Overview

• Maturation of risk-based assessment processes
• Compliance Oversight Plan (COP) Process Highlights
• Performance Impact
• Implementation Timeline
Maturation of Risk-based Assessment Processes

2016
IRA Process Harmonization

2018
COP Process Harmonization

2019 - 2020
Transition Period
Updated COP Process Highlights

**Enhanced Analysis**
Analysis of inherent and performance data provides an understanding of an entity’s overall inherent risk and performance profile.

**Targeted Oversight**
Provides considerations for an entity’s continuous improvement and a focus to a Regional Entity for its compliance monitoring activities.

**Prioritized Monitoring**
Identifies target interval for oversight, primary monitoring tools, and informs annual planning.

**Single Report**
One report to provide both inherent risk assessment results and the compliance oversight plan.
Inputs - Quantitative and Qualitative Data

Enhanced Analysis

Inherent risk assessment - quantitative entity data such as what you own or operate

Performance assessment - qualitative entity data such as internal controls, culture of compliance, compliance history, event data
COPs will communicate the Regional Entity’s current understanding of a inherent risk and performance profile

COPs will include selected Risk Categories for monitoring

- Provides considerations for an entity’s continuous improvement
- Provides focus for Regional Entity for its compliance monitoring activities
<table>
<thead>
<tr>
<th>Risk Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset/ System Identification</td>
</tr>
<tr>
<td>Entity Coordination</td>
</tr>
<tr>
<td>Identity Management and Access Control</td>
</tr>
<tr>
<td>Emergency Operations Planning</td>
</tr>
<tr>
<td>Operating During Emergencies/ Backup &amp; Recovery</td>
</tr>
<tr>
<td>Training</td>
</tr>
<tr>
<td>Asset/ System Management and Maintenance</td>
</tr>
<tr>
<td>Asset/ System Physical Protection</td>
</tr>
<tr>
<td>Long-term Studies/ Assessments</td>
</tr>
<tr>
<td>Operational Studies/ Assessments</td>
</tr>
<tr>
<td>Modeling Data</td>
</tr>
<tr>
<td>System Protection</td>
</tr>
<tr>
<td>Normal System Operations</td>
</tr>
</tbody>
</table>
Prioritized Monitoring

COPS will include a target monitoring frequency selected based on inherent risk and performance profile.

Identifies target interval for oversight, primary monitoring tools, and informs annual planning.
Prioritized Monitoring

1. Higher inherent risk without demonstrated positive performance - 1 – 3 Years
2. Higher inherent risk with demonstrated positive performance - 2 – 4 Years
3. Moderate inherent risk without demonstrated positive performance - 3 – 5 Years
4. Moderate inherent risk with demonstrated positive performance - 4 – 6 Years
5. Lower inherent risk without demonstrated positive performance - 5 – 7 Years
6. Lower inherent risk with demonstrated positive performance - 6 + Years
COPs establish target intervals for engagements based off of inherent risk and performance profile

**Category 1**

The target monitoring interval for a higher risk entity without demonstrated positive performance is once every 1 – 3 years.

A Regional Entity will use one or a combination of the following CMEP Tools:
- Audit (on or off-site)
- Self-Certifications
- Spot Check

**Category 2**

The target monitoring interval for a higher risk entity with demonstrated positive performance is once every 2 – 4 years.

A Regional Entity will use one or a combination of the following CMEP Tools:
- Audit (on or off-site)
- Self-Certifications
- Spot Check
Contents of the COP Report

1. Purpose

2. Analysis and Results

3. Oversight Strategy

App. A: IRA Results Summary

App. B: Standards and Requirements for Monitoring
• Throughout the second half of 2019 and the beginning of 2020, Regional Entities will begin implementation of new COP summaries.

