NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

ENERGY PROVIDER COMMUNITY OF INTEREST MEETING - MARCH

Date	**3/8/2016**	
Time Start-End	**2-3 PM**	
Attendees	**NCCOE team and roles:** Jim McCarthy (Federal Lead) Don Faatz (NCCoE Lead Architect) Karen Hathaway Viani (NCCoE Systems Engineer) Harry Perper (NCCoE Lead Engineer) Johnathan Wiltberger (NCCoE Lead Engineer) Julie Steinke (MITRE)	**Community Members**: Nadya Bartol (UTC) Tim Clancy (Arch Street, LLC) Ron Beck (Central Lincoln) Fred Hintermister (NERC) Deborah Watson (KPMG)

Agenda

- NCCoE news
- Project updates: Situational Awareness, Identity and Access Management (IdAM)
- Discussion on NERC CIP v5 compliance date

Discussion

- NCCoE meeting and conference review
- The monitoring and control needs of oil and gas are very similar from a situational awareness and access management perspective. Both electric utilities and oil and gas companies have nominally similar industrial control system problems.
    - Jim has been invited to speak at the 4th Annual Cyber Security for Oil & Gas, Houston, TX (June, 2016).
- A lot of investor-owned electric utilities also own a gas company.
    - A lot of municipal utilities do as well
    - Many discussions @ Distributech around smartcity activities
- Projects:
    - Situational Awareness solution:
        - Need to make sure NCCoE guidance is consistent with NIST Cybersecurity Framework (CSF). NCCoE practice guides are first mapped to industry standards and relevant components of CSF.
            - The understanding in Oil and Gas is that the CSF is required.
            - CSF is very high level. NERC CIP is more granular and there are mappings of NERC CIP and other areas. So CSF and NERC CIP and NCCoE Practice Guides are complementary, but NERC-CIP compliance is mandatory for electric utility compliance activities, not currently the case for Oil & Gas.

- Possible test case scenario – data loss prevention – detect exfiltration of configuration information – detect infiltration of new configuration information. Was change part of approved change and inside defined procedure or was it outside of procedure.
    - Tofino will alert on configuration changes. Possibly use as a sensor to contribute info to ArcSight.
    - Configure to auto-download configuration information.
    - New host is used to perform configuration – not the approved host.
- NCCoE will issue data call for additional test case scenarios. Thank you for your consideration and response.

- IdAM solution: update – final practice guide release soon
- NERC CIP v5: NERC CIP v.5 Compliance Deadline Extended
    - Filing by a group of trade associations – you will have companies doing v5 for three months and switching to v6 and there will be differences. There was also a problem of audit follow up given criteria change during remediation.

Thank you!