CYBERSECURITY WORKSHOP

Region 6, Critical Infrastructure Working Group

DECEMBER 7, 2017

King County

Pacific NorthWest Economic Region

CRDR
Center for Regional Disaster Resilience

UNCLASSIFIED

ADMINISTRATIVE HANDLING INSTRUCTIONS

1. The title of this document is Cybersecurity Workshop

2. The information in this AAR is Unclassified (U).

Contacts:

Brandon Hardenbrook, Deputy Director
Pacific Northwest Economic Region
206-443-7723
brandon.hardenbrook@pnwer.org
www.pnwer.org

Nate Weigel, Program Coordinator
Center for Regional Disaster Resilience, Pacific Northwest Economic Region
206-443-7723
nate.weigel@pnwer.org
www.regionalresilience.org

TABLE OF CONTENTS

ADMINISTRATIVE HANDLING INSTRUCTIONS 2
SECTION 1: WORKSHOP SUMMARY 5
SECTION 2: BACKGROUND 5
SECTION 3: WORKSHOP DESIGN 6
A. Design Team 7
B. Administrative Details 7
C. Purpose 7
D. Core Capabilities 8
E. Objectives 8
F. Participation 9
SECTION 4: SPEAKERS AND DISCUSSION 9
A. Welcoming Remarks 9
B. Cyber Incident Reporting 10
C. Lessons for the Maritime Community 15
D. Cyber Insurance 16
E. Cyber Reporting – Table Discussions 17
F. Cyber Civil Support Team Initiative 20
SECTION 5: EVALUATION 22
A. Participant Feedback Summary 22
B. Assessment by Objectives 24
SECTION 6: RECOMMENDATIONS 25
APPENDIX A: WORKSHOP AGENDA 27
APPENDIX B: SPEAKER BIOGRAPHIES 29
APPENDIX C: RECOMMENDATIONS SUMMARY 2010-2017 35
APPENDIX D: ACRONYMS 41
APPENDIX E: WEB LINKS 42
APPENDIX F: PARTICIPANT FEEDBACK FORM 43
APPENDIX G: PARTICIPANT FEEDBACK DETAILS 45

This page is intentionally blank

SECTION 1: WORKSHOP SUMMARY

A Cybersecurity Workshop was held on December 7, 2017 to engage participants from private, public, and non-profit organizations in information sharing and discussions on reporting cyber incidents as well as the development of a volunteer Cyber Reserve Corps. The workshop was funded by a grant from the Department of Homeland Security and administered through Washington State Region 6 Critical Infrastructure Workgroup.

Subject matter experts spoke to a varied group of participants about reporting cyber incidents and types of resources available to public and private sector organizations. Cyber insurance was also introduced and a presentation regarding the cyber-attack on a private shipping company from the Coast Guard's perspective were well received. Afternoon speakers focused on cyber response groups including those available through the National Guard and a volunteer group established in the State of Michigan. The room was arranged to include round tables for participants who were joined by speakers and they discussed a series of questions regarding reporting strategies.

95% of participants who turned in feedback forms rated this workshop as very good or excellent. Common remarks to the question "What, if any, was the most valuable "take away" or insight you gained from today's discussion?" were grouped into the following areas:

A. Multiple avenues to report cyber incidents
B. Participants like to hear of real life incidents and lessons learned
C. Need SOPs, resource, and contact lists for reporting cyber incidents

One of the important areas acknowledged by participants of this workshop was that the pace of activities including breaks and lunch provided an opportunity to meet people from different disciplines and organizations and encouraged information sharing in an informal setting. Continuing to work toward development of a Cyber Reserve Corps was also acknowledged by participants as an area that required further development.

Recommendations were based on participant feedback forms as well as recommendations from previous cyber workshops and include:

- Develop reporting protocols
- Develop a cyber reserve corps plan
- Product development during workshops

SECTION 2: BACKGROUND

Since 2010, WA Homeland Security Region 6 Critical Infrastructure Working Group has participated in development of exercises and workshops held in the Puget Sound Region that focus on cybersecurity interdependencies to encourage the development of public-private cyber partnerships. Ranging from seminars and workshops to games and functional exercises,

the Emerald Down exercises have brought together hundreds of stakeholders and have contributed to the development of many regional coordination and planning activities. Through networking at these events, individuals became familiar with the capabilities of other organizations, built relationships with individuals, and developed trust. These valuable relationships have helped this Region become a recognized leader in cybersecurity planning and have led to several initiatives to improve cyber resilience. A state cyber annex was developed with input from past Emerald Down participants and a regional coalition was comprised of volunteer public and private cyber professionals called Cyber Incident Response Coalition and Analysis Sharing (CIRCAS).

The *Emerald Down Cyber Exercise Series* findings and recommendations are incorporated into the Region 6 Critical Infrastructure Protection Committee work plan, and are intended to assist Puget Sound organizations to improve their cybersecurity response plans. A recap of these recommendations can be found in Appendix C.

Presidential Policy Directive (PPD) #41, United States Cyber Incident Coordination - July 2016 provides principles governing the Federal Government's response to any cyber incident, whether involving government or private sector entities. Throughout this document, there are references to Significant Cyber Incidents which are more severe than Cyber Incidents. The following definitions are identified in PPD 41.

Cyber Incident - 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.

Significant Cyber Incident - A cyber incident that is (or group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.

SECTION 3: WORKSHOP DESIGN

Working with a core group of individuals from federal, state, and local government as well as the private sector, the design team identified the purpose, scope, target audience, and objectives of this workshop.

Several members of the design team participated in the design and execution of previous cybersecurity workshops and exercises. Design team members included:

A. Design Team

First	Last	Organization
Barrett	Adams-Simmons	Department of Homeland Security
Keifer	Atkins	Puget Sound Blood Center
Brandon	Hardenbrook	PNWER
Mary	Hobday	Puget Sound Energy
Eric	Holdeman	PNWER / CRDR
Scott	Klauminzer	Tacoma Power
Elizabeth	Klute	Amtrak
Rob	Lang	WA EMD
Dana	Lockhart	Department of Homeland Security
Dave	Matthews	DRMatthews, LLC
Matt	Modarelli	Washington Military Department
Steve	Myers	PNWER
Tommi	Robinson	Aronson Security
Jodie	Ryan	T-Mobile
Selena	Tonti	Port of Seattle
Ron	Watters	Department of Homeland Security
Nate	Weigel	PNWER
Sheree	Wen	Deputy Mayor, City of Medina

B. Administrative Details

Type of Exercise: Workshop

Date: December 7, 2017

Duration: 8:30 AM – 3:30 PM

Location: DoubleTree Suites Seattle Airport – Southcenter
16500 Southcenter Parkway
Seattle, WA 98188

C. Purpose

Workshops are a good forum for participants to meet others not only in their industry but also those who work in other disciplines. This workshop was designed to capitalize on networking opportunities through interaction at individual tables as well as through a working lunch and sufficient breaks. Primary discussion areas of this workshop addressed two recommendations from the Emerald Down V exercise conducted in February 2017:

1. Cybersecurity reporting and information sharing protocols, and
2. Volunteer resources in cyber-response.

D. Core Capabilities

- ***Planning*** – All mission areas – 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.
- ***Cybersecurity*** – Mission area is Protection - Protect (and if needed, restore) electronic communications systems, information, and services from damage, unauthorized use, and exploitation.
- ***Operational Coordination*** – All mission areas – 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.
- ***Situational Assessment*** – Mission area is Response - Provide all decision makers with decision-relevant information regarding the nature and extent of the hazard, any cascading effects, and the status of the response.
- ***Intelligence and Information Sharing*** – Mission areas are Prevention and Protection - Provide timely, accurate, and actionable information resulting from the planning, direction, collection, exploitation, processing, analysis, production, dissemination, evaluation, and feedback of available information concerning physical and cyber threats to the United States, its people, property, or interests; the development, proliferation, or use of WMDs; or any other matter bearing on U.S. national or homeland security by local, state, tribal, territorial, federal, and other stakeholders. Information sharing is the ability to exchange intelligence, information, data, or knowledge among government or private sector entities, as appropriate.

E. Objectives

1. Explain and discuss with workshop participants, the concept of the Washington State Cyber Reserve Corps. This objective supports Core Capabilities of Planning, Cybersecurity, and Operational Coordination.
2. Enhance resiliency to cybersecurity incidents through discussion of cyber incident reporting, protocols, and available regional resources. This objective supports all five Core Capabilities cited in Section D.
3. Strengthen partnerships between local, county, state, federal, and private sector partners. The objective supports Core Capabilities of Planning and Operational Coordination.
4. Encourage networking among public and private sector stakeholders to identify interdependencies before a disaster. This objective supports all five Core Capabilities cited in Section D.

