Washington State Community Cybersecurity
“...A Matter of Public Safety and National Security”

"Status quo is no longer acceptable -- not when there's so much at stake. We can and we must do better." — President Barack Obama
Washington State as a National Leader

Community Cybersecurity

• Regional collaboration
• Resilience
• Research, analysis, and sharing
• Unity of effort
• Workforce development
“Through the Emergency Management Division and our National Guard, my Homeland Security Advisor – in partnership with the CIO – has taken great strides in addressing our cyber emergency preparedness and response capability.”

- Governor Jay Inslee, August 19th, 2015 Letter to DHS
Community Cybersecurity

MISSION
To minimize the impact of cyber emergencies on the people, property, environment, and economy of Washington State

VISION
A public, private, and tribal partnership able to prepare for and respond to cyber emergencies with unity, competence, and efficiency for the good of the citizens of Washington State
Relationships

• DHS Federal lead
• Key state offices work with one another and directly with DHS

• Military Department lead
• Critical partnerships
Working Together

Cyber Incident Response Coalition and Analysis Sharing | Exercise Partners | Cyber Resource Typing | Regional Monitoring | Cyber Hazard Threat Profile Partners

- Strategies, policies, and frameworks
- Unite efforts
- Secure resilient systems
- Support response
- Leaders and innovators
- Critical Infrastructure
- Backbone
What we prepare for

Public Safety Communications

Economic

Catastrophe

Critical Infrastructure
Emerald Down V
Regional Cyber Security Exercise

Mark your calendars for the upcoming Regional Cyber Security Exercise!

WHO SHOULD ATTEND:
- Emergency managers
- Security managers and affiliated IT staff
- Control systems technicians
- Business continuity professionals
- Critical infrastructure Managers/Operators
- Major employers
- Public/private organizations that impact the regional economy
- Limited to 200 participants

WHEN:
February 16, 2017
9:00am - 4:30pm

WHERE:
McCawick Conference Center
Gover Park Technical College
4500 Stellacoorn Blvd SW, Lakewood, WA

DETAILS:
There is no cost for this event, exercise funded by a state homeland security grant through King County (WA - Homeland Security Region 6).

REGISTER:

Washington State Homeland Security Region 6 Critical Infrastructure Protection Working Group

Practice a community cyber security response approach with our interactive exercise.

Understand how the region works to stabilize critical infrastructure functions, minimize health and safety threats, and efficiently restore and revitalize systems and services to support a viable, resilient community.

Explore how your organization’s Cyber Plan could integrate with the WA State Cyber Annex to the Comprehensive Emergency Management Plan.

Understand your organization’s capacity for timely communications in support of security, situational awareness, and response operations between impacted communities, organizations and response personnel.

Build trust among technology and security practitioners.

Provide decision makers with relevant information regarding the nature and extent of the threat, interdependencies, and the status of the response.

Practice the deployment of shared cyber responder resources.

A free cyber incident response template will be provided to attendees at the event.

A Pilot Program to develop a WA State Emergency Cyber Responder badge program will be explored with qualified attendees at the exercise.

Exercise Coordinated by the Pacific NW Economic Region - Center for Regional Disaster Resilience.
Contact: Brandon Hardenbrook, brandon@pnwe.org
Significant Cyber Incident Response
# Cyber Resource Typing

## Cyber Incident Response Team

<table>
<thead>
<tr>
<th>DESCRIPTION</th>
<th>RESOURCE CATEGORY</th>
<th>RESOURCE KIND</th>
<th>COMPOSITION AND ORDERING SPECIFICATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cyber Incident Response Team responds to a significant cyber incident affecting critical infrastructure</td>
<td>Cybersecurity</td>
<td>Cyber Incident Response Team</td>
<td>1. Logistics for deploying this team, such as security, lodging, transportation, meals, etc. should be discussed with the resource provider prior to deployment 2. Teams work up to 12 hours per shift, are self-sustained for 72 hours, and deployable for up to 14 days 3. Multiple teams may need to be ordered to provide 24 hour coverage 4. The entire team may or may not be constituted from a single source entity 5. The requestor should specify if the personnel should have training and experience with specific software applications, hardware, and equipment</td>
</tr>
</tbody>
</table>

## Overall Function

- Investigates and analyzes all relevant cyber and network activities related to the crisis situation with the purpose of achieving the speediest recovery of the impacted critical infrastructure
- Uses response methods to maximize preservation of life, property, and data integrity
- Documents all steps and actions taken during the operations and develops a Situation Report

## Type Response Team

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>METRIC/MEASURE</th>
<th>CAPABILITY</th>
<th>Type I</th>
<th>Type II</th>
<th>Type III</th>
<th>Type IV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personnel</td>
<td>Per Team</td>
<td>Management and oversight</td>
<td>2 – Team Chief and Deputy (Cyber Incident Responder)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Community Cybersecurity Capability Maturity Model

**LEVEL 1: Initial**
- Limited or no integration of cybersecurity in EMD units
- No EMD-run exercising of cyber events. No HSGP integration. No resource typing.
- Limited policy and planning. State agency roles and responsibilities unclear.
- Minimal direct engagement with public & private sector on cyber EM

**LEVEL 2: Advanced**
- CSM hired; evaluates each EMD unit
- State TEP includes cyber events in 5 of 8 exercises & TTX. HSGP/Resource typing researched.
- CEMP & Annex drafts finalized. Interagency MOA. HIVA and THIRA reviewed.
- EM outreach begins with public & private sector

**LEVEL 3: Self-Assessed**
- Formal training for EMD via TEP and internal staff events
- Cyber exercises conducted and assessed. Grant flow includes cybersecurity. Resource typing process est.
- CEMP updated; Annex published; MOA complete. HIVA and THIRA updated.
- UCG identified to include 16 CIKR POCs

**LEVEL 4: Integrated**
- EMD Units & jurisdictions trained; process updated
- CEMP/Annex exercised & revised. State agency roles defined.
- UCG and CIKR reps aware of roles, united, and prepared

**LEVEL 5: Vanguard**
- Cybersecurity a statewide EM business imperative.
- WA ready for cyber incident; recognized as national leader. Structured funding/typing flow.
- UCG prepared and available 24/7 for AWC notification.
Information Sharing

- CC-COP
- HSIN
- InfraGard
- CIRCAS
- AGORA
- XX-ISAC
- WSFC
- IRSC
Closing

• Washington State a leader
• All emergencies are local – Community Cybersecurity enhances readiness
• Cyber is an Emergency Management issue