Region 5 Cyber Dawn Tabletop Exercise (TTX)

After-Action Report/Improvement Plan

November 14, 2018

The After-Action Report/Improvement Plan (AAR/IP) aligns exercise objectives with preparedness doctrine to include the National Preparedness Goal and related frameworks and guidance. Exercise information required for preparedness reporting and trend analysis is included; users are encouraged to add additional sections as needed to support their own organizational needs.

Rev. 2017 508
HSEEP-IP01

EXERCISE OVERVIEW

Exercise Name	Cyber Dawn
Exercise Dates	October 30, 2018 11:00 pm – 3:30 pm
Scope	This exercise is a facilitated, discussion-based exercise, with a planned duration of four hours, held in the Pierce County Emergency Management EOC Policy Room. The exercise will build the foundation of local cyber incident management.
Mission Area(s)	Prevention, Protection, Mitigation, Response, and Recovery
Core Capabilities	Planning, Cybersecurity, Intelligence and Information Sharing, Operational Coordination, Situational Assessment
Objectives	1. Increase cybersecurity awareness to senior officials of cyber risk management, cyber related planning, and other issues related to cyber incident prevention, protection, response, and recovery of critical systems. 2. Assess cybersecurity integration into an organization's all-hazards preparedness. 3. Examine cybersecurity incident information sharing, escalation criteria, and related courses of action. 4. Examine cybersecurity incident management structures. 5. Review cyber resource request and management processes. 6. Measure and validate the Region 5 Cybersecurity Resiliency Concept of Operations draft version.
Threat or Hazard	Cyber
Scenario	A hacker exploits a software vulnerability and conducts spearphishing to steal personally identifiable information and protected health information from government systems. Additionally, malware capable of opening cell doors at a local prison is discovered.
Sponsor	Pierce County Emergency Management (PCEM) State Homeland Security Program (SHSP) Grant Department of Homeland Security (DHS) – National Cyber Exercise and Planning Program (NCEPP)
Participating Organizations	Twenty-two participants from state and local governments, the public and private sectors, and critical infrastructure.

Exercise Name	Cyber Dawn
Point of Contact	Natalie Stice Homeland Security Coordinator Pierce County Emergency Management 2501 South 35th Street, Suite D Tacoma, WA 98409 253-798-3311 natalie.stice@piercecountywa.gov DHS National Cyber Exercise and Planning Program (NCEPP) (703) 235-5641 cep@hq.dhs.gov

ANALYSIS OF CORE CAPABILITIES

Aligning exercise objectives and core capabilities provides a consistent taxonomy for evaluation that transcends individual exercises to support preparedness reporting and trend analysis. Table 1 includes the exercise objectives, aligned core capabilities, and performance ratings for each core capability as observed during the exercise and determined by the evaluation team.

Objective	Core Capability	Performed without Challenges (P)	Performed with Some Challenges (S)	Performed with Major Challenges (M)	Unable to be Performed (U)
Increase cybersecurity awareness to senior officials of cyber risk management, cyber related planning, and other issues related to cyber incident prevention, protection, response, and recovery of critical systems.	Planning Operational Coordination	P			
Assess cybersecurity integration into an organization's all-hazards preparedness.	Cybersecurity Planning		S		
Examine cybersecurity incident information sharing, escalation criteria, and related courses of action.	Intelligence & Information Sharing Operational Coordination Situational Assessment			M	
Examine cybersecurity incident management structures.	Operational Coordination	P			
Review cyber resource request and management processes.	Operational Coordination Situational Assessment			M	
Measure and validate the Region 5 Cybersecurity Resiliency Concept of Operations draft version.	Planning		S		

Table 1. Summary of Core Capability Performance

Ratings Definitions:

Performed without Challenges (P): The targets and critical tasks associated with the core capability were completed in a manner that achieved the objective(s) and did not negatively impact the performance of other activities. Performance of this activity did not contribute to additional health and/or safety risks for the public or for emergency workers, and it was conducted in accordance with applicable plans, policies, procedures, regulations, and laws.

Performed with Some Challenges (S): The targets and critical tasks associated with the core capability were completed in a manner that achieved the objective(s) and did not negatively impact the performance of other activities. Performance of this activity did not contribute to additional health and/or safety risks for the public or for emergency workers, and it was conducted in accordance with applicable plans, policies, procedures, regulations, and laws. However, opportunities to enhance effectiveness and/or efficiency were identified.

Performed with Major Challenges (M): The targets and critical tasks associated with the core capability were completed in a manner that achieved the objective(s), but some or all of the following were observed: demonstrated performance had a negative impact on the performance of other activities; contributed to additional health and/or safety risks for the public or for emergency workers; and/or was not conducted in accordance with applicable plans, policies, procedures, regulations, and laws.

Unable to be Performed (U): The targets and critical tasks associated with the core capability were not performed in a manner that achieved the objective(s).