F. Participation

143 individuals signed up to attend the Cybersecurity Workshop and over half attended from a variety of organizations with many different job titles. Tribes, military, federal, state, local government, and special purpose districts were represented as were large and small businesses, non-profit organizations, self-employed individuals, and those in education.

Examples of the disciplines represented include:

- Healthcare
- Information Technology (IT)
- Emergency Management / Homeland Security
- Law Enforcement / Security
- Fire
- Transportation
- Communications
- Education

SECTION 4: SPEAKERS AND DISCUSSION

Eric Holdeman, Director, Center for Regional Disaster Resilience, welcomed participants and talked about the history of previous cybersecurity workshops since 2010. He oriented participants to the facility, initiated introductions from each participant, and reviewed the day's agenda (Appendix A).

A. Welcoming Remarks

Walt Hubbard, Director of King County Emergency Management Division, stated that this is the sixth cybersecurity workshop or exercise that King County Emergency Management, Critical Infrastructure Workgroup has sponsored. Citing several cybersecurity events in recent years, Mr. Hubbard emphasized King County's commitment to these events to help educate participants and strengthen relationships among those impacted by cyber attacks.

Representative Zack Hudgins represents the Washington State 11th Legislative District and talked about the need for balancing transparency with risk. Sometimes sharing too much or sensitive information increases vulnerability.

Eric Holdeman reviewed recommendations from the Emerald Down V exercise held in February 2017. Those addressed during this workshop include:

- Coordinate the development and enhancement of cybersecurity plans and procedures,
- Capitalize on the opportunity to leverage volunteer resources in cyber-response,
- Region 6/King County should continue annual Cybersecurity Workshops, and
- Develop cybersecurity reporting and information sharing protocols

B. Cyber Incident Reporting

Cyber Incident Reporting Methods – A Local Perspective

Ralph Johnson, Chief Information Security & Privacy Officer for King County Department of Information Technology moderated a panel of representatives from three different organizations. They addressed specific questions regarding the reporting of cyber incidents.

Panelists:

1. Rob Lang, Cyber Security Manager, Washington State Military Department
2. Natalie Stice, Homeland Security Coordinator, Pierce County Emergency Management
3. Allen Avery, Intelligence Analyst, Cyber and Critical Infrastructure, Washington State Fusion Center

Panel Questions

1. At what point should private sector and governments report a <u>significant</u> cyber incident impacting critical infrastructure?

Cyber incidents that have a wide impact on the population should be reported. These may include those that could cause harm to the national security, economy, public confidence, civil liberties, or public health and safety of people as identified in PPD #41 cited previously.

Lang – Significant cyber incidents that are far reaching and impact state agencies or organizations in multiple counties should be reported through the Washington State

Emergency Management Division Duty Officer. The Duty Officer position is staffed at the State Emergency Operations Center (SEOC) 24 hours a day, 365 days a year. Duty Officers answer calls for reporting of all hazards that could require multi-department or multi-agency coordination.

Stice – Pierce County organizations and businesses can report significant cyber incidents through the Pierce County Emergency Management Duty Officer. A Duty Officer is 'on call' during non-business hours and can receive and make notifications or initiate coordination efforts 24 hours a day.

Avery – WSFC is an information clearing house to accept and distribute information. It can help identify resources and connect organizations with others that may be able to solve problems. The WSFC is not a 24-hour operation.

2. Who should receive the report and when and how should they report it?

Stice – When Pierce County Department of Emergency Management receives notification of a significant cyber incident, they base their response on the type and severity of the incident. Notifications to the public or to government organizations and stakeholder groups may be made through their Alert and Warning system. This system can be activated remotely or manually. DEM will also notify their Regional Intelligence Group (RIG).

Lang – Processes are in place and documented in Washington State Significant Cyber Incident Annex to the Comprehensive Emergency Management Plan (CEMP). Presidential Policy Directive (PPD) 41 also provides guidance. When the State Duty Officer is notified, they contact appropriate experts who determine the next course of action. Based on the severity of the event, the EOC may be opened to assist with coordination in response and recovery. Cyber events are treated the same as other hazards regarding opening the EOC.

Avery – WSFC is there to analyze and share information regarding terrorism incidents including cyber attacks. They don't have resources to address problems but can put agencies or businesses in touch with other organizations that may be affected or who can help.

3. What is the expectation for feedback and support once a significant cyber incident has been reported?

Avery – There may not be any feedback from the WSFC. The information will be accepted, analyzed, and distributed to others.

Lang – Feedback is dependent upon the nature of the incident. It is an area that needs more discussion and development of protocols.

Stice – Feedback is dependent on the situation. A simple notification where the reporting party is handling the situation may be shared with appropriate personnel with no further action taken. If the reporting party is looking for resources to help or needs coordination

support, there would likely be back and forth conversations until the proper resource is found.

4. What coordination and relationship currently exists between the emergency management departments and IT departments?

Stice – Each agency on the surface has very different focus areas which causes silos. There is so much time spent working on different program areas in our separate disciplines that it is difficult to determine the best ways we can identify and work toward common goals.

Lang – State Emergency Management and State IT have similar challenges to Pierce County. Departments have different priorities.

Avery – Interdependencies among disciplines are important. A cyber event can have cascading impacts that affect multiple organizations and disciplines.

5. What is the process for activating the EOC and how does it play a role in cyber events?

Ralph Johnson stated that there have been several attacks by ransomware across the country. Some organizations choose to pay while others wipe their servers clean and rebuild the databases. When taking the approach to rebuild database, it takes time. Example cited was Mecklenburg, NC who had 48 servers impacted. If a similar incident were to occur in our region, the loss of connectivity would impact most if not all departments within the organization. In addition, other agencies who depend on connectivity with the county would also suffer cascading impacts. This link to a National Association of Counties (NACo) article describes the Mecklenburg, NC incident. http://www.naco.org/articles/mecklenburg-county-refuses-pay-ransom-cyber-hackers

Stice – Pierce County DEM would provide the EOC for coordination with impacted agencies and organizations. Activation of the EOC is based on the need to coordinate activities as well as the complexity of the incident.

Lang – State would support activities at local jurisdictions and would coordinate state level activities. In addition, State EMD is the local jurisdictions' avenue to request federal resources. Activating the State EOC is based on the severity and complexity of the incident.

Avery – WSFC would support by helping to find subject matter experts that could assist local or state EOCs. They may send a representative to the State or Local EOC depending on the circumstances.

Questions or Statements from Participants

Question – How does the education system fit in to cybersecurity planning?

At this point the focus is on life line providers and there hasn't been a focus on other disciplines.

Comment – A reminder to folks to remember the Multi-State Information Sharing and Analysis Center (MS-ISAC).

The Center for Internet Security's MS-ISAC is a collaborative state, local, territorial, and tribal (SLTT) government-focused cybersecurity organization, bolstering SLTT capacity and network defense capabilities against cyber threats. The MS-ISAC provides a centralized forum for information sharing on cyber threats between the federal government and SLTT governing bodies through a number of crucial services, while providing opportunities to analyze and correlate information among SLTT members. Funded by the DHS Cybersecurity & Communications Office, the MS-ISAC has been designated by DHS as the cybersecurity ISAC for SLTT governments. Operationally, the MS-ISAC is a mechanism for cybersecurity coordination with SLTT governments. For more information, check the website. https://www.cisecurity.org/ms-isac/

REPORT SIGNIFICANT CYBER INCIDENTS

Washington State Duty Officer - 800-258-5990 (24 hrs)

Pierce County Duty Officer - 253-798-7470 (24 hrs)

Washington State Fusion Center - 877-843-9522 (M-F)
Intake@wsfc.wa.gov

Washington State Fusion Center (WSFC)

Allen Avery talked about the role of the WSFC which is also referenced as the Fusion Center in this report. As a Cyber and Critical Infrastructure Intelligence Analyst, he is responsible for identifying, collecting, analyzing, and disseminating actionable information related to cyber and critical infrastructure threats in Washington State. Allen emphasized that the Fusion Center is staffed Monday through Friday during business hours and is not a 24-hour, 7 day a week organization.

The Fusion Center works with many government agencies as well as organizations from the private sector. Examples include: Washington State Patrol, Federal Bureau of Investigation, MS-ISAC, University of Washington, and local and tribal organizations.

Currently, the WSFC produces and distributes cyber bulletins and situational awareness products with actionable intelligence that are geared towards the information technology and information security audiences. WSFC's focus is on domestic cyber intelligence topics as they relate to regional stakeholders and vetted partners. There are times when the Fusion Center becomes aware of a compromised site, staff reach out to the site administrator to provide them information on the compromise. If the organization compromised is outside of Washington State, the Fusion Center of that state or region is also notified.

