CYBER/PHYSICAL: INFORMATION SHARING

THREAT INFORMATION TRIAGING

- Review subject lines, looking for what sparks your attention/fits your role
- Look for key terms/topics: remote code execution, APT, pivoting from IT to OT, living off the land, etc.
- Evaluate patterns in monthly reports
- Assign scores to threats and escalate as needed

THREAT INFORMATION RESOURCES

IMPORTANT CONTACTS:

CESER SLTT PM:

CESER REGIONAL COORDINATOR:

CISA (PSA or CSA):

FUSION CENTER CONTACT:

OTHER CONTACT:

U.S. DEPARTMENT of ENERGY | Office of Cybersecurity, Energy Security, and Emergency Response

Pacific Northwest NATIONAL LABORATORY

NASEO National Association of State Energy Officials

CYBER/PHYSICAL: INFORMATION SHARING

THREAT INFORMATION TRIAGING

- Review subject lines, looking for what sparks your attention/fits your role
- Look for key terms/topics: remote code execution, APT, pivoting from IT to OT, living off the land, etc.
- Evaluate patterns in monthly reports
- Assign scores to threats and escalate as needed

THREAT INFORMATION RESOURCES

IMPORTANT CONTACTS:

CESER SLTT PM:

CESER REGIONAL COORDINATOR:

CISA (PSA or CSA):

FUSION CENTER CONTACT:

OTHER CONTACT:

U.S. DEPARTMENT of ENERGY | Office of Cybersecurity, Energy Security, and Emergency Response

Pacific Northwest NATIONAL LABORATORY

NASEO National Association of State Energy Officials

Threat Information Escalation Considerations

- **Identify and Document the Threat**
  - Source of information and validation—determine the credibility of the originator
  - Type of incident and potential trends
  - Status: ongoing or contained
- **Evaluate the Risk**
  - Geographical impact
  - Severity of the incident
  - Potential consequences—for sectors, assets or systems, interdependencies, critical facilitates, etc.
- **Follow an Escalation Protocol**
  - Consider adapting escalation protocols from your ESF-12 or fuel plan to fit a cyber incident
  - Define/modify criteria for escalation
  - Determine the breadth of information to include (and for what audience)
  - Clear the protocol with leadership prior to the incident and share it with state partners
- **Share Information**
  - Write up a report and distribute
  - Consider including a summary of findings, recommendations, and mitigation options
- **Develop Formal Documentation**
  - Define the threshold for formal documentation
  - Document who was notified and any actions taken
  - Ensure documentation meets security/privacy requirements (e.g., CUI or FOUO) and mark accordingly

POC Checklist

- [ ] Share/receive information with/from federal partners (i.e., E-ISAC/CESER/CISA/FBI)
- [ ] Set up regular communications with asset owners
- [ ] Create a roster of state contracts to share/receive information

U.S. DEPARTMENT of ENERGY | Office of Cybersecurity, Energy Security, and Emergency Response

Pacific Northwest NATIONAL LABORATORY

NASEO National Association of State Energy Officials

PNNL-SA-217473

Threat Information Escalation Considerations

- **Identify and Document the Threat**
  - Source of information and validation—determine the credibility of the originator
  - Type of incident and potential trends
  - Status: ongoing or contained
- **Evaluate the Risk**
  - Geographical impact
  - Severity of the incident
  - Potential consequences—for sectors, assets or systems, interdependencies, critical facilitates, etc.
- **Follow an Escalation Protocol**
  - Consider adapting escalation protocols from your ESF-12 or fuel plan to fit a cyber incident
  - Define/modify criteria for escalation
  - Determine the breadth of information to include (and for what audience)
  - Clear the protocol with leadership prior to the incident and share it with state partners
- **Share Information**
  - Write up a report and distribute
  - Consider including a summary of findings, recommendations, and mitigation options
- **Develop Formal Documentation**
  - Define the threshold for formal documentation
  - Document who was notified and any actions taken
  - Ensure documentation meets security/privacy requirements (e.g., CUI or FOUO) and mark accordingly

POC Checklist

- [ ] Share/receive information with/from federal partners (i.e., E-ISAC/CESER/CISA/FBI)
- [ ] Set up regular communications with asset owners
- [ ] Create a roster of state contracts to share/receive information

U.S. DEPARTMENT of ENERGY | Office of Cybersecurity, Energy Security, and Emergency Response

Pacific Northwest NATIONAL LABORATORY

NASEO National Association of State Energy Officials

PNNL-SA-217473