Maritime Cybersecurity Situational Awareness Project

February, 2018

Eric Holdeman, Director

Center for Regional Disaster Resilience (CRDR)

Pacific Northwest Economic Region (PNWER)

What is the Cybersecurity Reporting Gap?

- There is a requirement to report incidents of cybersecurity intrusions, 33 CFR 101.305 - Reporting
- The who, what—when can be fuzzy
- Options for reporting incidents include:
  - US Coast Guard—JHOC
  - Secret Service
  - FBI
  - Local Law Enforcement
  - WA Fusion Center
  - Washington State Emergency Management Division Duty Officer

CRDR
Center for Regional Disaster Resilience

Pacific NorthWest Economic Region

Project Origins

- The issue of cybersecurity reporting has been known for several years
- Port Security Funding explored as an option for project
  - Challenge: The requirement of a cash match for regional projects
- 2017 Resilience Challenge Grant obtained by the Pacific NW Economic Region (PNWER)
  - One time funding—Critical Infrastructure orientation
  - Project focused on maritime industry
  - Potential to expand to other critical infrastructure applications

CRDR
Center for Regional Disaster Resilience

Pacific NorthWest Economic Region

Project Teams

- Core Planning Group
  - PNWER/CRDR will facilitate the planning process and develop a Concept of Operations (CONOPS) for how reporting can be done
    - David Matthews supporting
  - Washington Fusion Center key to collecting and disseminating information to appropriate parties
  - CIRCAS (Cyber Incident Response Coalition & Analysis Sharing)
  - USCG Sector Puget Sound will be an "advisor to the project"
- Stakeholder Advisory Group
  - Maritime stakeholders: Ports; Terminals; Pilots; Ferry Systems; Trucking Companies; Railroads; Labor; Etc.
  - Law Enforcement…Federal; State; Local
  - Local & State Emergency Management

CIRCAS
Cyber Incident Response Coalition & Analysis Sharing

CRDR
Center for Regional Disaster Resilience

Pacific NorthWest Economic Region

Stakeholder Commitment

- Provide personnel, as appropriate, to assist with this effort
  - Participate in a survey
  - Attend initial workshop
  - Provide input to and review CONOPS when a DRAFT is available
  - Attend second workshop to provide feedback to the planning process
  - Attend tabletop exercise to test CONOPS

CRDR
Center for Regional Disaster Resilience

Pacific NorthWest Economic Region

Project Timeline

- December: Contacting Stakeholders; Core Planning Team; Advisory Group
- January: Create and Disseminate Survey
  - Current understanding of cyber-threat
  - Current level of preparedness, plans, procedures and protocols
- March 6: Kickoff Workshop with Stakeholders
  - Back-brief survey findings
  - Begin creation of CONOPS
- March: Create DRAFT CONOPS

CRDR
Center for Regional Disaster Resilience

Pacific NorthWest Economic Region

Project Timeline (Cont.)

- April: Host a second workshop
  - Review and DRAFT CONOPS

May: Produce Final DRAFT CONOPS

August: Test CONOPS via tabletop exercise with stakeholders

September: Submit final report and Final CONOPS to DHS

Questions?

eric.holdeman@pnwer.org
drmatthewsusa@gmail.com

CRDR
Center for Regional Disaster Resilience

Pacific NorthWest Economic Region