• Industry outreach will begin in July 2019 and continue through 2020.
Questions and Answers
OUTREACH PROGRAMS

Your Choice

PHYSICAL ASSESSMENT

CYBER ASSESSMENT

PHYSICAL AND CYBER ASSESSMENT
NPCC PSWG

As of 1/1/2019 NPCC has developed a Physical Security Work Group with the intent of:

Emphasizing physical security, establish a vehicle to enable NPCC registered entity’s physical security personnel to network, share information, best practices, technology, and strategies in a controlled, confidential setting.
To date the group has initiated communication and met with the SERC Physical Security Group and the CEA representative from the RCMP.
Training Opportunities

NYPD COUNTERTERRORISM TRAINING MODULES-NYPD SHIELD

- TERRORISM AWARENESS FOR THE SECURITY PROFESSIONAL
- VEHICLE BORNE EXPLOSIVE DEVICE SECURITY CHECKPOINT OPERATIONS
- ACTIVE SHOOTER
- DETECTING HOSTILE SURVEILLANCE
- SUSPICIOUS MAIL AND PACKAGES
- CRITICAL INFRASTRUCTURE PROTECTION
- INTRO TO MARITIME INFRASTRUCTURE PROTECTION
- BUILDING DESIGN FOR HOMELAND SECURITY
- SURVEILLANCE DETECTION FOR CRITICAL INFRASTRUCTURE OPERATORS AND SECURITY STAFF
- PORT AWARENESS
TRAINING cont’d

DESIGN BASIS THREAT

WHAT IS IT?
BASIC PRINCIPLES
• WHO SHOULD PARTICIPATE
BRIEF DESCRIPTION
• SCENARIOS
• TIMELINES
HOW CAN IT BENEFIT ME?

WORDS OF WISDOM:
If you are going to fight a problem, fight as if you are the third monkey on the ramp to Noah’s Ark and brother, it’s starting to rain!!
QUESTIONS?
CONTACT

Peter Scalici, CHPP
Manager, Security Outreach Programs
pscalici@npcc.org (The best way to contact me)
212 205-7065
Cyber Hygiene

- Insider Threats
- Ransomware
- Cyber Security Updates
  CISA Guidance
  (Cybersecurity Infrastructure Security Agency)
Verizon Data Breach Investigations Report 2019

Reference

  https://enterprise.verizon.com/resources/reports/dbir/
Insider Threats

Malicious insiders
- Disgruntled employees
- Off-boarding employees
- Other motives

Negligent insiders
- Users not cyber aware
- Un-practiced good cyber-hygiene
- Information Technology
Insider Threat Vectors

- E-mail
- USB Devices
Insider Threat Prevention

**Tools**
- End User Behavioral Analytics (EUBA)
- Privileged Access Management (PAM)
- Data dashboarding (SIEMs)

**Techniques**
- Enforcement policies procedures
- Baselining

Defense in Depth (castle approach)
- Systems segmentation
Ransomware

https://www.us-cert.gov/Ransomware

- Restricting to “least privilege”
- Application whitelisting
- Enable strong email spam filtering and scanning
- Configure firewalls to block known malicious IP address(s)
- ** Regular backup rotations stored offline**
Recent Vulnerabilities

- Bluetooth BR/EDR devices vulnerable to key negotiation attacks (9/3/19)
- Pulse Secure VPN multiple vulnerabilities (10/22/19)
- Multiple D-Link routers vulnerable to remote command execute (10/25/19)
- Vulnerabilities found Cobham EXPLORER 710 satcom terminals (10/11/19)

https://www.us-cert.gov/
https://www.kb.cert.org/vuls/
Product End of Life

Effective January 01, 2020
(Windows 7 & Server 2008 R2)

CISA - AA19-290A Alert

Microsoft officially ending extended support: Windows 7 & Server 2008 R2
- Free technical support
- Online technical assistance
- Automated fixes
- Software security update(s)

Questions

Cecil Elie
NPCC Senior CIP Analyst
celie@npcc.org
References

1 - https://enterprise.verizon.com/resources/reports/dbir/
3 - https://www.onespan.com/blog/phishing-emails-how-protect-your-customers-when-using-e-signature
5 - https://www.insurancejournal.com/magazines/mag-features/2019/06/03/528088.htm
NPCC 2019 Fall Compliance and Standards Workshop

NAGF Overview and Initiatives

Wayne Sipperly
NAGF Executive Coordinator
wsipperly@generatorforum.org
Agenda

- NAGF Overview
- Collaboration: Public Site & Groupsite
- NAGF Working Groups and Members
- Current Activities and Initiatives
- How to join the NAGF
- Questions
Who/What is the NAGF?

