responsibilities, and noted that more information about CIRCIA implementation will be coming soon.

Callahan also highlighted Presidential Policy Directive 41, U.S. Cyber Incident Coordination,[2] which set forth principles governing the federal response to cyber incidents that significantly affect a public or private sector entity, national security, or the economy. The cyber incident schema establishes a common framework to evaluate and assess cyber incidents.

Lastly, Callahan highlighted CISA's central all-government approach and response playbooks for coordinated cyber incident reporting and response,[3] the CISA Joint Cyber Defense Collaborative,[4] and top mitigations and controls for combating threats, including multi-factor authentication, patch management, and evaluating business needs and securing risky services.

> "We need to be using the same lexicon, the same playbooks, and the same indicators of compromise. By speaking the same the language, we build better, more consistent, and more effective solutions."
>
> Chris Callahan, CISA Region 10

Callahan from CISA Region 10 shared federal perspective on cyber incident response.

[1] https://www.cisa.gov/circia

[2] https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

[3] https://www.cisa.gov/cyber-incident-response

[4] https://www.cisa.gov/jcdc

Threat Overview and Case Study

Special Agent Jon Chinn, from the FBI, shared highlights from the top 2021 and 2022 cyber threats, including those that are state-sponsored, insider, and evolving.[1] Incidents in 2022 showcased that cyber criminals are opportunistic, motivated by money or monetizing data, and that ransomware, phishing, and compromised business email remain top threat vectors.

Chinn shared an overview of cybersecurity roles and responsibilities across the key agencies, including DHS, Department of Justice and FBI, and Defense. Beyond this triad, he emphasized the broad value of and need for information sharing. Common tools include private industry notifications, public service announcements, and flash notices highlighting a cyber threat, actor, or nation-state targeting a particular system. For the FBI, as the investigative arm of the process, sharing information is essential to how they communicate. Information is crucial to building a case against cyber criminals. Cyber investigations are a partnership between victims and the FBI. It is essential for others to share when they see something suspicious. For resources, Chinn shared InfraGard,[2] which is a partnership between the FBI and members of the private sector for facilitating information sharing, the Internet Crime Complaint Center,[3] the Cyber Task Force, and CyWatch.[4]

> “As the investigative part of the process, we rely on information sharing. Information is crucial to building a case against cyber criminals.
>
> Jon Chinn, Special Agent

Lieutenant Colonel Billy Rios, Commander of the 262nd Cyber Operations Squadron and On-Site Commander for Election Protect Element during the 2020 Presidential and Washington State election, provided personal perspective from an incident from Washington State. From the initial special order and call to duty, his squadron was able to analyze, accurately interpret, and respond to the information thanks to their training and preparedness. He noted such an understanding is crucial for effective response—teams need to be mindful of the lines of responsibility and understand the situation as quickly as possible.

Rios shared some of the specialized tools, dashboards, and programs designed to analyze data of interest and encouraged participants that the results they produced demonstrate his key point: segmentation works.

To that end, Rios also shared additional best practices, including reminders to be mindful and be respectful of opinions, develop contingency plans, manage relationships, and coordinate communications. Rios closed with a few recommendations for the future, including:

- Segmentation of mandated systems for collection and tabulation
- Funding designated for Air National Guard units
- Updated archival capabilities

[1] https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf
[2] https://www.infragard.org/
[3] https://www.ic3.gov/
[4] https://www.fbi.gov/investigate/cyber

- Information campaign on the Guard’s role in protecting election efforts
- Tabletop exercises to establish and maintain relationships
- Augment protect posture by proactive hunter activities
- Vendor support to host security measures at the county level.

Participants asked about best example technologies for segmentation and zero trust architectures. Rios emphasized the need for a system in which if any machine gets compromised, it will not compromise the entire system. Segmentation is a regulated requirement and an important first step; zero trust is a recommended next step but is very advanced.

A participant also asked how to bring others in decision-making positions up to speed to facilitate the urgency and understanding to act, particularly during an election year. Rios recommended that the work needs to start early, not when the incident is happening, and that states should better utilize their National Guard as a resource.

> “Washington is one of the leaders of learning where the lines are: what the federal government can do, what the National Guard can do, how to interact with law enforcement, how we interact with Cyber Command. Understanding these lines and responsibilities allows us to act as quickly as possible.”
>
> Lieutenant Colonel Billy Rios

From left, Chinn and Rios shared overviews of the threat landscape and recent case studies.

Washington State Perspective: Cyber Incident Response and Activities

Alisha King, Washington State Cybersecurity and Critical Infrastructure Manager with the Washington Military Department Emergency Management Division, shared a range of cyber incident response resources, including key structures, tools, and approaches, such as:

- The Cybersecurity and Critical Infrastructure Protection Unit, which maintains affiliations with the Joint Cyber Defense Collaborative, DHS Science and Technology Directorate, and the Government Coordinating Council through DHS CISA.
- The Washington State Protected Critical Infrastructure Information (PCII) Program, which was established to facilitate secure information sharing between sectors.
- The CISA Traffic Light Protocol, which is designed to safeguard content within civilian organizations.[1]
- The recently launched Washington Coalition for Infrastructure Protection and Homeland Resilience (WA-CIPHR), which is designed to enhance collaboration between public and private sector organizations statewide.

Of particular note, King outlined the differences between emergency management and other technical frameworks. For example, she differentiated between common but competing terms for information technology (IT) and emergency management, such as disaster recovery plans, industrial control systems, ICS, community lifelines, and emergency support functions. King reiterated Chris Callahan's point regarding inconsistencies with activation levels between IT and emergency management. King encouraged participants to adopt the ICS, which facilitates coordination of all hazards, and to assure that documentation correctly identifies the necessary escalation procedures for cyber incidents. See Appendix D for example alignment of the CISA Critical Infrastructure Sectors, Federal Emergency Management Agency (FEMA) Emergency Support Functions, and FEMA Community Lifelines.

King shared the recently revised State Emergency Operations Center structure for cyber and infrastructure incident response, which now includes the intelligence section. The center's intelligence section oversees the units for data analysis, infrastructure impacts, investigations, and threat monitoring. A snapshot of the new organizational structure is available in Appendix F.

King also gave an update on the Washington State Significant Cyber Incident Annex refresh and shared highlights from the new Cyber Incident Activation Checklist. She emphasized the legal definitions between emergency proclamations and disaster declarations, noting that these are distinct from activating the Incident Command Systems and that each option has different considerations for jurisdictional authority and resource allocation.

King closed with an overview of resources available to local and tribal jurisdictions, including the incoming State and Local Cybersecurity Grant Program as designated through the Infrastructure Investment and Jobs Act, and the Building Resilient Infrastructure and Communities grant.[2] Participants were encouraged to identify needs within their own communities and develop project proposals that could be used during future funding allocation rounds.

