NUCLEAR CYBER SECURITY INFORMATION SHARING – LICENSEE PERSPECTIVE

US NRC REGULATORY INFORMATION CONFERENCE 2015

NATHAN L. FAITH
EXELON GENERATION
CORPORATE NUCLEAR SECURITY, CYBER SECURITY MANAGER

PUBLIC-PRIVATE PARTNERSHIPS

- Information Sharing is of increased emphasis as a National Imperative
  - Public Sector and Private Sector stakeholder engagement is essential to the protection of our Nuclear Infrastructure
- Sector Specific Partnerships are being leveraged between Federal Agencies and the Private Sector
- NRC's Cyber Security Rule 10 CFR 73.54 and Event Reporting Rule 10 CFR 73.77 lend to increased communication on threats and information sharing

LICENSEE ACTIVITIES - THREAT MONITORING:

This is a condition of the Facility Operating License as regulated by 10 CFR 73.54

In accordance with NRC Approved Cyber Security Plan

Commitment of implementing Operational and Management cyber security controls in NEI 08-09, (Rev 6) Appendix E

The process is described in Section 3.5 SECURITY ALERTS AND ADVISORIES

This security control consists of requirements for (excerpted in part):

- Receiving security alerts, bulletins, advisories, and directives from credible licensee designated external organizations on an ongoing basis…
- Evaluating the information and determining the need, severity, methods and time frames for communicating or implementing mitigation measures

COMMUNICATION TO LICENSEES – GENERIC COMMUNICATIONS:

- Security Advisories, Threat Advisories or Information Notices may be communicated directly to the Licensee through existing channels
- For Non Safeguards Information retrieval, Licensees are encouraged to monitor the NRC Protected Web Server (PWS) https://pws.nrc.gov/

4

COMMUNICATION FROM FEDERAL AGENCIES - INFORMATION SHARING:

- Department of Homeland Security (DHS)
  - Nuclear Sector Specific Agency – Joint Cyber SubCouncil
  - Nuclear Sector Government Coordinating Council
- National Cyber Security and Communications Integration Center (NCCIC)
  - United States Computer Emergency Readiness Team (US-CERT)
  - Industrial Control Systems Computer Emergency Readiness Team (ICS-CERT)
  - Industrial Control Systems Joint Working Group (ICSJWG)
  - Statewide Terrorism & Intelligence Centers
  - Cybersecurity & Communications Integration Cells
- Federal Bureau of Investigation (FBI)
  - InfraGard

5

COMMUNICATION TO LICENSEES - NON-NRC PROVIDED INFORMATION:

- Licensees voluntarily utilize the Alert and Notification System (ALNOTS)
  - Service provided and managed by the Institute of Nuclear Power Operations (INPO)
  - Process screens industry sources for candidates
  - Enables licensees to evaluate for cyber vulnerabilities against their protected equipment
  - Utilizes Government produced intelligence products and deliverables
    - National Institute of Standards and Technology (NIST)
      - National Vulnerability Database (NVD)
    - DHS
      - US-CERT
      - ICS-CERT

6

COMMUNICATION WITH LICENSEES:

- Nuclear Energy Institute (NEI)
  - Nuclear Coordinating Council
  - Security Working Group
  - Cyber Security Task Force
- Nuclear Information Technology Strategic Leadership (NITSL)
  - Cyber Security Standing Committee
- Utilities Service Alliance (USA)
- INPO
- Electric Power Research Institute (EPRI) Cyber Security Technical Advisory Committee (CTAC)
- Edison Electric Institute (EEI) Security Committee
- Electricity Information Sharing & Analysis Center (E-ISAC)
- Multi-State Information Sharing & Analysis Center (MS-ISAC)

7

COMMUNICATION FROM OTHER PARTIES:

- Open Source Intelligence
- Threat Information Service Providers
- Third-Party Partners
- Suppliers
- Vendors
- Integrators

8

AREAS FOR IMPROVED COLLABORATION:

- Information Sharing is needed bidirectionally
  - Public Sector to the Private Sector

  as well as
  - Private Sector to the Public Sector
- Timely and actionable information is critical to maintaining a robust security posture
- Information classification downgrade (tear-line) is extremely important
  - Licensees need to receive information to enact the most time-critical increased focus on the identified potential indicators of compromise or the characteristics of the adversaries' activities for enhanced monitoring and vigilance

9

CONTACT INFO:

Nathan L. Faith, MABOSM, CISSP, GISP, GCIH, GICSP
Exelon Generation - Nuclear Corporate Security: Cyber Security Manager
Nathan.Faith@ExelonCorp.com | Office: 630.657.2910

10