Washington State Community Cybersecurity Update
“...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

To view an excerpt from the President’s 2009 speech on community cybersecurity, click on the following link:
http://mil.wa.gov/emergency-management-division/cyber-security-program
What we prepare for

Public Safety Communications

Economic

Catastrophe

Critical Infrastructure
Working Together

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

Public Sector
- Strategies, policies, and frameworks
- Unite efforts
- Secure resilient systems
- Support response

Emergency Management
- Leaders and innovators
- Critical Infrastructure
- Backbone

Private Sector
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.
Update - Policy

The White House
Office of the Press Secretary
For Immediate Release

Presidential Policy Directive --
United States Cyber Incident
Coordination

July 26, 2016

PRESIDENTIAL POLICY DIRECTIVE/PPD-41

SUBJECT: United States Cyber Incident Coordination

The advent of networked technology has spurred innovation, cultivated
knowledge, encouraged free expression, and increased the Nation’s economic
prosperity. However, the same infrastructure that enables these benefits is
vulnerable to malicious activity, malfunction, human error, and acts of nature,
placing the Nation and its people at risk. Cyber incidents are a fact of
contemporary life, and significant cyber incidents are occurring with increasing
frequency, impacting public and private infrastructure located in the United
States and abroad.

Lead for asset response
• Department of Homeland
Security/National
Cybersecurity and
Communications Integration
Center

Lead for threat activities
• Department of Justice (FBI)

Lead for intelligence support
• Office of the Director of
National Intelligence
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.

Cyber Incident: An event occurring on or conducted through a computer network that actually or imminently jeopardizes the confidentiality, integrity, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon.
Significant Cyber Incident Response

Significant Cyber Incident → Activation → Coordination Group
Update: Exercises and Training

• Exercises
  • Emerald Down – 16 February 2017
  • Pierce County Cyber VTXX – 26 April 2017
  • Executive Tabletop – 9 May 2017
  • Cyber Guard Prelude – 23-25 May 2017

• Training
  • TEEX Community Cybersecurity (AWR136, MGT452, MGT385) – 31 January – 2 February 2017
  • FEMA Cybersecurity & Cyber Incident Awareness: Knowing Yourself and Knowing the Enemy – 27 April 2017, 0800-1200
Update: PNW Cyber Reviews

• Preparedness Leadership Council, Cybersecurity A Way Forward

• The Center for Internet and Society at Stanford Law School. State-Level Cyber Security Efforts: Washington State and the Evergreen Approach to Cyber Security
Update: Cyber Related Legislation

- **HB 1417**: Concerning the harmonization of the open public meetings act with the public records act in relation to information technology security matters.

- **HB 1418**: Establishing a blue ribbon panel on cybersecurity.

- **HB 1419**: Granting the governor authority to proclaim a state of emergency in the event of a substantial cybersecurity incident.

- **HB 1929**: Concerning independent security testing of state agencies' information technology systems and infrastructure by the military department.

- **HB 2086**: Establishing a task force to address state interagency coordination in cybersecurity.
Update: 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

<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></td>
<td></td>
<td></td>
<td>2 – Team Chief and Deputy (Cyber Incident Responder)</td>
</tr>
</tbody>
</table>
Update: Outreach and Info Sharing

- Cyber Incident Response and Analysis Coalition (CIRCAS) – 15 March 2017
- Regional Emergency Communications Coordination Working Group (RECCWG) – 14 March 2017
- AGORA – 24 March 2017
- Partners in Emergency Preparedness (PIEPC), Tacoma – 19 April 2017
- Cyber Outreach to members of Bellevue Community - 5 May 2017

- Cyber Communications – Common Operating Picture Working Group/Critical Incident Operational Teleconference – ongoing
Questions?