> "Work collaboratively with your information technology and emergency management peers. Connect across disciplines, sectors, and jurisdictions. Identify interdependencies in advance, and expand your thinking beyond what has been to what is possible."
>
> Alisha King, Washington State Cybersecurity and Critical Infrastructure Protection Manager

[1] https://www.cisa.gov/tlp

[2] https://www.fema.gov/grants/mitigation/building-resilient-infrastructure-communities

King shares state perspective on cyber incident response activities.

Sector Breakout Sessions

Participants deployed into breakout sessions focused on cyber incident response planning for two sectors: water and transportation. During the Day 1 debrief, participants introduced themselves, their organizations, and their aspirations for the cyber incident response mission. Participants noted an interest in further discussion on:

- Whom to contact and at what threshold during an incident
- Resource identification
- Clarification on cyber insurance—what are the ramifications, and what are important considerations when using?
- Funding opportunities

Day 1 breakout sessions, led by Lesperance and Godwin, focused on cyber incident response planning for the water and transportation sectors.

Day 2: September 8, 2022

In reviewing the takeaways from Day 1, participants noted the importance of:

- Understanding the growing threat, including the increasing impact of misinformation
- Communications plans, and the need for organizations to have one prepared (and practiced) before an event, particularly for response to media in the wake of MDM

- Partnerships and whole-of-community approaches
- Assessments and tabletop exercises
- Understanding cyber insurance (implications and opportunities)
- Workforce development to build next-generation cyber professionals for all fields.

In response to a comment about designated responsibility and consistency in cyber incident response planning, Daugherty noted that he had asked state agencies "Who's got their eye on cybersecurity?" The answer was no single organization. This raised the question of whether a single organization could have that role—a regulatory agency for cybersecurity and set regulatory standards to override the multiple, conflicting requirements.

Research and Innovations: Asymmetric Resilience

Scott Godwin, a strategic advisor within PNNL's National Security Directorate, shared a presentation highlighting emerging cybersecurity innovations, with a focus on asymmetric resilient cybersecurity.[1] One of the laboratory's internal cyber investments has focused on resilience in particular, with the goal of bringing a scientific understanding as a foundation to develop novel techniques and technologies to drive complex cyber systems toward increased survivability/achieving mission/protection of assets, even in contested cyber spaces. In doing this, PNNL has developed a wide portfolio of approaches that address other needs for cyber defense and decision support, specifically in the areas of situational awareness, decision support, testing and evaluation platforms, and data protection.

With virtualization and the "bring your own device" trends on the rise, cyber environments are becoming increasingly more fluid. The transient nature of such environments, coupled with the complex dependencies of cyber assets, presents a unique challenge to network defenders and IT managers alike—making sure that when one asset moves, all the pieces it connects to also move. This challenge is present in several situations, in conflict and in natural progression with systems. Current methods allow a user to infer which processes depend on each other. However, most are active methods, requiring a change to the network messaging format or network stack. In these cases, only processes that have also changed their network stack will be visible, leaving a huge number of processes and dependencies undiscovered. In response to this challenge, PNNL developed the Passive Cyber Asset Dependency Discovery, or CADDY.[2]

CADDY looks for the co-occurrence of activity on the network and infers those connections in real time with statistical probability. CADDY is a passive monitoring tool that requires no foreknowledge of the network or assets. Once CADDY creates the model of assets and dependencies, the business model can be overlaid to determine which are the most critical. By linking business processes with their supporting cyber assets, CADDY improves the quality and speed of defenders' situation assessment and management. CADDY improves situational awareness for practitioners, increasing response speed and minimizing mistakes by continuously discovering assets and their dependencies and keeping information relevant as the network changes. Information such as triage, battle damage self-assessment, business continuity, and investments are based on criticality, thus significantly enhancing the defender's perspective with business knowledge.

[1] https://cybersecurity.pnnl.gov/

[2] https://cybersecurity.pnnl.gov/documents/roadshow/CADDY_FINAL.pdf

Godwin closed with a question: What is missing from the current offerings from industry, academia, and federally funded research and development centers to make this all possible? He shared six key focus areas as suggestions:

- Passive asset dependency discovery
- Uncertainty-tolerant decision support
- Distributed homomorphic encryption operations
- Model-driven situational awareness
- Experimental integrated testing and evaluation platform
- Tabletop cyber defense coordination and assessment.

Strategic Focus Areas: Water and Transportation Sectors

Participants redeployed to their breakout groups and focused on a series of questions designed to identify needs, challenges, and opportunities facing cyber incident response planning within the transportation and water sectors. The guiding questions are outlined in Appendix G, and the results of the discussions are summarized below and in Table 1.

Table 1. Sector Cyber Incident Response Planning

Focus Area	Transportation	Water
What do we have?	• American Public Power Association Cyber Incident Playbook • U.S. Coast Guard Maritime Transportation System Incident Response Plan • Lessons learned from recent local incidents • CISA tools – i.e., Playbooks, Portal, Known Exploitable Vulnerability List • Washington State Fusion Center	• Snohomish County Incident Response Plan and Playbook • Spokane and Tacoma – National Institute of Standards and Technology Cybersecurity Framework • 800-53 – General Cybersecurity • 800-62 – National Institute of Standards and Technology ICS Framework
What do we need?	• Easy, standardized process and templates (and bandwidth to use them) • Capacity within the community to plan, train, and exercise to build muscle memory • Resource sharing ○ Potential for legislature at the national level (e.g., bring National Guard for pen testing) ○ Struggle with legal implications, liability, authorization ○ Need champions for sector cybersecurity in legislature • Strengthen connections from local end users to the Fusion Center and the Fusion	• Communication between different segments within the organization (physical/engineers and cyber) • Funding/grants • Understanding opportunities and how to pursue resources • Team management: ○ Skills ○ Subject matter experts ○ Retention • Restoration efforts in the water sector are highly specialized

Focus Area	Transportation	Water
	Center to the state; increase robustness in Fusion Center - Curriculum/workforce development	
What can we leverage?	- Existing playbooks (CISA, Public Power, etc.) - CISA facilitates exercises from tabletop to national level - Lessons learned from the city of Sammamish - Increased cyber interest/awareness among the public – create civilian cyber corps, bring in universities	- Trade organizations ○ American Metropolitan Water Association ○ Water Environment Federation ○ WA Waren Network ○ Washington Association of Sewer and Water Districts - Mutual aid agreements/contracts - State emergency management - State and federal tools/guidance (e.g., Annex)
What is in our way?	- Funding - Separate plans (IT departments have their own cyber response plans vs. an organization-wide response plan, resilience vs. incident response) - Time to assemble a plan - Priority – needs to be required, needs to change mindset	- Resourcing – largest issue - Establishing roles and responsibilities - Silos (culture within different regulatory agencies) - Organizational/leadership – change management - Communication with key stakeholders/elected officials to prioritize - State restoration priority – understand Governor's priorities - Retaining skills - Culture shift within technology
Next steps	- Pursue projects suggested during discussion (i.e., cyber event at a small port in Eastern Washington) - Resume regularly scheduled exercises - Strengthen relationship with the Washington State Fusion Center	- Perform gap assessment of where we are today and what is required - Develop and collect survey to get truth on cyber insurance in the sector (costs, broker, and providers) - Establish state-sponsored resource pool to support small and medium organizations (training, consultation, and program management) - Leverage PNNL to develop framework templates, standard document library to support sectors