Products and alerts generated from the Fusion Center do not identify compromised organizations, but do address threat information, indicators, and origins. WSFC receives notification of or requests for resource coordination for the following situations:

- Phishing attempts
- Ransomware attacks
- DDoS/Degradation in service
- Known intrusions
- Business email compromise
- Anything that can be shared

The Fusion Center is developing a Cyber Liaison Officer program. The program is scheduled to be deployed in the first quarter of 2018 and it will be similar to the current Field Liaison Officer (FLO) program. It includes partner engagement, training, Indicators of Compromise (IOC), and other components.

The WSFC can be reached at (877) 843-9522 or intake@wsfc.wa.gov.

Federal Reporting Portal and Response Protocol

Speakers Ron Watters, Cyber Security Advisor, Department of Homeland Security (DHS) Region X, and A. Barrett Adams-Simmons, Regional Sector Outreach Coordinator, Department of Homeland Security, Region X, talked about the federal reporting portal identified in the Cybersecurity Information Sharing Act of 2015 (CISA 2015). Through this Act the DHS's National Cybersecurity and Communications Integration Center (NCCIC) is designated as the central hub for the sharing of cyber threat indicators and defensive measure between the private sector and the Federal Government. One of the tools used is through Automated Indicator Sharing (AIS) which allows DHS to leverage machine-to-machine communication to rapidly share cyber threat indictors and defensive measures. CISA 2015 grants liability protection and other protections to companies that share indictors through AIS. It also ensures privacy, civil liberties and compliance protections including the protection of personally identifiable information (PII). Cyber incidents that could jeopardize the confidentiality, integrity or availability of digital information or information systems that could result in significant damage are of concern to the Federal Government. Cyber incidents that should be reported include those that:

- Result in a significant loss of data, system availability, or control of systems;
- Impact a larger number of victims;
- Indicate unauthorized access to, or malicious software present on, critical information technology systems;
- Affect critical infrastructure or core government functions; or
- Impact national security, economic security, or public health and safety

Additional information on the NCCIC and AIS is available in ***Appendix E: WEB Links.***

C. Lessons for the Maritime Community

Lieutenant Commander Eileen Beck, U.S. Coast Guard was the lunchtime keynote speaker. She described the Coast Guard's role and observations of a cyber ransomware attack. The information below is taken from her slide presentation.

"The USCG has the primary responsibility for the safety, security, and environmental protection of the maritime domain, including enforcing customs and immigration laws at sea, managing the responses to incidents impacting the Federal navigable waters and ports, and coordinating and expediting the recovery of maritime transportation system." (PPD-21)

Maersk - APM Cyber Incident

June 27, 2017, Maersk/APM shipping company suffered a global operations attack from the Petya Ransomware malware.

- NRC/NCCIC reports received from APM **New York** and **Florida** @ **0730**
- NRC/NCCIC report received from Maersk Norfolk Comms office @ **0810**
- NRC/NCCIC report received from APM facility in **Mobile**, AL @**1100**
- Contact with APM facilities in **Los Angeles** and **Tacoma** indicate mandatory shutdown of all systems and company phones @ **1125**
- First media reporting of Petya began @ **1235**
- +70 hours – CG-FAC makes contact with Maersk CISO for Americas –Charleston SC
- Containers and cargo docs being done manually for 10 days.
- Backend Technologies with company in disarray for 6 weeks
- CG conducted 3 Hot washes of the event to create an extensive Lessons Learned document, and have already enacted 5 significant changes/updates as a result

---

Lessons Learned

- Patched /updated systems are still vulnerable to Cyber attacks. (Malware distributed through a Ukrainian accounting/filing tax software MeDoc; backdoor into the network software- automatic updates)
- Global supply chain: Ensure suppliers are accountable. Think NIST CSF 1.1
- Printed storage of key contacts is a MUST
- Review your system architecture: What systems are going to be unavailable during an extended outage. (i.e. VOiP [phone], Security, Access Control Systems, etc.)
- Consider internal system (server or data center) shutdown procedures. Safe shutdowns = easier restoration. Extreme shutdowns = Days of rebuilding production equipment
- Importance of timely voluntary reporting to NCCIC, NRC

Best Practices

- Fast Isolation: Quickly identified the lateral movement vector of Petya, and made the decision to shut down their entire global system
- Restoration Plan: High TEU [container] facilities first, minimize global supply chain disruption
- Communicate with CG and Maritime Partners: APM provided continual updates on physical cascading effects of the facility to avoid commerce delays
- System Architecture: Vessels [such things as navigation] were protected by being on entirely separate network

---

Impacts

- Business losses ~$700M!
- Copenhagen Stock Exchange trading began selling off into the early stages of the event, but gained neutral territory over the following 48 hours.
- Favorable reputation has remained consistent to date
- Maersk will continue to be a key case study in Maritime Cybersecurity
- Wake up call for Global Maritime community in how it addresses Cyber Risk Management overall

---

D. Cyber Insurance

Insurance to help protect organizations from losses as the result of cyber disruptions is a cost of doing business that must be considered. Anne Shackelford, Vice President, Public Entity Practice Group, Alliant, and Doug Selix, Washington State Department of Enterprise Services spoke about the growing market of cybersecurity insurance policies. Policies vary and are available for small business as well as large business. Anne talked about things to consider when shopping for insurance. She emphasized that buyers must read the policy as coverage varies and policies often come with exclusions. Be mindful of policy terms and conditions.

Alliant Insurance cybersecurity policies include breach security resources that include access to legal experts, forensics expert to determine the cause of the breach, and other services. Security breaches handled by Beazley Breach Response Services Unit have more than doubled since 2014 when over 800 incidents were handled to 2016 with more than 2,000.

Doug talked about cybersecurity policies from the Washington State Department of Enterprise Services perspective. He cited three breaches that occurred since 2014 that impacted public agencies. Even a small insurance policy provides access to resources such as legal, notification and credit monitoring, and forensic investigation support. As cybersecurity breaches become

more common and impacts widespread, it is important that risk management and IT professionals work together with other disciplines during incident response planning.

E. Cyber Reporting – Table Discussions

Participants seated at different tables came from a variety of disciplines and organizations including the public and private sectors, non-profit organizations, and education. The comments below are not attributed to any individual or organization and are summaries of various statements recorded by participants. Internet links are provided at the end of this section that might be useful in verification or additional information regarding comments stated in this section.

1. **What internal reporting procedures or processes do you have in place today?**

   Internal notification processes include:

   - Notify the IT service/help desk via email, telephone, or internal website – reporting tools in place may be developed in-house or by a vendor
   - Notify Security or the Cybersecurity Officer
   - Phishing – awareness training is in place for employees, reminders are sent periodically
   - Report to IT management, impacted departments, and top management

   External notification processes include:

- Contact government office if public is at risk
- Contact impacted organizations
- Share information with trusted partners
- Contact Washington State Fusion Center (WSFC) and/or local law enforcement
- Contact local and/or state emergency operations center
- Other agencies that might be notified depending on the situation include: Department of Defense (DOD), Coast Guard, Army Corps of Engineers, and National Cybersecurity and Communications Integration Center (NCCIC)

Other things to consider

- Enforcement of reporting policies
- Forensics and analysis of the incident
- Develop and document policies and procedures including security protocols – train employees
- Ensure that communications are two-way

2. What, if any, regulatory barriers are there to sharing cybersecurity information outside of your organization or infrastructure sector?

- Some data is federally protected (Ex. HIPPA laws).
- There are few explicit regulatory barriers but there are some cultural barriers. Some utilities may have discipline specific protocols that limit information sharing.
- Concern that private sector reports to the NCCIC may be reported to the FCC which could result in additional regulatory action.
- Analysis of information should focus on the threat and include redacting information per guidelines in the Freedom of Information Act (FOIA).
- For public agencies, there are no real barriers to reporting to Department of Homeland Security (DHS). For private companies with global operations, there are some country specific requirements that must be vetted by legal.
- DHS, Fusion Center, law enforcement agencies, and others may have requirements that limit the types of information to be shared.

3. What trust issues must be overcome to allow you to share cybersecurity information with other organizations?

a. Private Sector

b. Public Sector

Public Sector Trust Issues	Private Sector Trust Issues
Need to empower internal staff	Slow to update software
Concerns that the information shared is not used inappropriately	Shared information may impact the company's reputation
Disciplines such as law enforcement may hold on to information to protect investigations	When a company is named in a public presentation, competitors may use negatives stated to bash the company – loss of customers, business competition
The possibility of FOIA requests may reduce the amount of information shared to reduce exposure	Trade secrets may be exposed
Both	
Cultural or historical barriers may impede progress. "Why should we share this information?" History of a one-way street of information	
The reputation of an organization may be negatively impacted if an attack or breach is made public	
Need legal authority to share information and ensure safeguarding of information shared	
Some public and private sector organizations may work in silos which reduces the opportunity to build trust throughout the organization	
Some organizations tend to stay within their discipline and limit sharing to impacted organizations in other disciplines	
Security clearances and concerns can cause trust issues	

Some tables offered suggestions about how to build trust. They include:

- Develop relationships pre-incident through planning integration, training, and exercises.
- Ensure that laws, policies, and procedures are followed.
- Find opportunities to work outside of silos, across organizations and disciplines.
- Encourage interaction among staff from different departments and organizations.