The following sections provide an overview of the performance related to each exercise objective and associated core capability, highlighting strengths and areas for improvement.

Objective 1: Increase cybersecurity awareness to senior officials of cyber risk management, cyber related planning, and other issues related to cyber incident prevention, protection, response, and recovery of critical systems.

The strengths and areas for improvement for this objective are described in this section.

Strengths

The full capability level can be attributed to the following strengths:

Strength 1: Threat received at the Regional Coordinating Council level and participant attendance resultant of the call to action

Strength 2: Great, active participation from players and coordination across sectors.

Strength 3: A variety of expertise/players, organizations, and insight were present.

Areas for Improvement

The following areas require improvement to achieve the full capability level:

Area for Improvement 1: More regional members involved/representation from other agencies

Reference: individual-sector regulatory requirements

Analysis: Staffing levels and individual-agency priorities will continue to dictate attendance and participation in the regional planning team and exercises. Current members and participants are encouraged to advocate for attendance and leadership buy-in at their agencies and those of their partners wherever able.

Area for Improvement 2: More individual-agency collaboration with their IT personnel, end-users, and emergency management personnel.

Reference: [List any relevant plans, policies, procedures, regulations, or laws.]

Analysis: Most agency departments are still siloed, or don't freely collaborate across departments for planning purposes and information sharing to include threat awareness.

Objective 2: Assess cybersecurity integration into an organization's all-hazards preparedness.

The strengths and areas for improvement for this objective are described in this section.

Strengths

The partial capability level can be attributed to the following strengths:

Strength 1: Emergency management staff (where applicable) were present in addition to cybersecurity subject matter experts

Strength 2: CONOPs draft was in a template useable across a broad range of agencies

Areas for Improvement

The following areas require improvement to achieve the full capability level:

Area for Improvement 1: More leadership/executive involvement (mayors, exec, directors).

Reference: The 2002 Federal Information Security Management Act (FISMA)

Analysis: Many participants relayed a sense of inability to effect change in their current position. Leadership involvement is necessary to both understand the threat and garner approval for change to address the threat within their respective organization.

Area for Improvement 2: Incorporate Continuity of Operations Planning (COOP) and Business Impact Analysis (BIA) to cybersecurity

Reference:

- Pierce County Emergency Management, Comprehensive Emergency Management Plan, Incident Annex 3
- Washington State Military Department, Emergency Management Division, Comprehensive Emergency Management Plan, Annex D
- National Cyber Incident Response Plan

Analysis: Many of the participating agencies have not developed or exercised their COOP—with our without the use of computers—for a routine outage or cyber-based incident.

Objective 3: Examine cybersecurity incident information sharing, escalation criteria, and related courses of action.

The strengths and areas for improvement for this objective are described in this section.

Strengths

The partial capability level can be attributed to the following strengths:

Strength 1: CONOPs draft and appendices were in a template useable across a broad range of agencies

Strength 2: Good amount of collaboration and idea-sharing amongst the group

Areas for Improvement

The following areas require improvement to achieve the full capability level:

Area for Improvement 1: Lack of understanding and or knowledge of what is needed/expectations for pursuant law enforcement actions

References:

- DoJ-FBI Criminal Justice Information Services Security Policy
- The Cybersecurity Act of 2015

Analysis: Staffing levels and individual-agency priorities will continue to dictate attendance and participation in the regional planning team and exercises. The Regional Coordinating Council will be routinely briefed, and participation request honed.

Area for Improvement 2: Lack of understanding and or knowledge of legal liabilities and requirements

Reference:

- Sector-specific regulatory requirements

Analysis: lack of participation of a cyber-specific attorney

Area for Improvement 2: Lack of understanding and or knowledge of how the Washington State Fusion Center methods and processes

References:

- Washington State Fusion Center Suspicious Activity Report (SAR) – adopted by Pierce County Emergency Management and the South Sound Regional Intelligence Group (SSRIG)
- Region 5 Cybersecurity Resiliency Concept of Operations
- The National Cybersecurity Protection Act of 2014

Analysis: Lack of qualified Fusion Liaison Officers across sectors

Objective 4: Examine cybersecurity incident management structures.

The strengths and areas for improvement for each core capability aligned to this objective are described in this section.

Strengths

The full capability level can be attributed to the following strengths:

Strength 1: Incident management structures were well-established across sectors

Strength 2: Most agencies have well-developed Incident Response Plans and Security Best Practices

Areas for Improvement

The following areas require improvement to achieve the full capability level:

Area for Improvement 1: Lack of involvement of IT Managers and or lack of proper IT personnel in attendance

Reference: The Federal Information Technology Acquisition Reform Act (FITARA) of 2014

Analysis: Many of the participants stated they well understood the threat, but as programmers or engineers had little-to-no influence in organizational change or the ability to persuade the high priority threat to their IT managers for cross-discipline threat response and management.