The NAGF is an independent, member-driven, non-profit organization of generator owners and operators, focused on NERC and other grid reliability issues.

The NAGF’s mission is to promote the safe, reliable operation of the generator segment of the bulk power system through generator owner and operator collaboration with others who have a vested interest in the reliable operation of the bulk power system.
Collaboration: Public Site

http://generatorforum.org/

NORTH AMERICAN GENERATOR FORUM

The power to make a difference
Welcome to the North American Generator Forum

The North American Generator Forum (NAGF) was founded in 2009 as a vehicle for generator owners and/or operators to address issues related to registration, compliance, standards development and other NERC-related topics. In 2013, the North American Generator Forum, Inc. became a non-profit, dues-based corporation.

We provide entities who are generator owners and operators in North America a means to collaborate and communicate with FERC, NERC, the Regional Entities, the Canadian Provinces and other organizations with missions similar to ours, with the ultimate goal of improving the reliability of the bulk power system.

More information is available at: http://generatorforum.org/

REQUEST TO JOIN BY CLICKING HERE
NAGF Working Groups

- Peer Review
- Security Practices / CIP
- Standards Review Team
- Variable Resources
- Cold Weather Preparedness
## NAGF members

<table>
<thead>
<tr>
<th>Ameren Missouri</th>
<th>Clearway Energy</th>
<th>Dominion Energy</th>
<th>FMPA</th>
<th>NAES Corporation</th>
</tr>
</thead>
<tbody>
<tr>
<td>American Electric Power</td>
<td>DTE Energy</td>
<td>Duke Energy</td>
<td>FPL</td>
<td>NYP A</td>
</tr>
<tr>
<td>AECI</td>
<td>E.ON</td>
<td>EDR Renewables</td>
<td>Great River Energy</td>
<td>NextEra Energy</td>
</tr>
<tr>
<td>Austin Energy</td>
<td>ENGIE</td>
<td>Entergy</td>
<td>Indeck Energy</td>
<td>North Carolina Electric</td>
</tr>
<tr>
<td>Avista Corp</td>
<td>Entergy</td>
<td>Essential Power</td>
<td>Independence P &amp; L</td>
<td>NOVA Scotia Power Inc.</td>
</tr>
<tr>
<td>Basin Electric Power</td>
<td>EthosEnergy</td>
<td>Evergy</td>
<td>Invenergy</td>
<td>NCPA</td>
</tr>
<tr>
<td>Black Hills Corporation</td>
<td>Exelon Generation</td>
<td>Lewis County PUD</td>
<td>Lakeland Electric</td>
<td>NRG</td>
</tr>
<tr>
<td>BP Wind</td>
<td>First Energy Corp.</td>
<td>LG&amp;E and KU</td>
<td>Pattern Gulf Wind</td>
<td>NRG</td>
</tr>
<tr>
<td>Braintree Electric Light</td>
<td>FirstLight Power</td>
<td>M&amp;MWEC</td>
<td>Pattern Energy Group</td>
<td>NG&amp;G</td>
</tr>
<tr>
<td>Capital Power</td>
<td></td>
<td>MidAmerican Energy</td>
<td>Penobscot Energy</td>
<td>SunPower</td>
</tr>
<tr>
<td>CCI Rensselaer</td>
<td></td>
<td>Minnesota Power</td>
<td>ProEnergy Services</td>
<td>Sunflower Electric</td>
</tr>
<tr>
<td>Chelan County PUD</td>
<td></td>
<td>Muscatine Pwr &amp; Wtr</td>
<td>Santee Cooper</td>
<td>Talen Energy</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>TEP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Tri-State G&amp;T</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>TVA</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>US BR</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>US SBU</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>WEC Energy Group</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Xcel Energy</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
NAGF’s dual focus