4. To which organization do you prefer reporting cybersecurity intrusions?

a. Local law enforcement
b. FBI
c. Secret Service
d. U.S. Attorney's Office
e. Washington State Fusion Center
f. Local Emergency Management Agency
g. State Emergency Management Agency
h. Other

The most popular answers to this question were:

- FBI
- DHS
- Fusion Center

Other responses included:

- Federal – FCC, MS-ISAC, Secret Service
- State and Local – emergency management, law enforcement
- Whoever can expedite and assist depending on nature of incident

5. What do you think the criteria should be for reporting cybersecurity intrusions? What should the threshold be for reporting incidents?

- Life safety, loss of Personally Identifiable Information (PII), financial loss, incidents affecting public or third parties
- Anything that impacts public safety
- Develop a risk scale to be used for reporting high risk intrusions –list low risk separately
- Generate weekly reports of intrusions
- If your organization is overwhelmed and can't manage the incident with your own resources
- Inter-band attacks require private regulating
- A wide swath of industries or victims were targeted
- Ransomware attack if the intrusion will affect or impact other agencies
- Legal or industry reporting requirements

F. Cyber Civil Support Team Initiative

Citizens corps are utilized for various jobs during disasters. This concept is now being explored for cyber security events. This session was intended to educate participants and initiate discussions on some aspects of developing a volunteer group in Washington State that could

assist with cybersecurity disruptions in the public and private sector. The session was moderated by Jodie Ryan with T-Mobile Corporate Information Security who introduced the first speaker, Colonel Kelly Hughes, Washington Air National Guard (WANG). Colonel Hughes is currently assigned as the senior cyber advisor to the Joint Force Commander, Washington National Guard.

Colonel Hughes described the role of the Washington National Guard during disasters and explained the difference between federally directed missions under United States Code, Title 10, and state directed missions under Title 32. The National Guard has in place a dedicated 10-person cyber team that trains and exercises together and is available to respond to incidents when required. The Cyber Civil Support Team Initiative would supplement resources available and would:

- Provide the connective tissue that does not exist today with Federal and DoD Cyber command and operations centers for the state.
- Build resilience through joint training, system hardening and regular local interaction
- Serve to provide Mission Assurance of our DoD forces stationed within the borders of Washington to secure the 85% of the critical infrastructures they depend on but do not control.

Ray Davidson PhD, Program Manager, Office of the CSO, Michigan Cyber Civilian Corps (MiC3), spoke about a volunteer cyber group in the State of Michigan. Michigan Public Act 132 of 2017 is the "Cyber Civilian Corps Act", or the MiC3 program, which authorizes the Department of Technology, Management and Budget (DTMB) to appoint individuals with cybersecurity expertise to respond and assist individuals or entities experiencing a cybersecurity incident. The bill creates a process by which DTMB would deploy members to respond to cybersecurity incidents and requires volunteers to undergo a criminal history and records check.

Ray's Linked In page describes the group: "The Michigan Cyber Civilian Corps (MiC3) is a group of trained cybersecurity experts who volunteer to provide expert assistance to enhance the State's ability to rapidly resolve cyber incidents when activated under a Governor declared State of Emergency. The group includes volunteers from government, education, and business sectors."

This mutually beneficial relationship serves team members by:

- Sponsoring training and certification opportunities for volunteers through MiC3;
- Enhancing professional relationships through networking with other IT security professionals during training, exercises, and events;
- Providing needed service to state government during times of cyber emergencies.

By providing support for their employees who are members of MiC3, their employees develop relationships with other cyber professionals, learn about other businesses and state processes that could be beneficial to the company, and support public service through volunteering.

Following the presentations, three questions were posed to each table for discussion.

1. What would your expectations be if you called on the cyber reserve corps for help? Would you call for help? At what point during an incident would you request help from the reserve corps?
2. How do we create a sustainable funding/management model for a cyber reserve corps? Is there a governing body that exists already or is it an entity that needs to be created?
3. What legal frameworks are currently in place to support a cyber reserve corps? What new frameworks need to be created (i.e. new legislation agreements, etc.)? What legal barriers exist (i.e. privacy of vulnerability data concerns over liability etc.)

Due to a loss of participants at the end of the day, there were not enough comments recorded to address these questions.

SECTION 5: EVALUATION

Evaluation of this workshop is primarily based on information gathered from Participant Feedback forms provided to individuals. Questions and forms are summarized below with more detailed input provided in Appendix G.

A. Participant Feedback Summary

Participant Feedback forms were returned by more than 50% of attendees and they rated the day on a scale of 1-5 with 5 as Excellent and 1 as Poor. 95% of all participants that turned in evaluation forms rated the overall events of the day as Excellent or Very Good. There were no ratings of Poor in any category.

	Excellent - 5	Very Good - 4	Satisfactory - 3	Fair - 2	Poor - 1
Overall Impression of Workshop	14	21	1	1	
Quality of Speakers	20	15	2		
Met Your Objectives	11	23	2	1	
Quality of Discussion	16	19	1	1	

What, if any, was the most valuable "take away" or insight you gained from today's discussion?

- Multiple avenues to report cyber incidents
- Participants like to hear of real life incidents and lessons learned
- Need SOPs, resource, and contact lists

What key "take away" or suggestions do you have regarding reporting protocols for significant cyber incidents?

- Need a single point for notification and resource coordination
- Need protocols for reporting (who, what, when, and how)

Does your organization have a cyber response plan? YES NO If yes, does it include reporting protocols for significant cyber incidents? If you needed support after a significant cyber incident who would you contact outside your organization?

- Many marked yes to a plan, but some indicated the plan was limited to internal issues or was very general with few detailed protocols

Does your organization use cyber insurance? YES NO If yes, what recommendation and advice would you give other organizations looking to purchase cyber insurance?

- Most participants did not respond to this question. Some said they didn't know.

What suggestions do you have for the State of Washington as it works toward the creation of a Cyber Reserve Corps?

- Create incentives such as training, skill building, certifications
- Use the Michigan model or a system already in use in Washington State (Citizen Corps, Emergency Worker Program)

What type of cyber security related legislation would you like to see the Washington State Legislature introduce during the upcoming session?

- Safe harbor act for information sharing. Helping other entities should not cost the reporting organization unless a certain degree of negligence is detected if the incident is reported within a certain amount of time.
- Confidential reporting; protection from public disclosure
- Funding for training, certification, and program development

Please provide any topics for future cyber security discussions and recommendations on how to improve or enhance this type of event.

- More discussion, less pre-scripted panel comments and more Q&A from floor
- Real life incidents, how they were handled, lessons learned
- Develop resource documents or fact sheet handouts
- Subject area topics: cyber insurance, forensics, incident response,
- Continue interaction between private and public sectors, different disciplines, and how cyber disruptions can impact other entities beyond the owner's business

B. Assessment by Objectives

1. **Explain and discuss with workshop participants, the concept of the Washington State Cyber Reserve Corps.**

This objective was partially met. Participants were very interested in learning more about the concept of developing a cyber reserve corps. Presentations by Colonel Kelly Hughes of the Air National Guard and Ray Davidson from the Michigan Cyber Civilian Corps were well received and helped identify some of the challenges of establishing a volunteer corps for cyber incidents as well as how one state is working toward solutions. Several participants left the workshop early before the final table discussions which led organizers to determine that table discussions should be cut short and saved for another day.

2. **Enhance resiliency to cybersecurity incidents through discussion of cyber incident reporting, protocols, and available regional resources.**

This objective was met, and discussion emphasized that there is more work to be done regarding who, what, when, and how to report cybersecurity incidents. This workshop provided more information about local, state, and federal organizations that either perform a role to help resolve cybersecurity compromises or that provide a mechanism for coordinating information or efforts between impacted organizations. There was education provided regarding what happens at the Pierce County Department of Emergency Management as well as Washington State Emergency Management Division when those organizations are notified of a cybersecurity incident. The Washington State Fusion Center explained their capability for helping to find resources, but they are not a response organization for cybersecurity incidents. Federal agencies such as the National Cybersecurity and Communications Integration Center are also available to receive reports regarding cybersecurity incidents. Most organizations, public and private, knew that their Information Technology Department would handle a cyber problem but there seemed to be no protocols in place for notification of other organizations. Work needs to be done in this area to determine common protocols for reporting cyber incidents.

