NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

SEPTEMBER ENERGY PROVIDER COMMUNITY (EPC) MEETING

Date	**9/29/2015**	
Time Start-End	**2-3 PM**	
Attendees	**NCCOE team and roles:** Jim McCarthy (Federal Lead) Jim Bradshaw (NCCoE Outreach) Don Faatz (NCCoE Lead Architect) Karen Hathaway Viani (NCCoE Proj Mgmt) Harry Perper (NCCoE Lead Engineer)	**Community Members**: Ralph King (EPRI) Tim Clancy (Arch Street, LLC) Bryan Fite (BT

Agenda

- IdAM project update
- Situational Awareness project update

Discussion

- Welcome and introduction of Karen as assisting Jim McCarthy with project management.
  - Contact information: (email) khv@nist.gov; (mobile) 703-283-0221.
- IdAM project update and call to action
  - IdAM practice guide released!
  - Guide may be found online at https://nccoe.nist.gov/projects/use_cases/idam
  - Discussion of how the guide is structured and what to expect when one visits the site
    - The practice guide consist of three distinct documents intended for different audiences.
      - A - A stand-alone executive summary targeted to CEOs and senior executives
      - B - A full description of the reference design and the approach to building an instance of the reference design that is targeted at security maangers and engineers
      - C - A how to guide, targeted at IT staff, that provides detailed instructions for installing, configuring, and integrating the products used to build an instance of the reference design
  - Next steps
    - NCCoE may demonstrate the solution as requested.
    - NCCoE may provide a tailored review of the solution and/ or lessons learned with your organization.
    - Please contact us to arrange a demonstration or review.
  - Request to review and submit comments and feedback by October 23, 2015
  - Sincere gratitude expressed by the NCCoE for your participation in the development of this practice guide! This publication is a huge accomplishment. We look forward to future collaboration.
- Situational Awareness project update
  - Situational Awareness notional reference architecture
    - Don reviewed the Situation Awareness notional reference architecture slides

- NCCoE has input from small companies that have no current capability, and large companies who have the need for more automation. This use case is attempting to balance the needs of both.
- Step 1: gather data from existing sensors, aggregation and correlation across silos where feasible.
- Step 2: applies analytical tools to learn about what we haven't learned from just one sensor's returns.
    - We'll probably have a dashboard but part of the intent is to provide information back to the centralized alerting system. There is a need to integrate results of analysis back into individual silos while also pulling information from the separately.
- Step 3: sample mined data to determine "bad behavior" and learn more about what might have happened
- Step 4: could add new sensors to each silo
- Within the scope of a 9 month build it is questionable that we will accomplish all of these steps so we may need to only address a subset of the steps for the practice guide. Of all the things we could do, what is reasonable to plan to do in the next 9 months?

- High level project lifecycle introduction
    - Provide insight into internal NCCoE process
    - We are at P3: forming build team
    - Anticipate/ goal of 9-12 months to complete lifecycle
- Next steps
    - Community – request to review and share IdAM practice guide
    - Community – contact NCCoE to arrange demonstration and/ or tailored review
    - Community – request to review and provide feedback to Situation Awareness use case
    - Community – plan for update calls to take place every 4th Tuesday of the month