- **Compliance with existing Standards**
  - “The here and the now”
  - Collaborative efforts
  - Best Practice sharing
  - Discussion boards, file cabinet, etc. on Groupsite

- **Shaping policy**
  - Helping paint the futurescape
  - Ensuring the unique perspective of the generation segment is understood and accounted for.
  - Improve “first time success” of new regulations
Activities and Initiatives

- **FERC Communications**
  - FERC and NERC Cold Weather Event January 2018 Draft Report:
    - Conference Call with NAGF to review draft report and findings on June 18, 2019
    - Confidential information presented
    - NAGF provided feedback on draft findings
  - FERC/NERC White Paper on CIP NOPs:
    - Provide transparency and public access regarding CIP violation information
    - NAGF provided comments regarding the proposed public information sharing format
NERC Communications:

- NAGF Standards Review Team (SRT) Working Group
  - Submit comments as part of NERC Balloting and Commenting process
  - Monthly conference calls with NERC staff and NAGF members to discuss project status, concerns and generator sector participation
  - Periodic Standard Reviews
  - NERC Projects

- NERC BOT Policy Input and NAGF Activities Summary
  - Reliability and Security Technical Committee (RSTC) Proposal
  - NERC Supply Chain Report
NERC Communications:

☑️ PRC-005-6 and Digital AVR Protective Function Testing
  - Issue focused on testing of Automatic Voltage Regulator (AVR) protective functions and applicability of PRC-005-6:
    - Open questions regarding scope of applicability to AVR protective systems, testing, crossover compliance with PRC-019 and MOD-026
  - NAGF Standard Authorization Request (SAR):
    - Clearly limit scope of AVR protective functions to elements that open a breaker directly, via lockout, or tripping aux relays
    - Provide acceptable methods of testing
    - Evaluate cascading applicability to other NERC Standards
  - Project 2019-04: Modifications to PRC-005-6:
    - Initiated July 30, 2019
    - SAR comment period 7/30/19 – 8/28/19
    - Drafting team reviewing comments received
NERC Communications:

NAGF Standardized Procedure Templates for Generator Low Impact Cyber Systems

- Finalized Generic Low Impact procedures for CIP-003-7/8:
  - Physical Security
  - Electronic Access
  - Transient Cyber Assets and Removable Media
  - CIP Exceptional Circumstances
- Incorporates comments provided by NERC and the EROs
- Provides NAGF members with a template for developing low impact procedures.
- Members are currently implementing and testing
- Available to all NAGF members
NERC Communications:

- NERC Electromagnetic Pulses (EMP) Task Force
  - Conference call held with NAGF membership on August 20, 2019:
    - Reviewed work performed to date
    - Draft strategic recommendations
    - Next steps
      - Draft Strategic Recommendations comment period 08/30/19 – 09/30/19
      - Review comments received
      - Submit for approval at the NERC BOT meeting November 5th
    - Need for generator segment engagement
  - NAGF continues to actively participate on this task force
NERC Communications:

- **Inverter-based Resource Performance Task Force (IRPTF)**
  - NERC Reliability Guideline posted: Recommended Improvements to IBR Interconnection Agreements
    - [Recommended Improvements to IBR Interconnection Agreements](https://www.nerc.com/comm/OC_Reliability_Guidelines_DL/Reliability_Guideline_IBR_Interconnection_Requirements_Improvements.pdf)

- **Continuing Work**
  - IEEE working on development of a new performance standard P2800 – Interconnection and Interoperability of Inverter-Based Resources Interconnecting with Associated Transmission Electric Power Systems
  - Guidelines
    - BPS Reliability Studies w BPS Battery Storage and Hybrid Resources
    - BPS Protection Practices w Increasing Penetrations of BPS IBR
  - White Papers
    - FFR Fundamentals and Reliability Needs
    - Roadmap for Reliability under High IBR Connected to the BPS
Activities and Initiatives (continued)