Resources

Both groups discussed diverse resources and existing plans available within their sectors, including:

- **County- and District-level Incident Response Plans and Playbooks –** classify systems by departments and integrate IT throughout. Several are based on the American Public Power Association model.[1]
- **Annual External Assessments –** conducted by an external entity. Having an objective outside source is helpful.
- **Trade Organizations –** post-recovery pieces help communicate sector-specific lessons learned.
- **State Resources for Smaller/Medium Agencies –** can assist in creating plans, resources, training, etc. (e.g., Evergreen Rural Water of Washington[2]).
- **Multi-Rural Community Assistance Corporation –** federal grants and work locally to pursue funding to deliver training.
- **Infrastructure Assistance Coordinating Council**[3] – sponsors an annual statewide conference and provides technical assistance to communities and tribes.
- **Area Maritime Security Committee**[4] **–** established per Maritime Transportation Security Act to better address maritime security issues.
- **Requirements and Standards**
  - National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61 Computer Security Incident Handling Guide[5]
  - NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations[6]
  - NIST SP 800-82 Guide to ICS Security[7]
  - Title 33 Code of Federal Regulations, Navigation and Navigable Waters[8]
  - House Bill 5432, Concerning Cybersecurity and Data Sharing in Washington State Government[9]
  - National Response Framework.[10]

Needs and Challenges

Participants discussed needs within their individual sectors and barriers to success, including:

- **Resources –** There is a widespread need for more time, people, and money to build the capacity to effectively work within sectors and communities to plan, train, and build muscle

[1] https://www.publicpower.org/system/files/documents/Public-Power-Cyber-Incident-Response-Playbook.pdf
[2] https://www.erwow.org/
[3] https://infrafunding.wa.gov/
[4] https://www.dco.uscg.mil/Our-Organization/Assistant-Commandant-for-Prevention-Policy-CG-5P/Inspections-Compliance-CG-5PC-/Office-of-Port-Facility-Compliance/Domestic-Ports-Division/amsc/
[5] https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final
[6] https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
[7] https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final
[8] https://www.ecfr.gov/current/title-33
[9] https://app.leg.wa.gov/billsummary?BillNumber=5432&Initiative=false&Year=2021
[10] https://www.fema.gov/emergency-managers/national-preparedness/frameworks/response

memory. With fewer resources and time, an intentional approach is key. An outside consulting team can be hired if short on time. Additionally, support services such as forensics services, easily accessible templates, and dedicated collaboration space (virtual and in-person) would be helpful.

- **Mutual Aid –** Mutual aid is difficult due to the uniqueness and age of equipment and further complicated by the supply chain for operational technology (OT).
- **Coordination** – This was proposed to establish sector cyber committees similar to the Area Maritime Security Committee. Also, regularly scheduled assessments and exercises should be executed across sectors, leveraging subject matter experts in design, implementation, and lessons learned. Participants also urged the need for a coordinated, prioritized, and unified plan by FEMA and CISA, as well as consistency in policy direction and implementation.
- **Guidance**/**Documentation –** Specifically, how to use ICS to manage cyber incidents, a common contact list or process flow for whom to contact and at which threshold, and consistency in policy direction. Additionally, legislature could be proposed to facilitate nongovernmental sharing of resources, address legal indemnification, etc. Cyber champions in legislature are needed.
- **Training and Workforce Development** – Mandated training should be implemented. Set a specific timeline and expectation for drills and exercises. Training should include tabletop exercises with realistic scenarios. Build affordable and accessible cyber training at various levels, similar to the Public Infrastructure Security Cyber Education Program.[1]
- **Relationships and Expertise** – In particular, strengthen connection through the Fusion Center, from local end users to the Fusion Center and from the Fusion Center to the state. Additionally, subject matter experts are needed for every phase and plan component, including disaster communications experts.
- **Organizational Structures –** Cyber is often positioned inconsistently across sectors, changing its operational span of control. Further, there is a common false perception of isolation between OT and IT, rather than understanding the interconnection between systems.
- **Silos –** No single regulatory agency is responsible for cyber incident response, and regulatory agencies often operate in silos as a result, limiting their visibility into the different sectors. For example, water does not fall under one specific municipality and thus has contacts and regulations under different municipalities.
- **Vendor Management –** Sectors need better mechanisms in place for contract management in the event of a crisis. Specialized third parties could be used to assist with cyber incident response planning, exercise/training management, etc.
- **Prioritization –** Participants encouraged more visibility regarding the governor's priority and state restoration priority in the event of an emergency.
- **Cyber Insurance –** Participants were united in their concern for and desire to better understand cyber insurance. Agencies are misunderstanding escalation processes after an incident. Further, most cyber insurance stipulations claim if the victim (government agency) officially notified another entity (FBI, CISA, etc.) before reporting to insurance, they void

[1] https://pisces-intl.org/

insurance. Participants recommended that regulations more clearly state what insurance companies must cover and provide protection for sectors.

Best Practices and Opportunities

Participants identified the following best practices and opportunities for advancing sector-specific cyber incident response planning:

- Hire a consultant to create comprehensive guidance that includes a communication strategy, roles and responsibilities, and relevant documentation.
- Conduct a needs assessment/initial assessment to identify existing needs and gaps, then work through decision makers for direct funding to dedicate to the system and tools (teams and funding).
- Keep plans live and dynamic with regularly scheduled audits and exercises (annually at minimum).
- Organizations can establish boards or leadership directives to drive priorities and practices toward becoming a regional leader in cyber incident response.
- Create a team dedicated to cyber incident response. Leverage the teams' existing expertise (communications, planning, etc.) and encourage training/continuous education. This team reporting to an executive provides heightened visibility, accountability, and awareness of priorities.
- Quantify risk into business models and translate into model/impact. Every department/stakeholder has business risk. Identify someone to translate OT/IT problems into actionable models and strategies to minimize risk.
- Improve dissemination of incident response plans and expectations at all levels (county, employee, public) through awareness campaigns and outreach events.
- Leverage CISA resources and capabilities, such as:
  - Facilitation of exercises from tabletop to national level
  - Known Exploitable Vulnerability List[1]
  - Multi-State Information Sharing and Analysis Center [2]
- Create civilian cyber corps focused on cyber incident response planning; include universities and national laboratories.