3. **Strengthen partnerships between local, county, state, federal, and private sector partners.**

This objective is addressed during all cyber seminars, workshops, and exercises and is met in increments. Participants were from local, state, and federal agencies as well as large and small businesses and non-governmental organizations. Round tables were mixed and included speakers as well as participants of 8-10 individuals. They spent the day together not only discussing questions provided by workshop organizers but also spent the day together at round tables of 8-10 participants at each with an opportunity to talk among themselves and meet speakers from various organizations.

4. **Encourage networking among public and private sector stakeholders to identify interdependencies before a disaster.**

There were at least two different table discussion sessions which provided an opportunity for participants to build understanding of their tablemate's operations and ultimately encourages trust between individuals and organizations. In addition, a working lunch, and ample breaks with refreshments, provided more informal opportunities for networking with people outside the office.

SECTION 6: RECOMMENDATIONS

Reporting Protocols - Plans and procedures for reporting cybersecurity incidents beyond company or organization parameters are not fully developed though many have some plans in place. The State of Washington Emergency Management Division has written a cyber incident annex that identifies some guidelines for reporting for state organizations. The King County Emergency Management Critical Infrastructure Work Group should consider ways to bring members of the private and public sectors together to develop plans and protocols that answer the who, what, when, and how organizations should report significant cybersecurity incidents. Future workshops should focus on specific processes which could then be developed into a plan and procedures.

Cyber Reserve Corps - Capitalize on the interest shown by persons wanting to work on developing volunteer resources that would be available to help during significant cybersecurity incidents. A work group should develop a plan that includes recruitment, identification of skillsets needed, roles of volunteers, and how they should be managed and motivated. Identify a lead agency to develop a volunteer organization with members that possess appropriate knowledge, skills, and abilities to respond effectively to a cyber incident. Investigate different models of volunteer groups. Also consider various types of mutual aid that might be incorporated into a cyber response.

Product Development During Workshops – This workshop provided several pieces of information and was an excellent opportunity for participants to network, but did not meet the need for defined outcomes. Consider hosting a small facilitated workshop that is focused solely

on developing plans or protocols for reporting significant cyber incidents. A second suggested workshop would be to focus exclusively on the development of a cyber reserve corps. The goals of both workshops would be to walk out the door with agreed upon protocols or next steps in development of the process.

APPENDIX A: WORKSHOP AGENDA

Cyber Security Workshop Agenda

8:30-9:00 Registration and Networking Continental Breakfast

9:00-9:30 Welcome and Introductions

Welcoming Remarks

- Walt Hubbard, Director, King County Office of Emergency Management

Update from Region 6 Critical Infrastructure Working Group

- Elizabeth Klute/Tommi Robison, Co-chair, Region 6 CI Working Group

Recommendations from Emerald Down V

- Eric Holdeman, Director, Center for Regional Disaster Resilience

Introduction of All Participants

Cyber Incident Reporting

9:30-10:30 Cyber Incident Reporting Methods

A Local Perspective At what point should private sector and governments report a significant cyber incident impacting critical infrastructure? Who should receive the report and when and how should they report it? What is the expectation for feedback and support once a significant cyber incident has been reported? What coordination and relationship currently exists between the emergency management departments and information technology departments? What is the process for activating the EOC and how does it play a role in cyber events?

Moderator: Ralph Johnson, CISO, King County

Panelists:

- Rob Lang, Cyber Security Manager, Washington State Military Department
- Natalie Stice, Homeland Security Coordinator, Pierce County Emergency Management
- Allen Avery, Intelligence Analyst, Cyber and Critical Infrastructure, Washington State Fusion Center

10:30-10:45 Break

10:45-11:00 Update from the Washington State Fusion Center

- Allen Avery, Intelligence Analyst, Cyber and Critical Infrastructure, Washington State Fusion Center

11:00-11:15 Overview of Federal Reporting Portal and Response Protocol

- Ron Watters, Cyber Security Advisor, Region 10, Dept. of Homeland Security

11:15-12:15 Tabletop Discussion and Report-out

12:15-1:15 Lunch – Keynote Speaker (30 min.)

- Lieutenant Commander Eileen Beck, U.S. Coast Guard Thirteenth District

1:15-1:45 Cyber Insurance – Panelists

- Anne Shackleford, Vice President, Public Entity Specialty Group, Alliant Insurance Services, Inc.
- Doug Selix, IT Security and Accessibility Officer, State of Washington Department of Enterprise Services

1:45-3:15 Cyber Reserve Corps

Working Session on Washington State Cyber Reserve Corps Concept, Best Practices from Michigan, and Stakeholder Input

Citizens corps are utilized for various jobs during disasters. This concept is now being explored for cyber security events. States and municipalities are developing volunteer citizens corps for resilience from cyber security events. This working session will work through such the concept for Washington State and how it would be implemented, with input from stakeholders and the State of Michigan. Stakeholders will discuss the potential for a working group and next steps to further a Cyber Reserve Corps in Washington.

Moderator: Jodie Ryan, Corporate Information Security, T-Mobile

- Col. Kelly Hughes, Senior IT Security Advisor, Washington State Military Department
- Ray Davidson, Office of the CSO, Michigan Cyber Civilian Corps (MiC3)

3:15 Wrap-up

- Eric Holdeman, Director, Center for Regional Disaster Resilience

3:30 Adjourn

APPENDIX B: SPEAKER BIOGRAPHIES

Walt Hubbard, Director
King County Office of Emergency Management

Walt Hubbard grew up in the Seattle area and has a portfolio of public service that includes emergency preparedness manager for the King County Department of Transportation. While there, he worked to improve the department's all-hazards response, with a special focus on Green River flooding, winter storms, and long-term recovery.

Hubbard also served as director of the Odessa Brown Children's Clinic, where he honed community collaboration skills and his commitment to equity and social justice as an essential part of health care delivery to a diverse population. As special assistant for public safety to Seattle Mayor Paul Schell, Hubbard was directly involved in several emergency events – including the response to the Nisqually Earthquake in 2001 – forming strong relationships with police, fire, and first responders across the region.

Eric Holdeman, Director
Center for Regional Disaster Resilience

Eric Holdeman is a nationally known emergency manager. He has worked in emergency management at the federal, state and local governments. Today he serves as the Director, Center for Regional Disaster Resilience, which is part of the Pacific Northwest Economic Region (PNWER). The focus for his work there is engaging the public and private sectors to work collaboratively on issues of common interest. He is a prolific writer authoring numerous articles for professional journals and opinion pieces for local, regional and national newspapers including the Washington Post. He is a contributing writer and Senior Fellow for Emergency Management Magazine where he writes feature articles and has a regular column, "Disaster Zone." An experienced and accomplished public speaker he is sought after to present at national and regional conferences. Eric has the United States' most popular blog on the topics of emergency management and homeland security at www.disaster-zone.com

Ralph Johnson, Chief Information Security Officer
King County Department of Information Technology (KCIT), Security and Privacy

Mr. Johnson has held the position of Chief Information Security and Privacy Officer for the past 13 years in which he oversees information security and privacy issues for the entire county. In this capacity, he established the information assurance program from policy development, compliance, information risk management, metrics and controls selection, implementation, monitoring and evaluation. Mr. Johnson has been with King County for 28 years serving in multiple IT and management roles.

Mr. Johnson is an Instructor in the Information Security and Risk Management Continuum Program at the University of Washington. He is also a certified instructor for the Holistic Information Security Practitioner Institute course.

Mr. Johnson also serves on the Executive Committee, Product Review Board for the Trusted Purchasing Alliance and is a co-chair of the Education and Awareness Sub-Committee of the Multi State – Information Sharing and Analysis Center (MS-ISAC).

Rob Lang, Cyber Security Manager
Washington State Military Department

Robert Lang is the cyber security manager for the Washington State Emergency Management Division. He reports to the Director of Emergency Management, under the direction of the state Homeland Security Advisor. He serves as Washington State's cybersecurity policy leader and strategist for emergency management. He conducts outreach, collaboration, and integrated policy, planning, and exercise activities with the private, public, tribal, and critical infrastructure/key resource (CIKR) sectors in furtherance of statewide significant cyber incident preparedness. Robert is a retired military officer where he last served as the Chief Information Officer of Madigan Army Medical Center. He holds a Master of Science in Technology Management from George Mason University, and a Federal CIO Certificate.

Natalie Stice, Homeland Security Coordinator
Pierce County Emergency Management

Natalie Stice is the Homeland Security Coordinator for Pierce County Emergency Management. She functions under the Operations Division and conducts operationally-related exercises and readiness activities, grant management, and collaborates with the public and private stakeholders of Pierce County and its neighboring jurisdictions. Natalie previously served as a Firefighter/EMT for 16 years, holds a Bachelor's degree in Emergency & Disaster Management with a minor in Homeland Security, and carries an Associate Emergency Manager certification from IAEM.