Objective 5: Review cyber resource request and management processes.

The strengths and areas for improvement for each core capability aligned to this objective are described in this section.

Operational Coordination

Strengths

The partial capability level can be attributed to the following strengths:

Strength 1: CONOPs draft and appendices were in a template useable across a broad range of agencies

Strength 2: A variety of expertise/players, organizations, and insights were present.

Areas for Improvement

The following areas require improvement to achieve the full capability level:

Area for Improvement 1: Lack of organizational cybersecurity awareness and best practices across sectors (end-user to technical).

Reference: Region 5 Cybersecurity Resiliency Concept of Operations

Analysis: independent standards for training, education, and exercises

Objective 6: Measure and validate the Region 5 Cybersecurity Resiliency Concept of Operations draft version.

The strengths and areas for this objective are described in this section.

Strengths

The partial capability level can be attributed to the following strengths:

Strength 1: CONOPs draft and appendices were in a template useable across a broad range of agencies

Strength 2: Appropriate scenario to for all agencies to become familiar with the draft

Strength 3: Well laid-out CONOPS draft

Areas for Improvement

The following areas require improvement to achieve the full capability level:

Area for Improvement 1: Lack of familiarity with the CONOPs escalation process against existing organizational policies, procedures, and guidelines

Reference: Region 5 Cybersecurity Resiliency Concept of Operations

Analysis: More review of the CONOPs is needed from participating agencies.

Appendix A: Improvement Plan

Objective	Issue/Area for Improvement	Corrective Action	Capability Element	Start Date	Completion Date
Objective 1: Increase cybersecurity awareness	1. More regional members involved/representation from other agencies	Current members and participants are encouraged to advocate for attendance and leadership buy-in at their agencies and those of their partners wherever able.	**Planning, Organization**	11/29/18	03/21/19
	2. More individual-agency collaboration with their IT personnel, end-users, and emergency management personnel.	Increase collaboration across organizational departments and divisions for a common understanding of the threat and how to mitigate it	**Planning, Organization**	11/29/18	03/21/19
Objective 2: Cybersecurity integration	1. More leadership/executive involvement (mayors, exec, directors).	Increase collaboration with leadership in the pursuit of organizational change and threat management	**Planning**	11/29/18	03/21/19
	2. Incorporate Continuity of Operations Planning (COOP) and Business Impact Analysis (BIA) with organizational cybersecurity	Collaboratively review existing COOP and BIAs for alignment with cybersecurity	**Planning, Organization**	11/29/18	03/21/19
Objective 3: Cybersecurity incident information sharing, escalation criteria, and related courses of action.	1. Lack of understanding and or knowledge of what is needed/expectations for pursuant law enforcement actions	Have a Law Enforcement Subject Matter Expert/Forensic Analyst share processes of expectations and related courses of action	**Training**	11/29/18	03/21/19
	2. Lack of understanding of legal liabilities and Washington State	Participants are encouraged to pursue legal expertise within	**Training**	11/29/18	03/21/19

	Fusion Center methods and processes	their agency, as counsel differs between the disciplines and agencies.			
	3. Lack of understanding and or knowledge of Washington State Fusion Center methods and processes	Participants are encouraged to become Fusion Liaison Officers (FLO) for their agency (8-hour course offered quarterly), which covers the gamut of suspicious activity reporting.	**Training**	11/29/18	Ongoing
Objective 4: Cybersecurity Incident Management Structures	1. Lack of involvement of IT Managers and or lack of proper IT personnel in attendance	Encourage IT Managers through increased collaboration to be more involved or get proper personnel to attend	**Organization**	11/29/18	03/21/19
Objective 5: Cyber resource request and management processes.	1. Lack of organizational cybersecurity awareness and best practices across sectors (end-user to technical).	Review organizational SOGs, training plans, and cybersecurity best practices	**Training, Planning**	11/29/18	03/21/19
Objective 6: Validation of the Region 5 Cybersecurity Resiliency Concept of Operations draft	1. Lack of familiarity with the CONOPs escalation process against existing organizational policies, procedures, and guidelines	Convene a review of current incident response plans against the CONOPs across multiple departments of the individual agency for compatibility	**Planning, Training**	11/29/18	03/21/19

This IP has been developed specifically for Homeland Security Region 5 as a result of Cyber Dawn conducted on October 30, 2018.

APPENDIX B: EXERCISE PARTICIPANTS

Participating Organizations
Local
City of Puyallup Emergency Management
City of Sumner
Pierce County Emergency Management
Pierce County Information Technology
State
Washington State Military Department Emergency Management Division
Washington Technologies Solutions (WaTech)
Private
Cascade Water Alliance
Critical Infrastructure Cyber Security Consultants
Cybersecurity and Information Assurance Solutions
Critical Infrastructure
Pierce Transit
Port of Tacoma
SouthSound 911
Tacoma-Pierce County Health Department
Pierce County Planning & Public Works