Recommendations

Participants shared recommendations to advance sector-specific cyber incident response planning:

- Develop and collect a survey to get the truth on cyber insurance in the sector (costs, brokers, providers).
- Create a white paper on how to perform gap analyses.

[1] https://www.cisa.gov/known-exploited-vulnerabilities-catalog
[2] https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf

- Create a resource catalog for a state-sponsored resource pool, including project management, WaTech, and consulting services.
- Leverage PNNL to develop framework templates and state standard to support all sectors.
- Pursue grant funds for risk assessments. Clear authorities and budget to perform ongoing assessments, training, etc.
- Coordinate vendor management/contract management (Government Services Administration).
- Issue Governor’s office official communication stating cybersecurity priority and why programs should be funded.
- Conduct another summit or establish a task force to lead cyber incident response planning.
- Develop sector-specific cyber incident response tools.

Day 2 breakout sessions took a deep dive into cyber incident response planning for the water and transportation sectors.

Participant Feedback

Throughout the event, participants were invited to complete a short questionnaire capturing their organization's cyber incident response needs and capabilities to better understand the resources, opportunities, and challenges in our state. The responses are summarized below.

Participants indicated they hailed fairly equally from the water and transportation sectors, as well as state and local government, technology, military, WaTech, CISA, and other sectors. Majority of the work was for large (250+) entities and within Western Washington.

The overall survey elicited details regarding existing resources and needs:

- Participants indicated that risk management tools and discussions on processes, conduct of operations, and procedures were their top priority.
- Incident response training and tools were cited as the top resource need.
- Personnel/subject matter expertise was the most-cited resource available from organizations.

- In addition to a cyber incident response plan, knowing whom to call or coordinate with was the second greatest need indicated.

Additionally, when asked to list two options to better prepare their organization for a cyber incident, priorities included:

- Identified network capabilities and analysis at a strategic level
- Fully developed Security Operations Center
- More vulnerability testing
- Improved monitoring tools
- Well-drafted standard operating and emergency procedures
- Managed security services
- Stronger communication network
- More resources or trained personnel
- Training, including trained cyber staff who can triage live incidents
- Helping all organizations with their cyber incident response plan
- Business impact analysis of entire system
- Updated systems and tools
- Modernize legacy systems
- Develop and exercise playbooks
- In-house IT
- Manage centralized response to coordinate resources where appropriate
- OT cybersecurity subject matter expertise
- More in-house resources
- Security tools and resources
- Maintenance tracking system design and implementation
- Mature incident response plan
- Documentation
- Pre-planned press briefings
- Planning that is operational
- More fluent and secure remote network access for end users.

Conclusion

Key takeaways from the two-day discussion highlighted both challenges and opportunities facing Washington State in the mission for effective cyber incident response:

- The threat is real, and the threat is growing. Cyber criminals are opportunistic, motivated by money and putting health and safety at risk.
- Misinformation can be as big of a concern as an actual cyberattack, making a communications plan essential.
- There is a desire for sector-specific Security Operations Centers with consistent Conduct of Operations, training, and reporting structures.
- Partnerships, communications plans, assessments/tabletop exercises, and structured information sharing with well-defined tiers/triggers are essential because there is no 911 for cyber incidents. Tools and resources are available from CISA, FBI, state, etc. to aid in cyber incident response, but they need to be more effectively communicated.

Participants were also greatly encouraged, should a cyber incident occur and they do not know whom to call, to contact TAG or the Washington Military Department Emergency Management

Division. King also encouraged participants to reach out to the Cybersecurity and Critical Infrastructure Protection Unit at CCIP@mil.wa.gov for opportunities including access to cybersecurity assessments to identify gaps, numerous types of grants, and additional training. Participants can also sign up for notifications to:

- Cyber incidents affecting Washington State
- State Emergency Operations Center activations
- Updates on grant funding opportunities
- Training and credentialing opportunities
- Inquire about the Washington State PCII Program
- Request training for your organization and your partners
- Resilience planning resources for industry, infrastructure, and private sector partners.

Next Steps

The summit emphasized a need for growing a network of partners and mutual aid to align sectors across Washington State. Recommended next steps include:

- Conduct a follow-on event and maintain communications among participants to build on the two-day discussion.
- Expand the invitees to include other critical infrastructure sectors and organizations, such as trade organizations, to provide heightened awareness of resources to fill any gaps agencies identified.
- Continue communication among sectors to help determine common areas of opportunity to provide state and federal leaders insight into high priorities on how to respond to cyber incidents within Washington State and across the nation.

Appendix A. Participating Organizations

- Department of Homeland Security Science and Technology Directorate
- Cybersecurity and Infrastructure Security Agency
- 252 Cyberspace Operations Group
- Chelan County Public Utility District
- City of Spokane
- Department of Ecology
- Department of Health
- Highlight Water District
- LOTT Water Alliance
- Northwest Seaport Alliance
- Office of Governor Jay Inslee
- Port of Benton
- Port of Edmonds
- Port of Seattle
- Port of Tacoma
- Seattle City Light
- Snohomish County
- Tacoma Public Utilities
- Transportation Security Administration
- TRIDEC
- U.S. Coast Guard
- Washington Air National Guard
- Washington Military Emergency Management Division
- Washington State Department of Transportation
- Washington State Ferries
- Washington State Fusion Center
- Washington State House of Representatives
- Washington State Office of the Chief Information Officer
- Washington Utilities and Transportation Committee
- WaTech

Appendix B. Agenda

September 7, 2022

Time (PST)	Activity	Lead
09:00–09:30	Check-in and Networking (30 min)	—
09:30–10:15	Welcoming Remarks (45 min)	MG Bret Daugherty, TAG, WA State National Guard Leadership Team Patrick Massey, Regional Director CISA Region 10
10:15–10:30	Cyber Summit Plan and Expectations (15 min)	MG Bret Daugherty Ann Lesperance, PNNL
10:30–11:15	Election Security – Approaches to Cyber Incident Response (45 min)	Steve Hobbs, Secretary of State, WA State Kim Wyman, Senior Election Security Advisor, DHS CISA
11:15–11:30	Break (15 min)	—
11:30–12:00	Federal Perspective: Cyber Incident Response and Activities at CISA (30 min)	Chris Callahan, Chief of Cybersecurity, CISA Region 10
12:00–12:15	Group Picture (15 min)	Maren Disney
12:15–13:30	Working Lunch – Threat Overview (FBI) Case Study (Guard) (75 min) (15min/30min/30min)	Special Agent Jon Chinn Lt. Col Billy Rios
13:30–14:15	Washington State Perspective: State of Cyber Incident Response and Activities in Washington State (45 min)	Alisha King, Washington State Cybersecurity and Critical Infrastructure Manager, Emergency Management Division
14:00–14:15	Break (15 min)	—
14:15–15:15	Sector Breakouts (60 min)	Krystal Ayala, Ian Moore, Scott Godwin, Alisha King, Ann Lesperance, Rich McLaughlin
15:15–15:30	Closing Remarks and Next Steps (15 min)	PNNL