Allen Avery, Cyber and Critical Infrastructure Intelligence Analyst
Washington State Fusion Center

Allen Avery is a Cyber and Critical Infrastructure Intelligence Analyst with the Washington State Fusion Center (WSFC) in Seattle, WA. Allen has held his current role with the fusion center for nearly 3 years and is responsible for identifying, collecting, analyzing, and disseminating actionable information related to cyber and critical infrastructure threats in Washington State. Allen also supports the state's Fusion Liaison Officer (FLO) program, is the Geographic Information System (GIS) analyst, and the Call Data Records analyst for the fusion center.

Prior to joining the fusion center, Allen was a Program Analyst for more than eight years with the Transportation Security Administration (TSA) and assigned to the fusion center as the TSA-Liaison. He was also a CyberCorps Scholarship for Service fellow and holds a Master's degree in Infrastructure Planning and Management and a certificate in Information Security and Risk Management from the University of Washington. Allen's email: allen.avery@wsfc.wa.gov

Ron Watters, Cyber Security Advisor

Department of Homeland Security, Region 10

Ron Watters serves as the Region X (WA, OR, AK, ID) Cybersecurity Advisor for the Stakeholder Engagement and Cyber Infrastructure Resilience Division of the Office of Cybersecurity and Communications (CS&C) National Protection and Programs Directorate (NPPD). Based in Seattle, WA, he supports the Department of Homeland Security (DHS) mission of strengthening the security and resilience of the nation's critical infrastructure.

Prior to joining DHS, Ron served 27 years with the U.S. Navy and Naval Reserve as a Submarine Sonar Technician and Diver. Finding not much use for a Submarine Sonar Technician in the Surface reserve Ron utilized his talents as an Intelligence Analyst and was utilized accordingly. Ron retired from the US Navy in 2007. During his active duty Ron completed his Bachelor's degree in Public Administration with Criminal Justice emphasis (Cum Laude). Ron completed his two Master's Degrees in Education (School Administration and Secondary Education) at Loyola Marymount University. He continued his education and achieved certification as a Microsoft Certified Systems Engineer and Microsoft Certified Trainer, in 1998 he was hired as the Computer science department chairman at Chaminade College Preparatory High School in West Hills, CA until he was recalled to Active duty following 9/11. Upon his demobilization he was offered a position as the Deputy Information Systems Management Officer with the 4th Marine Corps recruiting District in New Cumberland, PA. He rose to the position of S-6 before leaving in 2009 to take a position as the Chief, Information Assurance Division, Directorate of Information Management Ft Irwin, CA. Ron remained in that position until he left to become the Branch Manager of the Cybersecurity Branch of the Puget Sound Naval Shipyard in March of 2016. Ron interviewed and was hired as the Region X Cybersecurity advisor in June of 2017 and has filled that position presently.

Ron's computer certifications are numerous to include Microsoft Certified Systems Engineer (MCSE), Certified Novell Administrator (I), GIAC Security Leadership Certification (GSLC), CompTia Security+ CE, and Microsoft Certified Trainer (MCT). In addition to the professional certifications Ron has been awarded numerous Commander's Coins for excellence and received Two Commander's Awards for his work at Fort Irwin.

Lieutenant Commander Eileen Beck

US Coast Guard, Thirteenth District

Native to the Seattle, Washington area, LCDR Eileen Beck graduated from the U.S. Coast Guard Academy in 2004 with a bachelor of science in electrical engineering. After graduation, she reported to Coast Guard Cutter CHASE as a student engineer from 2004 – 2006, then went to Naval Engineering Support Unit, Seattle from 2006 – 2008. While there, she served icebreaker HEALY through a dockside and drydock availability as Port Engineer.

In 2008, LCDR Beck was selected for graduate school and attended Johns Hopkins University. In 2010, she graduated with an M.S. in computer science. The following four years were spent in CG-9, managing C4IT requirements for the OPC from 2010 – 2011, then the acquisition of the HC-144A's C4ISR suite from 2011 – 2014. LCDR Beck traveled back to CGC HEALY as Assistant Engineer Officer from 2014 – 2016, then fleeted up to Engineer Officer from 2016 – 2017. After three and a half deployments to the Arctic, including a trip to the North Pole, LCDR Beck reported to District Thirteen and is currently assigned as the Computer & Communications Division Chief. Eileen Beck is married to Matthew Beck and has three children: Mae (10), Lucy (7) and Ida (5). Contact at Eileen.Beck@uscg.mil

Anne Shackelford, Vice President

Public Entity Specialty Group, Alliant Insurance Services Inc.

Anne joined the Alliant Insurance Services team in 2016. Her 15 years' experience in a wide variety of business segments and a diverse skill set enables her to manage all aspects of a complex insurance program. Prior to joining Alliant, Anne worked for a global retail brokerage servicing a broad array of clients that included public entities, life science and technology companies, manufacturers, not-for-profit organizations, and real estate firms.

Anne entered the insurance profession in 1999 with two large national brokers, moved on to manage a smaller firm focused primarily on commercial real estate (all the while providing Account Executive Support) and then back to a large international firm to head their Small/Medium Enterprise Department.

Anne's momentous growth from an Administrative Professional to a full-time insurance Producer demonstrates her commitment to the industry. She prides herself on maintaining very strong client relationships as well. Her insurance expertise ranges from marine, general liability, cyber, public officials' liability, workers' compensation to property and terrorism and active shooter/workplace violence. Contact at anne.Shackelford@alliant.com

Doug Selix, IT Security and Accessibility Officer

State of Washington Department of Enterprise Services

Doug has been working in IT since 1970. The past 16 years he has been working for the State of Washington. First at the Office of Financial Management as their IT Security Administrator, and more recently at the Department of Enterprise Services as their IT Security and Disaster Recovery Architect. In February 2014 he joined the State Office of Risk Management to head up

their statewide Cyber Liability Program. Doug works with risk managers from state agencies, colleges, and universities to help them understand and manage cyber liability and associated cyber risks. In January 2017 Doug returned to DES IT in the roles of IT Security and Accessibility Officer in addition to working with the state Office of Risk Management.

Colonel Kelly Hughes, Senior IT Security Advisor

Washington State Military Department

Colonel Kelly Hughes is currently the senior cyber advisor to the Joint Force Commander, WA National Guard. He recently returned from duty in Washington DC where he served as the Division Chief for Space and Cyber Forces at the Air National Guard Readincess Center. He was responsible for the resourcing, programmatic support, strategic planning, and operations for all ANG Cyber Warfare, Combat Communications, Engineering and Installation, Communications, and Space Operations Squadrons. He was responsible for the training and operational support of over 9,000 airmen across more than 100 units. This $2B portfolio maintains and operates equipment and facilities in all 54 states/territories to maintain full-spectrum communications and space operations readiness for worldwide deployments and home-station support.

Colonel Hughes received his Aeronautical Rating at Mather Air Force Base, California in 1989. He flew the EC-135 “Looking Glass” Airborne Command Post and the RC-135 “Rivet Joint” aircraft while on active duty at Offutt Air Force Base, Nebraska. He joined the Washington Air National Guard in 1996 where he served in a variety of squadrons as a KC-135 navigator, Air Liaison Officer, Fighter Duty Officer, and finally Cyber Warfare Operations. Over the span of his career he has deployed to combat on three occasions supporting Operations Desert Storm, Enduring Freedom, and a three-year activation for Operation Noble Eagle.

Colonel Hughes is married to Captain (Ret) Marcella Hughes (USAFA 87’), and has two adult children, Sydney and Jake.

Ray Davidson, Program Manager

Michigan Cyber Civilian Corp

G. W. Ray Davidson, PhD, is the former dean of academic affairs for the SANS Technology Institute. He continues to serve as a mentor, subject matter expert and technical reviewer for the SANS Institute and holds several GIAC certifications. Ray started his career as a research scientist and subsequently led global security projects for a major pharmaceutical company. He has taught at the college level and cofounded a security startup. He currently serves as program leader for the Michigan Cyber Civilian Corps.

This page is intentionally blank

APPENDIX C: RECOMMENDATIONS SUMMARY 2010-2017

Item #	Year	Exercise	Recommendation	Actions Taken
2010 – 1	2010	Emerald Down I	Organizations should consider implementing a formal program cycle for developing, training, exercising, and revising Cybersecurity Incident Response Plans.	The Region 6 CIP working group is assisting with this effort through hosting annual cyber workshops and exercises.
2010 – 2	2010	Emerald Down I	Organizations should address policies for both internal and external communications structure for responding to a cyber event. Response organizations should be educated on available tools and resources that can be used during a cyber event in either a seminar or workshop.	As part of Emerald Down V, stakeholders were provided with a draft cyber response plan template for organizations to use or enhance their internal policies.
2010 – 3	2010	Emerald Down I	Individual organizations should identify and train or cross-train possible cyber response team members that could be activated during a large scale cyber event.	This best practice has been noted and is occurring in individual organizations.
2010 – 4	2010	Emerald Down I	Organizations should identify key leadership that can take ownership of responding to and mitigating cyber-event issues.	This best practice has been noted and is occurring in individual organizations.
2010 – 5	2010	Emerald Down I	Local Emergency Operation Centers (EOCs) should review plans on how cybersecurity response efforts are integrated within all hazard incidents and cybersecurity events.	The City of Seattle held a workshop with Information Technology and EOC in 2011 to better inform response.