- **NERC Communications:**

  - NAGF-ESIG-NERC Battery Storage, Hybrid Resources, Frequency Response, and Grid Services Workshop
    - September 17-18, 2019 at the NERC Offices in Washington D.C. and Atlanta
    - Approximately 90 participants from DOE, FERC, NERC, and industry
    - Six (6) discussion panels:
      - Technical capabilities of Battery Storage Systems
      - Hybrid projects: Motivations, Drivers, and Challenges
      - Planning, Modeling, and Interconnection with Storage/Hybrid Systems
      - ISO/RTO Markets and Storage/Hybrid Participation
      - PFR and Grid Services Considerations – Conventional and IBR
      - Policymaker Viewpoints on Grid Services and Grid Transformation
    - The presentations are located on the NERC website: [https://www.nerc.com/pa/rrm/Resources/Pages/Conferences-and-Workshops.aspx](https://www.nerc.com/pa/rrm/Resources/Pages/Conferences-and-Workshops.aspx).
Regional Entity (RE) Communications:

- Increasing interaction with RE’s:
  - NAGF CIP Low Impact Procedure templates
  - NPCC – Spring/Fall Workshops & DER Forum
  - Participation at RF, SERC, and TRE compliance workshops
  - Additional opportunities under discussion

- RE News Letters
  - Update of key NAGF activities included in periodic RE news letters:
    - RF
    - SERC
    - TRE
Regional Entity Communications:

- NPCC Distributed Energy Resources (DER) Forum
  - NAGF continues to support
  - Opportunity for open discussion of DER issues, enhance awareness, understand impacts to the BES, and facilitate the integration of DER
    - Second day of NPCC RSC meetings
  - Key Issues:
    - Impacts on NPCC UFLS-UVLS programs
    - Potential to impact the “Reliable Operation” of the BES/BPS
    - Coordinate interoperability between Transmission and Distribution for DER
Activities and Initiatives (continued)

- **2019 NAGF Annual Meeting & Compliance Conference**
  - October 15-17, 2019 @ NERC’s Offices, Atlanta
  - SERC President & CEO Jason Blake Keynote Address
  - O&P and CIP topics:
    - CIP Low Impact Implementation (CIP-003-7) – How’s Its Going?
    - CIP-013 Supply Chain Implementation
    - Internal Controls Evaluation
    - Battery Integration – Issues and Successes
    - DHS/Cybersecurity and Infrastructure Security Agency (CISA) update
  - Panel Discussions:
    - REs – MRO, NPCC, RF, SERC, TRE, and WECC
    - ISO/RTO – CAISO, ISO-NE, MISO, and PJM
Activities and Initiatives (continued)

- **NAGF- NATF PRC-027-1 Collaboration Effort**
  - Initiated per member’s interest and request
  - NATF Protection System Coordination document update
    - Focus on entity coordination as it applies to generation
    - Data exchange and communication paths
  - NAGF member representatives to participate:
    - EthosEnergy
    - NAES
    - Ready Engineering
    - Southern Company
  - Kickoff meeting scheduled for November 5th
Joining the NAGF

Visit our website: http://nagf.groupsite.com/
Click on: REQUEST TO JOIN BY CLICKING HERE

-Or-

Send an email requesting membership to: wsipperly@generatorforum.org
Q & A
E-ISAC NPCC 2019 Workshop Presentation is not available for distribution.
Enabling Security and Compliance Using Cloud Services

November 21, 2019

Samara Moore, AWS Security Assurance
Regulatory & Industry Security Engagement (RISE), Lead Americas
Enabling security and compliance using cloud services

- **What** is cloud computing and how does it work?
- **Why** are organizations choosing cloud services?
- **How** are customers managing security using AWS?
- **How** do CIP standards align with cloud services?
Equipment Resources and Administration

Contracts

Cost

Traditional Infrastructure

Cloud Services

No Up Front Expense Pay for what you Use

Improve Time to Market & Agility

Scale Up and Down

Self-Service Infrastructure
AWS Global Infrastructure

- AWS Regions are comprised of multiple AZs for high availability, high scalability, and high fault tolerance. Applications and data are replicated in real time and consistent in the different AZs.

22 Regions – 69 Availability Zones

A Region is a physical location in the world where we have multiple Availability Zones.