September 8, 2022

Time (PST)	Activity	Lead
09:00–09:30	Check-in and Networking (30 min)	—
09:30–10:00	Research and Innovations – Asymmetric Resiliency (30 min)	Scott Godwin, PNNL
10:00–12:00	Strategic Focus Area: Water and Transportation Sector Building blocks for cyber incident response planning in each sector (120 min)	Ann Lesperance, Scott Godwin, Alisha King, Ian Moore
12:00–13:30	Working Lunch – Continue Group Work (90 min)	—
13:30–15:00	Leadership Team and Session Report-Outs (90 min)	Sector Representatives
15:00–15:30	Closing Remarks	Leadership/TAG

Appendix C. Resources

The following are resources shared during the Washington State Cyber Incident Response Summit. This is for educational purposes and does not indicate ownership or endorsement.

General Resources

- Public Infrastructure Security Cyber Education System https://pisces-intl.org/
- FBI Cyber https://www.fbi.gov/investigate/cyber
- FBI 2021 Internet Crime Report https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf
- Infragard https://www.infragard.org/
- FEMA Building Resilient Infrastructure Communities Grants https://www.fema.gov/grants/mitigation/building-resilient-infrastructure-communities
- PNNL Asymmetric Resilient Cybersecurity https://cybersecurity.pnnl.gov/
- PNNL Cyber Asset Dependency Discovery Tool https://cybersecurity.pnnl.gov/documents/roadshow/CADDY_FINAL.pdf
- American Public Power Association Public Power Cyber Incident Response Playbooks https://www.publicpower.org/system/files/documents/Public-Power-Cyber-Incident-Response-Playbook.pdf
- National Governors Association Cybersecurity Policy Academy Washington State Report https://watech.wa.gov/sites/default/files/public/privacy/NGA%20Cybersecurity%20Policy%20Academy_Washington%20State_Final.pdf
- Infrastructure Assistance Coordinating Council https://infrafunding.wa.gov/

Standards and Requirements

- NIST SP 800-61 Computer Security Incident Handling Guide https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final
- NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
- NIST SP 800-82 Guide to ICS Security https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final
- Title 33 Code of Federal Regulations, Navigation and Navigable Waters https://www.ecfr.gov/current/title-33
- House Bill 5432, Concerning Cybersecurity and Data Sharing in Washington State Government https://app.leg.wa.gov/billsummary?BillNumber=5432&Initiative=false&Year=2021
- National Response Framework https://www.fema.gov/emergency-managers/national-preparedness/frameworks/response
- Committee on National Security Systems Instruction No. 1253, Security Categorization and Control Selection for National Security Systems https://www.dcsa.mil/portals/91/documents/ctp/nao/CNSSI_No1253.pdf

CISA Resources

- CISA Traffic Light Protocol https://www.cisa.gov/tlp
- CISA Alerts, Bulletins, Security Updates, Best Practices https://us-cert.cisa.gov/
- CISA Playbooks https://www.cisa.gov/cyber-incident-response
- National Cyber Incident Response Plan https://www.cisa.gov/uscert/ncirp
- CISA Incident Response Training https://www.cisa.gov/incident-response-training
- CISA "Protect Your Network: Strengthen Your Cybersecurity with Our Incident Response Training" YouTube Playlist https://www.youtube.com/playlist?list=PL-BF3N9rHBLJaSbTRPyWYj56f0m2uDQD7
- CISA Federal Virtual Training Environment Public Courses https://fedvte.usalearning.gov/public_fedvte.php
- CISA Joint Cyber Defense Collaborative https://www.cisa.gov/jcdc
- Protected Critical Infrastructure Information Program https://www.cisa.gov/pcii-program

Washington State Emergency Management Division Resources

- Cybersecurity and Critical Infrastructure Protection Unit CCIP@mil.wa.gov
- Washington Coalition for Infrastructure Protection and Homeland Resilience (WA-CIPHR)
- Washington State Protected Critical Infrastructure Information Program
- Washington State Protected Critical Infrastructure Program – refresh anticipated 2023
- Washington Significant Cyber Incident Annex – refresh in progress

Water Sector Resources

Trade Organizations, National Models, Networks, and Agreements

- Washington Water/Wastewater Agency Response Network (WAWARN)
- American Water Works Association (AWWA)
- American Metropolitan Water Association (AMWA)
- Water Environment Federation (WEF)
- Multi-Rural Community Assistance Corporation
- Evergreen Rural Water of Washington
- WASWD Washington Association Sewage District
- Infrastructure Assistance Coordinating Council

Transportation Sector Resources

- Area Maritime Security Committee https://www.dco.uscg.mil/Our-Organization/Assistant-Commandant-for-Prevention-Policy-CG-5P/Inspections-Compliance-CG-5PC-/Office-of-Port-Facility-Compliance/Domestic-Ports-Division/amsc/