Item #	Year	Exercise	Recommendation	Actions Taken
2010 – 6	2010	Emerald Down I	Identify how to implement clear legal and regulatory requirements before an incident so that recovery efforts can be prioritized and executed without delay.	Being accomplished in individual organizations, both public and private.
2010 – 7	2010	Emerald Down I	Regional stakeholders need to develop a strategy for improved communications and two-way information sharing on cyber events.	PNWER is working with stakeholders within the maritime transportation system to develop protocols for cyber incident reporting and information sharing. Currently CIRCAS and NWWARN are available resources and could be expanded.
2010 – 8	2010	Emerald Down I	Memoranda of Understanding should be explored between critical service providers and organizations that might be impacted by a cyber event.	This issue was explored further during a recent statewide cyber exercise in 2017.
2012 – 1	2012	Emerald Down II	There is a clear need to develop methods for regional data and resource sharing and communication about the threat environment that formalizes the important trust based network that has developed between information security specialists in the region.	CIRCAS was formed to work toward developing a trusted network of cyber professionals to work to assist in response and recovery.
2012 – 2	2012	Emerald Down II	Organizations need a clearly delineated escalation path in order to access both regional and Federal resources in the event of a major crisis.	PNWER is working with stakeholders to develop a CONOPS for cyber incident reporting in the Maritime Transportation System which will be scalable to include other sectors upon completion.

Item #	Year	Exercise	Recommendation	Actions Taken
2012 – 3	2012	Emerald Down II	Finally, there is an urgent need to develop a common taxonomy about situation severity and response thresholds.	The Washington Military Department and FEMA recently develop ICS/NIMS typing for cyber functions.
2014 – 1	2014	Emerald Down III	The region would benefit on a series of short workshops that outlined the various considerations of different pieces of a cyber plan– for instance, policies for employees. Throughout the series, participants will learn how to build pieces of their plans, ending with an outline for scalable cyber preparedness plans which could be adopted throughout the region.	A cyber response plan template was developed and provided to stakeholders as part of Emerald Down V.
2014 – 2	2014	Emerald Down III	The region has a number of voluntary groups that come together to share best practices and emerging concerns in the field of cybersecurity. These organizations have the institutional knowledge to provide input on a brief best practices and checklist to be distributed to participants throughout the region to help build greater resiliency throughout the region.	CIRCAS, US CERT, Infragard, Agora are a few voluntary groups that share information and work with the WA State Fusion Center.
2014 – 3	2014	Emerald Down III	The Region should continue the tradition of frequent workshops and exercises centered on cyber systems. We recommend that the next such event center on the protection of, response to incidents impacting, and recovery of the physical infrastructure that supports our cyber systems in the region.	The region has agreed to continue to hold annual cybersecurity workshops and exercises to build trust and better understand the interdependencies of the region.

Item #	Year	Exercise	Recommendation	Actions Taken
2015 – 1	2015	Emerald Down IV	Develop a database of resources, including sources of information and templates for planning, for use throughout the Puget Sound	A regional cyber resources website is currently being developed by the Center for Regional Disaster Resilience.
2015 – 2	2015	Emerald Down IV	Integrate cybersecurity with physical security as part of a company-wide security integration	This is occurring in individual organizations.
2015 – 3	2015	Emerald Down IV	Develop a cyber policy, train your employees in it, and develop performance measures around it	Individual organizations are implementing cybersecurity training.
2015 – 4	2015	Emerald Down IV	Identify your mission critical systems and simulate system outages and how to respond	Accomplished in government COOP planning and business continuity plans.
2015 – 5	2015	Emerald Down IV	Develop a functional exercise in the Puget Sound to help test plans and partnerships	The region hosted Emerald Down V Exercise to test plans and partnerships.
2015 – 6	2015	Emerald Down IV	Integrate cybersecurity into all exercises and planning	Being accomplished on a case by case basis. A Cybersecurity Game has been developed and used to increase cybersecurity awareness and make players aware of cybersecurity countermeasures.
2017-1	2017	Emerald Down V	Multi-agency plan development workshops that address coordination issues will benefit agencies in both the private and public sectors.	Follow-on Emerald Down Workshops have address these coordination issues.
2017-2	2017	Emerald Down V	Organizations should identify and develop procedures that support plans and improve the ability of organizations to respond and recovery quickly from cyber disruptions.	This is occurring in individual organizations.

Item #	Year	Exercise	Recommendation	Actions Taken
2017-3	2017	Emerald Down V	Capitalize on the interest shown by persons wanting to work on developing volunteer resources by following up with them to establish a work group to refine how volunteers can be used during cyber incidents.	Working group developed and workshop conducted in 2017 which brought the cyber reserve corps lead from Michigan to share information and best practices.
2017-4	2017	Emerald Down V	Keep the interest in cybersecurity including response and recovery to significant cyber incidents by continuing to bring cross-jurisdictional and multi-disciplinary groups together through annual Emerald Down workshops and tabletop exercises.	Region 6 Critical Infrastructure Workgroup has continued to host annual Emerald Down Workshops.
2017-5	2017	Emerald Down V	In future events, engage in more discussion on the impacts to business operational processes through response and recovery. Connect disaster recovery with business continuity planning and response.	March 2018 Blue Cascades VII will focus on Recovery after a major disaster
2017-6	2017	Emerald Down V	Work with local, state and federal leaders to develop reporting and information sharing protocols to ensure all levels of government are informed. Likewise, develop protocols for identifying specific events that should trigger an organization to report an incident. These could be developed by sector with industry specific stakeholders.	PNWER is working with DHS to develop a maritime cyber reporting CONOPs for the Puget Sound region.

Item #	Year	Exercise	Recommendation	Actions Taken
2017-7	2017	Cybersecurity Workshop	The King County Emergency Management Critical Infrastructure Work Group should consider ways to bring members of the private and public sectors together to develop plans and protocols that answer the who, what, when, and how organizations should report significant cybersecurity incidents. Future workshops should focus on specific processes which could then be developed into a plan and procedures.	Workshop planned for March 2018 to begin to develop protocols for reporting.
2017-8	2017	Cybersecurity Workshop	Capitalize on the interest shown by persons wanting to work on developing volunteer resources that would be available to help during significant cybersecurity incidents. A work group should develop a plan that includes recruitment, identification of skill-sets needed, roles of volunteers, and how they should be managed and motivated.	The CI working group will explore developing this recommendation in the near future.
2017-9	2017	Cybersecurity Workshop	Consider hosting a small facilitated workshop that is focused solely on developing plans or protocols for reporting significant cyber incidents. A second suggested workshop would be to focus exclusively on the development of a cyber reserve corps. The goals of both of these workshops would be to walk out the door with agreed upon protocols or next steps in development of the process.	A survey and workshop on this topic are being developed for early 2018 as part of the Maritime transportation cyber resilience initiative.

APPENDIX D: ACRONYMS

AAR	After Action Report
AIS	Automated Indicator Sharing
CRDR	Center for Regional Disaster Resilience
CEMP	Comprehensive Emergency Management Plan
CIRCAS	Cyber Incident Response Coalition and Analysis Sharing
CISA	Cybersecurity Information Sharing Act of 2015
DOD	United States Department of Defense
DHS	Department of Homeland Security
EMD	Emergency Management Division
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
FTC	Federal Trade Commission
HIPPA	Health Insurance Portability and Accountability Act
IC3	Internet Crime Compliant Center
IOC	Indicators of Compromise
IT	Information Technology
MS-ISAC	Multi-State Information Sharing and Analysis Center (MS-ISAC)
MiC3	Michigan Cyber Civilian Corps
NACo	National Association of Counties
NCCIC	National Cybersecurity and Communications Integration Center
NIMS	National Incident Management System
PII	Personally Identifiable Information
PPD	Presidential Policy Directive
PNWER	Pacific Northwest Economic Region
RCW	Revised Code of Washington
SLTT	State, local, territorial, and tribal
SSA	Social Security Administration
UCG	Unified Coordinating Group
US-CERT	United States Computer Emergency Readiness Team
VoIP	Voice over Internet Protocol
WAC	Washington Administrative Code
WSFC or Fusion Center	Washington State Fusion Center