Availability Zones consist of one or more discrete data centers, each with redundant power, networking, and connectivity, housed in separate facilities.
Enabling security and compliance using cloud services

- Inherit global security and compliance controls
- Scale with superior visibility and control
- Highest standards for privacy and data security
- Automate with comprehensive, integrated security services
- Largest network of security partners and solutions
Inherit global security and compliance controls
Traditional on-premises security model

Customers are responsible for end-to-end security in their on-premises data centers.

Customer data

Platform, applications, identity, & access management

Operating system, network, & firewall configuration

Client-side data
- Encryption & data integrity authentication

Server-side data
- File system and/or data

Network traffic
- Protection (encryption, integrity, identity)

Software

Compute
Storage
Database
Networking

Hardware/AWS Global Infrastructure

Regions
Availability zones
Edge locations
Shared responsibility model

Customer responsibility will be determined by the AWS Cloud services that a customer selects.

AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud.
Alignment with compliance security objectives

**Identity & access management**
- Access Authorization, Audit, and Revocation
- Define, enforce, and audit user permissions across AWS services, actions, and resources

**Detective controls**
- Security Event Logging and Monitoring
  - Gain the visibility needed to spot issues before they impact the business, improve security posture, and reduce the risk profile of the environment

**Infrastructure protection**
- Managing Security Perimeters and Data Flows, Patch and Vulnerability Management
  - Reduce surface area to manage and increase privacy for and control of your overall infrastructure on AWS

**Data protection**
- Managing Encryption, Data Access, Decommissioning / Sanitization
  - Data encryption and management services, employ features for data protection (data management, data security, and encryption key storage)

**Incident response**
- Incident Response, Testing and System Recovery
  - Use tools to automate aspects of containing events and returning to a known good state
Financial industry regulatory authority

• Looks for fraud, abuse, and insider trading over nearly 6 billion shares traded in U.S. equities markets every day
• Processes approximately 6 terabytes of data and 37 billion records on an average day
• Went from 3-4 weeks for server hardening to 3-4 minutes
• DevOps teams focus on automation and tools to raise the compliance bar and simplify controls
• Achieved incredible levels of assurance for consistencies of builds and patching via rebooting with automated deployment scripts

“I have come to realize that as a relatively small organization, we can be far more secure in the cloud and achieve a higher level of assurance at a much lower cost, in terms of effort and dollars invested. We determined that security in AWS is superior to our on-premises data center across several dimensions, including patching, encryption, auditing and logging, entitlements, and compliance.”

—John Brady, CISO FINRA
Thank you!

Samara Moore, AWS Security Assurance Regulatory & Industry Security Engagement (RISE), Lead Americas
samaranm@amazon.com
Supply Chain Risk Management
NPCC 2019 Fall Compliance and Standards Workshop
November 21, 2019

Tony Eddleman
Nebraska Public Power District
Chair, NERC CIPC Supply Chain Working Group (SCWG)
Discussion Topics

- New and Updated NERC Reliability Standards
- NERC Website Resources
- NERC Supply Chain Working Group (SCWG)
  - Security Guidelines – Short Papers
- North American Transmission Forum (NATF)
Supply Chain Risk Management Regulatory Requirements

- The Federal Energy Regulatory Commission (FERC) approved new Supply Chain Risk Management requirements and these will be effective on July 1, 2020
  - CIP-013-1 (new); CIP-005-6 (updated); CIP-010-3 (updated)
  - Initial scope is limited to Control Centers and more impactful substations and generators
  - FERC is evaluating whether these new requirements should apply to basically all generation and transmission
    - NERC 1600 Data Request
R1. Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems. The plan(s) shall include:

1.1. One or more process(es) used in planning for the procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).
Supply Chain Cyber Security Risk Management Plan(s)

- First - what parts, equipment, services, etc. does this apply?
  - High and Medium Impact Bulk Electric System (BES) Cyber Systems (see NERC Standard CIP-002)
    - A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact.
Supply Chain Cyber Security Risk Management Plan(s)