Legislature

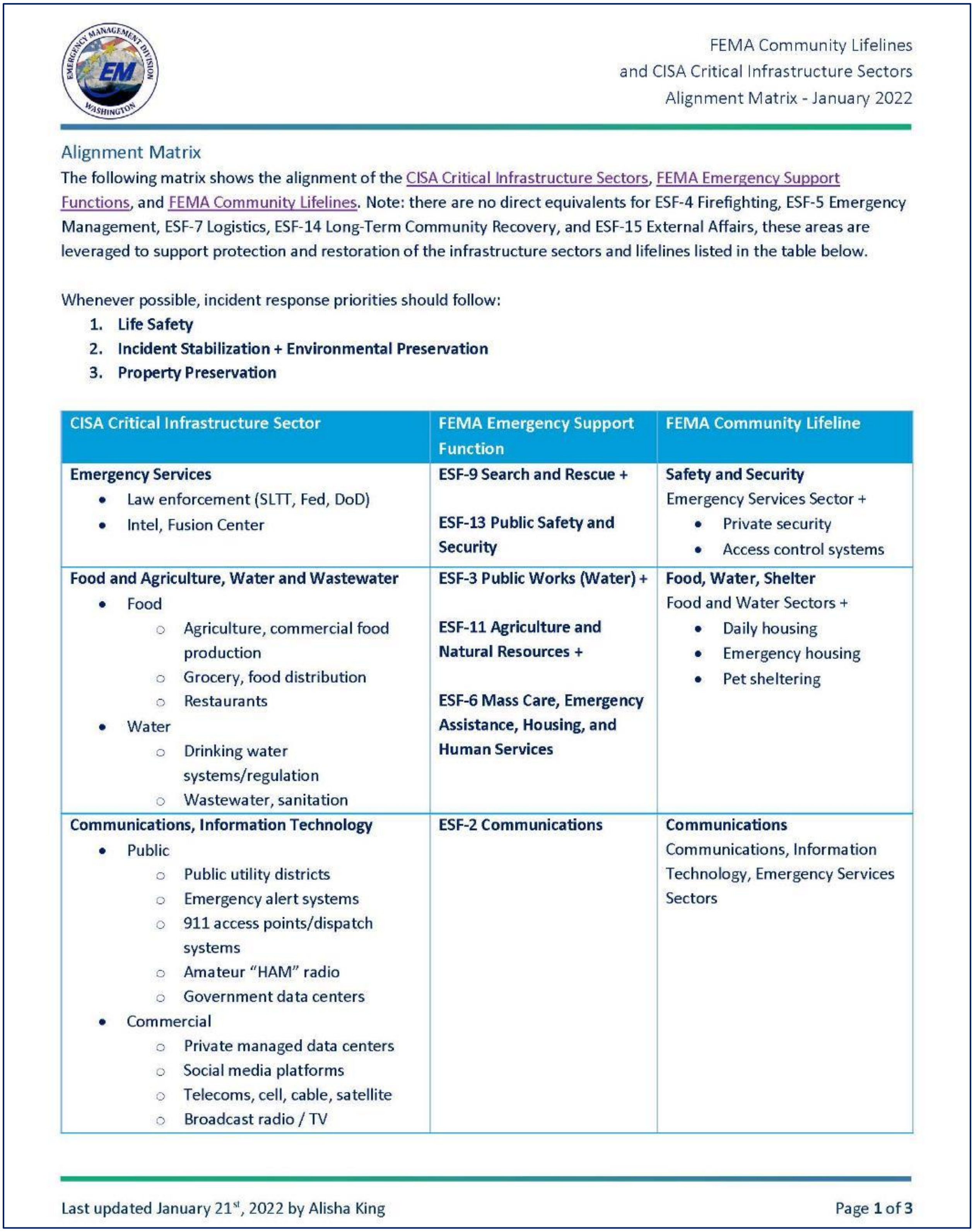
- Cyber Incident Reporting for Critical Infrastructure Act of 2022 https://www.cisa.gov/circia
- Presidential Policy Directive 41, United States Cyber Incident Coordination https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident
- House Bill 5432 Concerning cybersecurity and data sharing in Washington State government https://app.leg.wa.gov/billsummary?BillNumber=5432&Initiative=false&Year=2021

Incident Notification and Support Contacts

- Washington State Emergency Management Alert and Warning Center 1-800-258-5990
- WA State Agencies Only – Notify WaTech at 360-407-8800 option #2 within 24 hours of identifying a significant cybersecurity incident
- OPTIONAL: Report the incident to CISA http://www.us-cert.cisa.gov
- MITRE ATT&CK https://attack.mitre.org/

Appendix D. Infrastructure Sector and Lifeline Alignment

Provided by Alisha King, Washington State Cybersecurity and Critical Infrastructure Protection Manager



FEMA Community Lifelines
and CISA Critical Infrastructure Sectors
Alignment Matrix - January 2022

Alignment Matrix

The following matrix shows the alignment of the CISA Critical Infrastructure Sectors, FEMA Emergency Support Functions, and FEMA Community Lifelines. Note: there are no direct equivalents for ESF-4 Firefighting, ESF-5 Emergency Management, ESF-7 Logistics, ESF-14 Long-Term Community Recovery, and ESF-15 External Affairs, these areas are leveraged to support protection and restoration of the infrastructure sectors and lifelines listed in the table below.

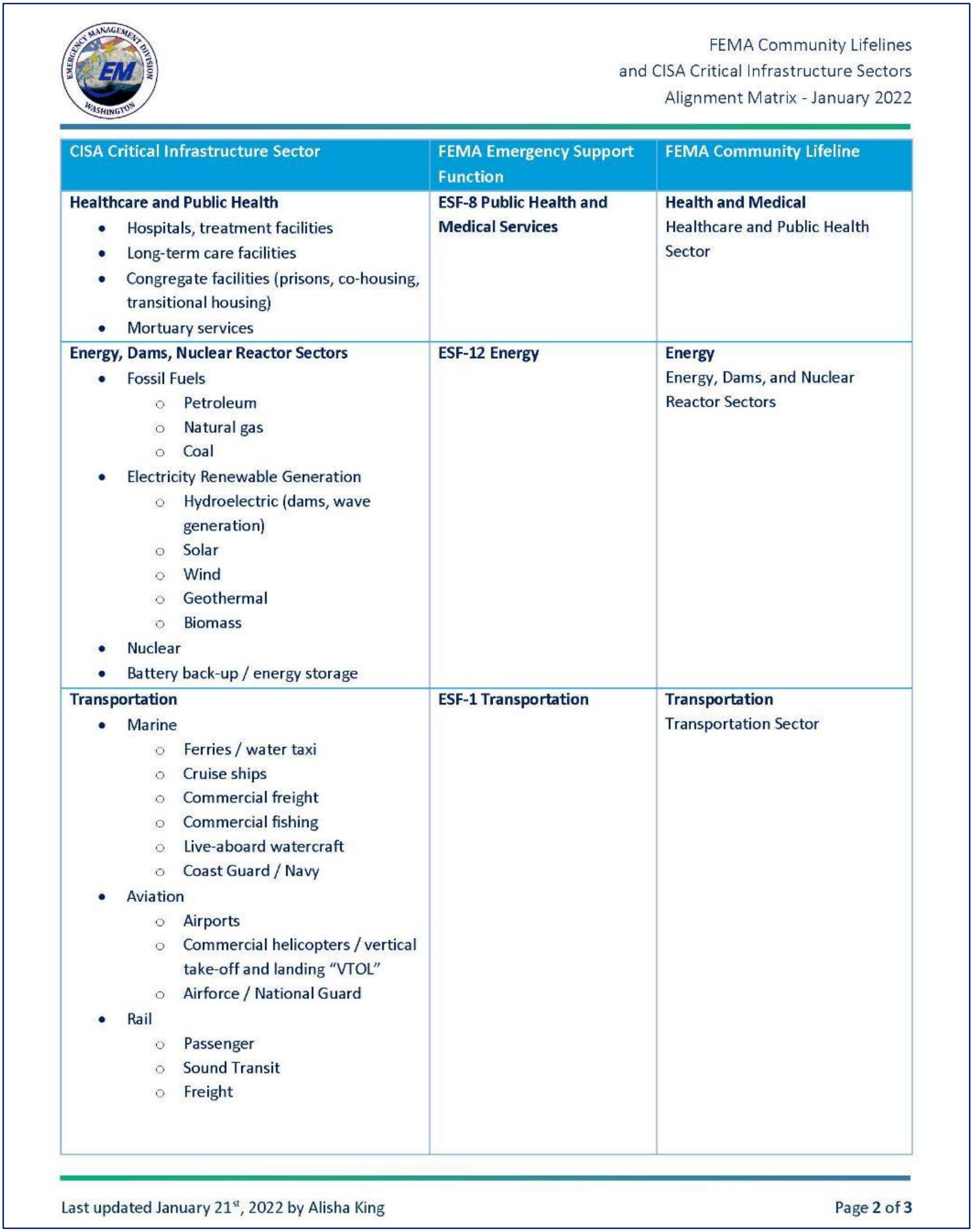
Whenever possible, incident response priorities should follow:

1. **Life Safety**
2. **Incident Stabilization + Environmental Preservation**
3. **Property Preservation**

CISA Critical Infrastructure Sector	FEMA Emergency Support Function	FEMA Community Lifeline
Emergency Services • Law enforcement (SLTT, Fed, DoD) • Intel, Fusion Center	**ESF-9 Search and Rescue +** **ESF-13 Public Safety and Security**	**Safety and Security** Emergency Services Sector + • Private security • Access control systems
Food and Agriculture, Water and Wastewater • Food ○ Agriculture, commercial food production ○ Grocery, food distribution ○ Restaurants • Water ○ Drinking water systems/regulation ○ Wastewater, sanitation	**ESF-3 Public Works (Water) +** **ESF-11 Agriculture and Natural Resources +** **ESF-6 Mass Care, Emergency Assistance, Housing, and Human Services**	**Food, Water, Shelter** Food and Water Sectors + • Daily housing • Emergency housing • Pet sheltering
Communications, Information Technology • Public ○ Public utility districts ○ Emergency alert systems ○ 911 access points/dispatch systems ○ Amateur "HAM" radio ○ Government data centers • Commercial ○ Private managed data centers ○ Social media platforms ○ Telecoms, cell, cable, satellite ○ Broadcast radio / TV	**ESF-2 Communications**	**Communications** Communications, Information Technology, Emergency Services Sectors

Last updated January 21st, 2022 by Alisha King

Page **1** of **3**



CISA Critical Infrastructure Sector	FEMA Emergency Support Function	FEMA Community Lifeline
Healthcare and Public Health • Hospitals, treatment facilities • Long-term care facilities • Congregate facilities (prisons, co-housing, transitional housing) • Mortuary services	**ESF-8 Public Health and Medical Services**	**Health and Medical** Healthcare and Public Health Sector
Energy, Dams, Nuclear Reactor Sectors • Fossil Fuels ○ Petroleum ○ Natural gas ○ Coal • Electricity Renewable Generation ○ Hydroelectric (dams, wave generation) ○ Solar ○ Wind ○ Geothermal ○ Biomass • Nuclear • Battery back-up / energy storage	**ESF-12 Energy**	**Energy** Energy, Dams, and Nuclear Reactor Sectors
Transportation • Marine ○ Ferries / water taxi ○ Cruise ships ○ Commercial freight ○ Commercial fishing ○ Live-aboard watercraft ○ Coast Guard / Navy • Aviation ○ Airports ○ Commercial helicopters / vertical take-off and landing "VTOL" ○ Airforce / National Guard • Rail ○ Passenger ○ Sound Transit ○ Freight	**ESF-1 Transportation**	**Transportation** Transportation Sector

CISA Critical Infrastructure Sector	FEMA Emergency Support Function	FEMA Community Lifeline
- Roadways ○ Highways/bridges ○ Overpass signs ○ Traffic signals (stoplights)		
Chemical Manufacturing - Plastics - Refrigerants - Cleaning products	**ESF-10 Oil and Hazardous Materials Response**	**Hazardous Material** Chemical Manufacturing Sector + - Solid waste disposal - Food storage (refrigerant) - Biological waste (healthcare)
Financial Services - Economic safety-nets EBT, WIC - Traditional banks, credit union, ATMs - Cryptocurrency		*Correlated with Communications*
Government Facilities - Continuity facilities - Equipment warehouses		*No equivalent*
Commercial Facilities - Commercial warehouses - Retail stores, "bigbox" stores - Entertainment venues		*No equivalent*
Critical Manufacturing - Vehicles - Electronics - Appliances		*No equivalent*
Defense Industrial Base - Production of equipment for US military		*No equivalent*