APPENDIX E: WEB LINKS

- Multi-State Information Sharing and Analysis Center (MS-ISAC) https://www.cisecurity.org/ms-isac/
- Department of Homeland Security, National Cybersecurity and Communications Integration Center (NCCIC), https://www.us-cert.gov/nccic
- DHS, NCCIC Automated Indicator Sharing (AIS) www.us-cert.gov/ais.
- Federal Communications Commission, Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security Bureau https://www.fcc.gov/cybersecurity-and-communications-reliability-division-public-safety-and-homeland-security-bureau
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html
- Freedom of Information Act (FOia) https://www.foia.gov/

APPENDIX F: PARTICIPANT FEEDBACK FORM

Region 6 CIWG: Cybersecurity Workshop
ATTENDEE FEEDBACK FORM
December 7, 2017
DoubleTree Southcenter, Seattle, WA

Overall impression and general comments on the Exercise- **Please rate each component on a scale of 1-5 (5 being excellent /valuable; 1 being not valuable)**

Exercise	Excellent	Very Good	Satisfactory	Fair	Poor	N/A
Overall Impression of Exercise	5	4	3	2	1	N/A
Quality of Speakers	5	4	3	2	1	N/A
Exercise Format	5	4	3	2	1	N/A
Quality of Discussion	5	4	3	2	1	N/A

1. What type of organization do you represent? (e.g., Education; Emergency Services; Law Enforcement; Energy; Local, County, State, Federal Government, Private Sector and type of business, etc.)

2. What, if any, was the most valuable "take away" or insight you gained from today's discussion?

3. What key "take away" or suggestions do you have regarding reporting protocols for significant cyber incidents?

4. Does your organization have a cyber response plan? **YES NO** If yes, does it include reporting protocols for significant cyber incidents? If you needed support after a significant cyber incident who would you contact outside your organization?

5. Does your organization use cyber insurance? YES NO If yes, what recommendation and advice would you give other organizations looking to purchase cyber insurance?

6. What suggestions do you have for the State of Washington as it works toward the creation of a Cyber Reserve Corps?

7. What type of cyber security related legislation would you like to see the Washington State Legislature introduce during the upcoming session?

8. Please provide any topics for future cyber security discussions and recommendations on how to improve or enhance this type of event.

9. Would you be interested in joining the Cyber Reserve Corps? YES NO

10. Would you like to be included in future cybersecurity events? YES NO

Optional:

Name:
Title:
Organization:
Email:

Thank you for your feedback. Please return this form to the organizers as you leave or email Nate.Weigel@pnwer.org

APPENDIX G: PARTICIPANT FEEDBACK DETAILS

The feedback form asked participants additional questions. Some comments that carried a similar message have been consolidated and summarized below.

2. **What, if any, was the most valuable "take away" or insight you gained from today's discussion?**

- Several participants felt that scenarios of real incidents and how they were handled was interesting and beneficial for their purpose.
- Currently there are multiple avenues of reporting cyber incidents. There is a desire to develop a single point of contact for reporting cybersecurity.
- The private sector as well as public sector can access some government resources and services.
- It is important for all organizations to develop written policy and procedures before an event as well as fact sheets and contact lists that are easily accessible during cyber incidents.
- Identification of thresholds for reporting and clearly defining Significant Cyber Incidents was useful as organizations develop reporting protocols.
- The cyber threat is not limited to computer terminals and company networks but can have cascading effects on other organizations and even the general public.
- The presentations regarding cyber insurance, the Washington State Fusion Center, National Guard cyber response, and DHS Cybersecurity provided information that was cited on several forms.
- Networking with people from different organizations and disciplines was highlighted by attendees as being valuable for professional development and future cyber activities.
- The continuing challenge of balancing transparency with privacy and organization concerns regarding the sharing of sensitive information remains a hurdle for establishing reporting standards.
- It is important to establish and maintain communications links among business, non-government organizations, and government agencies.
- Several participants appreciated the Cyber Reserve Corps concept and feel that continuing work in that area is important.
- Third party vendor vulnerability was identified as an area that some had not considered.
- Public and private entities have similar issues and resource limitations. There is a need to develop a coordinated plan.

3. **What key "take away" or suggestions do you have regarding reporting protocols for significant cyber incidents?**

- Need a better understanding of legal requirements for cyber incident reporting
- Sharing information is critical

- Need a single point of contact for reporting incidents or for seeking resources that is a trusted entity (ex: 911, Fusion Center).
- Reduce the number of agencies who would receive reports.
- Need a way to overcome internal reluctance to share national, sensitive information with regional partners
- Coming to consensus on reporting protocols should be a priority
- Check to see what Michigan is doing and follow their lead
- Need to have better notification processes
- Create an anonymous, secure platform for reporting to reduce concern of private sector reporting
- Engage the WSFC more frequently
- It seems like large business understands who to notify and when, but smaller businesses may not
- Create a process for reporting that can be followed consistently. Consider an on-line portal for reporting incidents.
- Awareness of resources (agencies)
- Develop reporting protocols for public agencies. Build a process before an incident to keep from having to address issues on the fly. Private organizations may be reluctant to share cyber incident information

4. **Does your organization have a cyber response plan? YES NO If yes, does it include reporting protocols for significant cyber incidents? If you needed support after a significant cyber incident who would you contact outside your organization?**

Of the participants that answered this question, three times as many responded that they had a plan vs. those that don't. Comments are below.

- There is internal and external reporting within the maritime domain – no reverse notification – plan addresses internal reporting
- Very generic with few detailed protocols
- WSFC, DHS
- FBI or others – dependent on incident type
- Have protocols for reporting all types of incidents
- Have verbal discussions and processes but they are not documented

5. **Does your organization use cyber insurance? YES NO If yes, what recommendation and advice would you give other organizations looking to purchase cyber insurance?**

Most participants did not respond to this question. More said they did not have cyber insurance than had it, however some did not know if their agency had any type of cyber insurance. Comments that were included are:

- Know your risks and purchase according to those risks
- Engage risk management professionals

6. **What suggestions do you have for the State of Washington as it works toward the creation of a Cyber Reserve Corps?**

- Develop a team that includes representatives from public and private sectors
- Threat intelligence sources need to be improved. They should be skilled at vetting data and Indicators of Compromise (IOC), and they should understand response
- Consider how the group will use emerging technologies
- Advertise and promote the initiative
- Establish a clear asset or resource development plan
- Plan how to grow skills, experience, and effectiveness of people. Identify incentives to encourage volunteer participation.
- Advertise a major recruitment campaign through all professional organizations
- Utilize universities and industry for volunteers and to develop the program
- Include healthcare and public health professions
- Consider making it part of Citizen Corps or some other type of volunteer program already in place such as the State Emergency Worker program. There are established groups in each county already for different purposes – use that process for IT.
- Follow the Michigan model
- Offer a valued certification in exchange for providing a certain number of hours toward a cyber team response or team support activities.
- Develop fact sheets that include process
- Find a way to bring in help and keep them through methods not generally used by government
- Keep the Cyber Reserve Corps active and build them up to be reputable and trustful. I like the local aspect
- Encourage executive buy-in and how to negotiate legislative barriers
- Pool resources across jurisdictions
- Use students as interns
- Include credentialing process

7. **What type of cyber security related legislation would you like to see the Washington State Legislature introduce during the upcoming session?**

- Amnesty for reporting within 30 days. Helping other entities should not cost the victims
- Safe harbor act for information sharing
- Authority, objectives, adequate funding and clear evaluation criteria
- Provide incentives for organizations to report incidents where they might otherwise feel compelled to remain silent
- Scholarship programs to reflect a WA State Cyber Corps to mimic the SFS Cyber Corps
- Funding for state response teams beyond just staff, that is in place today
- State initiative for cybersecurity volunteer corps

- Confidential reporting requirement
- Training requirement for cyber experts
- Funding and protection from public disclosure
- No legislation unless it streamlines processes
- Need cyber security professionals assigned to school districts
- Funding for training, certification, and program development
- Fund more cyber initiatives

8. Please provide any topics for future cyber security discussions and recommendations on how to improve or enhance this type of event.

- More detailed discussion about cyber insurance
- More discussion regarding how public and private entities can work together
- Printed list of resources
- Neighborhood watch
- Implementing a cyber resilient population across the entire state
- Guidance on reporting and preparedness: up and down (i.e. state to local to state)
- Incident response and forensics evidence collection
- More discussion of real events
- More hands-on and fewer speakers
- Be inclusive of small and medium enterprises by having business organization promote cyber security discussions
- Continue working on Cyber Reserve Corps
- Less introduction of panel speakers and more questions allowed from participants
- How to incorporate NIMS and ICS in cybersecurity response
- Hardware / Firmware vulnerabilities and supply chain security
- There is still a gap between cyber security professionals and the need for the service