- Second, what does risk look like to you?
  - Individual risk plans may, and probably will be different for each of us!
    - EPRI posted a report: Supply Chain Cyber Security Risk Management Plan(s) (July 2018)
      - Report provides a basic understanding of how Cyber Systems are in use in the Electric Industry
      - Discusses Common-Mode Vulnerabilities (how many do you have and where are they located)
      - Please read this report!
  - Risk is based on where the Cyber Asset will be used, how it will be used, access to the Cyber Asset (routable or non routable)
  - What is the risk to the BES if the Cyber Asset is compromised?
Supply Chain Cyber Security Risk Management Plan(s)

- If CIP-013 is applicable to your entity, you must have one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems.
  - If a vendor or service provider is using a 3rd party to assess their products or services, great, but you still have to have your own plan!
  - If a vendor or service provider is certified by another process, great, but you still have to have your own plan!
Supply Chain Cyber Security Risk Management Plan(s)

1.1. One or more process(es) used in **planning for the procurement of BES Cyber Systems** to **identify and assess** cyber security **risk(s)** to the Bulk Electric System from vendor products or services resulting from:
   - (i) procuring and installing vendor equipment and software; and
   - (ii) transitions from one vendor(s) to another vendor(s).
1.2 One or more process(es) used in procuring BES Cyber Systems that address the following, as applicable:

- 1.2.1 Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;
- 1.2.2 Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;
- 1.2.3 Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;
NERC CIP-013-1
Reliability Standard

• 1.2 One or more process(es) used in procuring BES Cyber Systems that address the following, as applicable:
  ▫ 1.2.4. Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;
  ▫ 1.2.5. Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System; and
  ▫ 1.2.6. Coordination of controls for (i) vendor-initiated Interactive Remote Access, and (ii) system-to-system remote access with a vendor(s).
Supply Chain Cyber Security Risk Management Plan(s)

- **R1.** Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems. The plan(s) shall include:
  - R1.1 - planning for the procurement
  - R1.2 - used in procuring BES Cyber Systems

- If you have questions on your plans, please discuss them with your Regional Entity
NERC CIP-013-1
Reliability Standard

• **R2.** Each Responsible Entity shall **implement** its supply chain cyber security risk management plan(s) specified in Requirement R1.

• **R3.** Each Responsible Entity shall **review and obtain CIP Senior Manager or delegate approval** of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months.
NERC CIP-005-6
Reliability Standard

- Reliability Standard CIP-005-6 includes two new parts, Parts 2.4 and 2.5, to address vendor remote access
  - 2.4 Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).
  - 2.5 Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).
NERC CIP-010-3
Reliability Standard

- Reliability Standard CIP-010-3 includes a new part, Part 1.6, to address software integrity and authenticity
  - 1.6 Prior to a change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5, and when the method to do so is available to the Responsible Entity from the software source:
    - 1.6.1. Verify the identity of the software source; and
    - 1.6.2. Verify the integrity of the software obtained from the software source.
NERC Website
https://www.nerc.com
NERC Website

Supply Chain Risk Mitigation Program

On August 10, 2017, the NERC Board of Trustees (Board) adopted proposed Reliability Standards CIP-005-6, CIP-010-3, and CIP-013-1 (Supply Chain Standards), addressing cyber security supply chain risk management issues, and approved the associated implementation plans. NERC has initiated a collaborative program with industry, trade organizations, and key stakeholders to manage the effective mitigation of supply chain risks.

In adopting the Supply Chain Standards, the Board concurrently adopted additional resolutions related to their implementation and evaluation. The resolutions outlined six actions, developed by NERC management and stakeholders, to assist in the implementation and evaluation of the Supply Chain Standards and other activities to address potential supply chain risks for assets not currently subject to the Supply Chain Standards. Those resolutions, in summary form, include the following actions:

**Action 1:** Support Effective and Efficient Implementation

NERC to commence preparations for implementation of the Supply Chain Standards using similar methods as the CIP V5 transition and regularly report to the Board on those activities.

**Action 2:** Cyber Security Supply Chain Risk Study

Study the nature and complexity of cyber security supply chain risks, including risks associated with low impact assets not currently subject to the Supply Chain Standards, and develop recommendations for follow-up actions that will best address any issues identified.

