



Exercise Schedule

- 1100-1115 Welcome & Opening
- 1115-1130 Current Cyber Threat Landscape Briefing
- 1130-1215 Lunch & Phase 1 – Preparation
- 1215-1300 Phase 2 - Detection
- 1300-1345 Phase 3 – Escalation
- 1345-1430 Phase 4 – Notification
- 1430-1515 Phase 5 – Containment, Eradication, and Recovery
- 1515-1530 Hot Wash & Closing Comments

Resources and Contacts

Resources

National Cyber Incident Response Plan

https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf

Washington State Significant Cyber Incident Annex (CEMP Annex D)

<https://www.mil.wa.gov/uploads/pdf/PLANS/wastatesignificantcyberincidentannex20150324.pdf>

Pierce County Cyber Incident (CEMP Incident Annex 3)

<https://www.co.pierce.wa.us/DocumentCenter/View/35761/IA3-2014-Final?bidId=>

Region 5 Cyber Resiliency Concept of Operations DRAFT

Contacts

Natalie Stice, Exercise Coordinator
natalie.stice@piercecountywa.gov

This exercise is sponsored by Pierce County Emergency Management in cooperation with the Department of Homeland Security's National Cyber Exercise Planning Program



Region 5 Cyber Dawn

October 30, 2018

Region 5
Cyber Planning Team



Purpose, Scope, & Scenario

This is a tabletop exercise. Play will be limited to 11:00 a.m. – 3:30 p.m.

The focus will be the response to a cyber event focusing on preparedness, information sharing, incident response, and recovery.

Cyber Dawn will be conducted at Pierce County Emergency Management.

Assumptions & Artificialities

Earnest effort has been made to create a plausible and realistic scenario to evaluate and validate identified objectives.

Because the exercise is of limited duration and scope, certain details will need to be simulated. This simulation may require players to use their best judgment in response to requests for additional information.

Exercise Objectives

- **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*
- **Assess cybersecurity integration into an organization's all-hazards preparedness.** - *Planning*
- **Examine cybersecurity incident information sharing, escalation criteria, and related courses of action.** – *Intelligence and Information Sharing, Planning*
- **Examine cybersecurity incident management structures.** – *Operational Coordination*
- **Review cyber resource request and management processes.** – *Operational Coordination*



Exercise Intent

This exercise was designed for an organization to validate its newly drafted cybersecurity incident response plan and improve its current Emergency Operations Plan or Cyber Incident Annex. The scenario focuses specifically on incident response. The scenario includes one element—spearphishing emails disguised as HR messages—that impacts all organizational departments, as well as other elements that target individual departments. Participants discuss questions after each scenario update, rather than grouped modules or phases. This format is intended to allow a step-by-step examination of current plans at a detailed level.

The intended audience for this exercise includes, but is not limited to, IT staff, emergency management staff, planners, and members of the cyber incident response team.

This exercise will be conducted in a no-fault environment and will evaluate the existing plans, policies, and procedures as if players were responding to a real-world emergency. The exercise is not to be viewed as a test or inspections of individual performance.