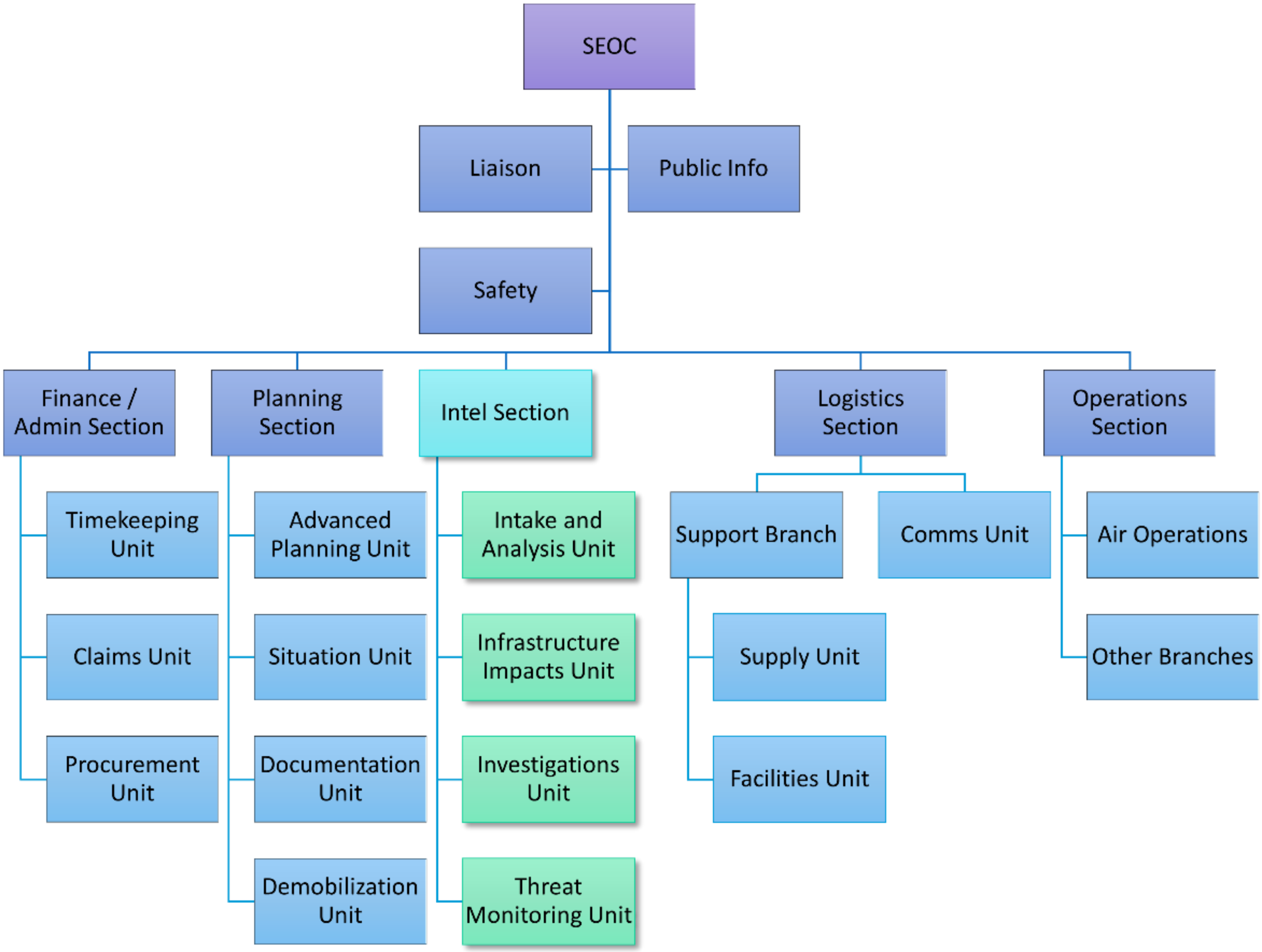
Appendix E. Activation Levels Matrix

Provided by Alisha King, Washington State Cybersecurity and Critical Infrastructure Protection Manager

Washington State Activation Levels	Washington State Activation Level Description
Level 1 **Full Activation**	**FEMA/WA-EMD** In a Full Activation, all the SEOC functions activate to support the incident or the impacted jurisdictions from the SEOC or Joint Field Office (JFO). State agencies activate to fill Emergency Support Functions (ESFs) as dictated by the incident. In a catastrophic incident, SEOC staffing will expand to include representation from other states, federal agencies, local representatives, the private sector, and volunteer staff as required by the incident. **CISA/NIST** • Level 5 - Poses an imminent threat to the provision of wide-scale critical infrastructure services, national government security, or the lives of US citizens. • Level 4 - Likely to result in a significant impact to public health or safety, national security, economic security, foreign • Level 3 - Likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 2 **Partial Activation**	**FEMA/WA-EMD** When an incident exceeds the capability or capacity of the Alert and Warning Center, the SEOC activates to a level 2 Partial Activation. In a Partial Activation, one or more of the SEOC functions activate to support the incident or the impacted jurisdictions from the SEOC or Joint Field Office (JFO). State agencies activate to fill Emergency Support Functions (ESFs) as dictated by the incident. **CISA/NIST** • Level 2 - May impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 3 **Monitoring Activation**	**FEMA/WA-EMD** Level 3 reflects the routine activation level in which state agencies conduct their daily emergency management responsibilities. The State Emergency Operations Officers (SEOOs) in the SEOC Alert and Warning Center (AWC) manage and coordinate incidents in cooperation with local, state, and federal agencies. The AWC operates 24 hours a day, including weekends and holidays. **CISA/NIST** • Level 1 - Unlikely to impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence. • Level 0 - Unsubstantiated or inconsequential event.

Appendix F. Incident Command System Structure

Provided by Alisha King, Washington State Cybersecurity and Critical Infrastructure Protection Manager



Appendix G. Breakout Session Questions

Cyber Incident Response Breakout Sessions

Water and Transportation Sector

10:00–10:45 Group Breakout

The goal of this session is to talk in general about cyber incident response templates or frameworks, and about how you approach cyber incident response and communication with others should an event occur.

1. Are there some examples of cyber incident response planning templates or frameworks in your sector today?
    - If yes, are there best practices and key learnings to be leveraged?
    - If not, why not?
2. How would you approach an incident in your sector?
    - What about your own organization—has your organization planned for or do you have a conduct of operations for cyber-related events?
    - If yes—why?
    - If not —why not?
3. Does the annex or other state resources help in developing a cyber incident response plan for your sector?
    - If yes—what is beneficial?
    - If not, what’s missing?
    - How much of ICS and incident response is known in the Cyber/CISO realm?
    - Who, if anyone, would your organization call if there was a cyber-related event?
    - What would trigger your informing someone outside of your organization?

10:45 Report Out (5 minutes per group)

11:00–11:45 Group Breakout

The goal of this session is to identify any barriers or challenges in putting together a cyber incident response plan (and how those could be addressed) and talking about sharing resources and information.

4. Are there unique barriers in putting together an incident response plan for a cyber event in general?
    - Are there unique positions that need to be added from a standard response plan?
    - What is needed to overcome the barriers?
5. Are there unique challenges that are barriers to putting together a cyber incident response plan in your sector?
    - Do you, and if so, how do you share information without sensitivity/attribution with others in your sector?
    - What might you want/need in terms of mutual aid?
        - Who has the assets? Can they be shared? How? Who would coordinate?
        - Does the Stafford Act adequately support the sharing of cyber-specific resources?
    - Do you already have mutual assistance plans/agreements in place?
6. What would be the foundational resources that would be needed in implementing an incident response plan?

Is there a way to "stockpile" resources that can be called up like in other disasters?
What priority resources would be needed?
Expertise? Equipment?

12:00–1:15 Group Breakout

The goal of this session is to take a deeper dive into the types of cyber incident response (triggers) and use of insurance. Finally, we want you to identify two things the state or federal government could do or provide that could make your organization better prepared to respond to a cyber event.

7. Would you be able to quantify a cyber incident into the incident types (1-5) that ICS currently uses?
   What would be needed to determine these scales?
8. Is there a pathway to make a plan that can be used by all critical infrastructure sectors?
9. Cybersecurity insurance
   What do the policies say, what are their restrictions, what do they cover, how are they invalidated?
10. If there are two things that the state and or federal government could provide to your organization to make you better prepared to address a cyber event—what would those be?

1:15 Prep for Report-Outs

1:30 Report Out

Breakout sub-sessions		
Each session will last 45 mins of working time	5 min of consolidation/speaker selection	10 min of reporting
Session 1	Current response	Questions 1, 2, 3
Session 2	Resources	Questions 4, 5, 6
Session 3	What to include in a plan	Questions 7, 8, 9

Pacific Northwest National Laboratory

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99354

1-888-375-PNNL (7665)

www.pnnl.gov