

Communicating Cyber Security Information NRC Perspective

Jonah Pezeshki
NSIR/DPCP/CSB



1

General Communication Activities:

- The staff generates a weekly Dashboard product that provides a summary of recent cyber security-related events at licensees
 - Although initially distributed internally, these reports are available to external stakeholders with a need to know, via the Protected Web Server (PWS)
 - More information on PWS can be found at: <https://pws.nrc.gov/>



2

Communication to Licensees: Generic Communications

- The NRC typically communicates with licensees via its Generic Communications program
- Generic Communications to licensees regarding cyber security-related activity are typically limited to either Security Advisories or Threat Advisories



3

Communication to Licensees: Security Advisories

- Cyber related Security Advisories are distributed to licensees when:
 - Lessons learned from an event reveal potential vulnerabilities for other licensees
 - A publically-released cyber security-related event, threat, or vulnerability may have an impact on licensees



4

Communication to Licensees: Threat Advisories

- Threat Advisories are developed by the NRC Threat Assessment group and distributed to licensees when:
 - The NRC has become aware of a seemingly imminent threat to licensees



5

Communication to Federal Agencies: Presidential Policy Directive (PPD) 41

- Presidential Policy Directive (PPD) 41 sets forth the principles governing the Federal Government's response to cyber incidents
 - For significant cyber incidents, PPD-41 establishes lead Federal agencies for coordinating the broader Federal Government response
 - DHS is the lead for Asset Response Activities
 - FBI is the lead for Threat Response Activities



6

Communication to Federal Agencies: Information Sharing

- Per PPD-41, NRC shares cyber security-related event information with Department of Homeland Security (DHS), via the National Cyber Security and Communications Integration Center (NCCIC)
 - Includes all events reported under 10 CFR 73.77: "Cyber Security Event Notifications"
 - CSB also informs DHS of any targeted cyber security-related events, regardless of whether they meet 10 CFR 73.77 criteria
- NRC shares event-related information and lessons learned from its regulatory activities with the Federal Energy Regulatory Commission (FERC)



7

QUESTIONS?



8
