

# SG Security Webinar

---

*Monday, March 21<sup>st</sup> – 2-3pm EST*

Chair: Darren Highfill  
Vice-Chair: Bobby Brown  
Secretary: Nick Gerbino

## Agenda

1. Review Agenda / Call for Items of Business **None**
2. NEXT MEETING: Tentative April 4<sup>th</sup>
3. Old Business
  - a. Subgroup updates
    - i. ASAP-SG
      1. Call for how Security Profiles are being used
        - a. IF of value, drop a note to DH or BB on how the document has been used or provided value
      2. Draft due in April for synchrophasors security profile
        - a. To be distributed to NIST, SG Sec, and NASPI
    - M. Ahmadi offered to work on marketing of ASAP-SG – follow-up offline with DH and BB
    - J. Lilley – It should be pointed out that Utilities need to participate more
  - ii. CyberSec-Interop Task Force
    1. No updates since the face to face meeting
  - iii. Usability Analysis Task Force
    1. 3PDA
      - a. Analysis Report
      - b. Procedures and Posting for Review prior to Call for Vote
      - c. Updated link on SharePoint
    2. DMS
      - a. Flag section RE: VPN over Public Networks for clarification/elaboration
        - i. Input incorporated from f2f and have revised wording for review by the task force at next Monday's meeting
  - iv. Embedded Systems Security Task Force
    1. Interest in the TF is growing
    2. Additional tasks for deliverables have been assigned

- a. Secure Protocol Section still needs an owner
    - 3. Create a Foundational Document that contains common requirements across all devices :
      - a. Estimated Completion 7/1/2011
      - b. Device Profiles may contain additional requirements
  - M. Ahmadi – Call for more Utility involvement and AMI Vendors
  - DH – Outreach component for this Task Force
  - Suggestion: Create 1 page flyer for Utilities
  - b. Ad-hoc tasks
    - i. SG Network support (C-I-A rankings)
      - 1. Review of Ron Cunningham’s note 3/15/11
        - a. Comments were due 3/21/2001
        - b. S. Bacik: CIA ranking in the spreadsheet are not the CIA rankings in the NISTIR 7628 but does reference the LIC in the NISTIR 7628
        - c. Call for one more review of the CIA ranking spreadsheet
4. External Engagements, Business, & Issues
  - a. NIST CSWG & PAPs
    - i. NIST AMI-SEC – weekly calls on Tuesdays @1 PM
      - 1. New process being discussed
      - 2. Call for Utility participation
    - ii. PAP10
      - 1. Focused on Third Party Data Access and using the SG Security 3PDA Profile
      - 2. Darren Highfill forwarded the 3PDA Analysis Report from the SG Usability TF
  - b. NERC CIP SDT
    - i. No new update
  - c. IEC TC 57 WG 15
    - i. No new update
  - d. ICSJWG Vendor Subgroup
    - i. Conference call – M. Ahmadi coordinating this effort to have conference call between the leadership of both groups
    - ii. Next ICSJWG Meeting – May 2<sup>nd</sup> – May 5<sup>th</sup>, Dallas TX
  - e. NERC Cyber Attack Task Force
    - i. 2 Task Forces – NERC Cyber Attack and NERC Severe Impact Resiliency
      - 1. Parallel activities that feed into each other
    - ii. Severe Impact Resiliency Task Force
      - 1. Severe (physical or operational loss, i.e. > 1mo.) impacts to utilities
    - iii. Had kickoff, focused on a few key scenarios – purely cyber security
      - 1. S. Bacik to reach out and inform of these groups about SG Security work
      - 2. Will put a report together for NERC BOT by year end

From Bill Muston of Oncor

Publicly accessible information on the NERC Cyber Attack Task Force (CATF):

The CATF was formed as part of a broader NERC initiative on high impact low frequency (HILF) events that would be threats to the bulk power grid (using NERC's definition of bulk power grid). These include pandemic, physical attack, cyber attack, and geomagnetic disturbances.

A press release from NERC on the formation of the CATF is attached, also accessible from the NERC web site. A key sentence from the press release is:

"By developing flexible options, system operators will be better prepared to recognize an event and implement mitigation tactics they may include unique solutions not typical to daily operations. "

The focus is on power grid operators who must be trained and prepared to address a wide variety of operating scenarios and contingencies. My understanding is that the CATF will identify how to help grid operators recognize that a cyber attack is underway, and then respond to it.

The broader NERC initiative and the relationship of the CATF with the other task forces is described in the presentation on the Coordinated Action Plan that is among the presentations in the following zip file from the NERC site:

<http://www.nerc.com/docs/docs/ecoc/March%201%20Joint%20Meeting%20Presentations.zip>

A question arose on the call about the relationship of the CATF with the NERC Smart Grid TF. As per a statement in the presentation, the two are not directly related.

- f. DOE-NIST-NERC collaboration: Risk Management Framework – No new update
5. New Business
- a. OpenADR
    - i. Establish X-talk listserv
    - ii. Analysis
      - 1. Define/map OpenADR actors against 3PDA roles
      - 2. Can OpenADR functionality be expressed using 3PDA use cases?

Question: Why was the 3PDA profile recommended to OpenADR and not the DMS profile?

Response: DMS is applicable to the utility systems that are part of the equation but does not address third party data access; further analysis would be required to determine how best to use each document for OpenADR. 3PDA is a larger issue with OpenADR for now.

- 6. AOB
- 7. Roll Call
  - a. Ahmadi, Mike [mike.ahmadi@granitekey.com](mailto:mike.ahmadi@granitekey.com)

- b. Arensman, Will [<mailto:warensman@swri.org>]
- c. bemmel,vincent vbemmel@trilliantinc.com
- d. Chasko,Stephen stephen.chasko@landisgyr.com
- e. Daniel , Fijitsu
- f. Ellison,Mark ellisonm@dteenergy.com
- g. Fennell,Kevin kevin.fennell@landisgyr.com
- h. freund,mark mcf1@pge.com
- i. Gassko,Irene irene.gassko@fpl.com
- j. Gerbino,Nick nick.j.gerbino@dom.com
- k. Greenfield,Neil ngreenfield@aep.com
- l. griffin,slade slade@enernex.com
- m. Haynes,David dhaynes@aclara.com
- n. Highfill, Darren darren@utilisec.org
- o. Khera,Rohit rxkw@pge.com
- p. Lawrence,Bill william.f.lawrence@lmco.com
- q. Lilley,John jlilley@sempra.com
- r. Loffreda,Daniele daniele.loffreda@us.fujitsu.com
- s. Murray,Eric eric.murray@itron.com
- t. Muston,Bill bill.muston@oncor.com
- u. Pyles,Ward wpyles@southernco.com
- v. Rivaldo,Alan alan.rivaldo@puc.state.tx.us
- w. Robinson,Louis louis.robinson@constellation.com
- x. Smith,Brian brian@enernex.com
- y. Sorebo,Gib sorebog@saic.com
- z. Tolway,Rich rtolway@aps.com