**Action 3:** Communicate Supply Chain Risks to Industry

Communicate supply chain risk developments and risks to industry and in connection with the Cyber Security Supply Chain Risk Study.

**Action 4:** Forum White Papers

The Board requests the North American Transmission Forum and the North American Generation Forum to develop white papers to address best and leading practices in supply chain management, as described in the resolution.

**Action 5:** Association White Papers

**Key Resources**

- Board Resolution
- Supply Chain FERC Order
- Supply Chain Standard
- DOE Procurement Language
- Supply Chain Small Group Advisory Sessions FAQs
- Managing Cyber Supply Chain Risk: Best Practices for Small Entities
- EPRI Supply Chain Risk Assessment Report
- NATF Cyber Security Supply Chain Risk Management Guidance
- NAGF Cyber Security Supply Chain Management White Paper
- Supply Chain Cyber Security Practices - Letter to Industry
- Final Supply Chain Report
- Final Supply Chain Report redline to Board policy input version
- Executive Order on Securing the Information and Communications Technology and Services Supply Chain
- Draft Supply Chain Risk Assessment Data Request
- Draft Supply Chain Risk Assessment Data Request Unofficial Comment Form
- Final Supply Chain Risk Management Assessment Data Request
- Final Supply Chain Risk Management Assessment Data Request - Redline to Draft
- Supply Chain Risk Assessment Data Request Response to Comments
- Security Guidelines

**Endorsed Implementation Guides**

- Cyber Security Supply Chain Risk Management Plans
- CIP-010-3 R1.6 Software Integrity and Authenticity (NATF)
- CIP-013-1, R1, R2 - Supply Chain Management (NATF)
Managing Cyber Supply Chain Risk-Best Practices for Small Entities
EPRI Supply Chain Risk Assessment Report (July 2018)
North American Transmission Forum (NATF) (June 20, 2018)

NATF CIP-013-1 Implementation Guidance

- Reliance on Independent Assessments of Vendors as an Acceptable Means of Identifying and Assessing Vendor Risk
- Using Independent Assessments of Vendors
  - The third-party assessment is made part of the entity’s overall process used in procuring BES Cyber Systems that addresses each of the security issues listed in Part 1.2 of Requirement R1
- Attachment A – Cyber Security Criteria
- Attachment B – Cyber Security Framework Mapping
Supply Chain Cyber Security Practices
(NERC CIPC Approved March 6)

March 6, 2019

Dear Electric Industry Vendor Community:

Re: Supply Chain Cyber Security Practices

On July 21, 2016, the Federal Energy Regulatory Commission (FERC) directed the North American Electric Reliability Corporation (NERC) to develop or modify necessary Reliability Standards to address concerns that relate to supply chain risk management for industrial control system (ICS) hardware and software as well as computing and networking services associated with Bulk Electric System (BES) operations.¹ In October of 2018, FERC approved the Reliability Standards,² which will become effective on July 1, 2020.

This letter is intended to inform vendors to the electric utility industry of these new regulatory requirements and open a dialogue about the importance to electric utilities of working with their vendors to implement controls to manage supply chain security risks. Vendor products and services have a significant potential to impact the reliability of the BES. It is imperative that electric utilities work with their vendors to implement technical controls and processes to allow utilities to both meet their new regulatory obligations under NERC’s Critical Infrastructure Protection (CIP) standards and to provide for a secure grid.
NERC Report Provided to FERC

Cyber Security
Supply Chain Risks
Staff Report and Recommended Actions

May 17, 2019
NERC Cybersecurity Supply Chain Risks

- NERC Staff recommends revising the standard to **include EACMS** that provide electronic access control (excluding monitoring and logging). NERC Staff also recommends revising the Supply Chain Standards to **include PACS** that provide physical access control (excluding alarming and logging) to **high and medium impact BES Cyber Systems**. In the interim, NERC Staff expects that entities will apply supply chain security practices to EACMS and PACS to help mitigate supply chain risks associated with these devices.
  - EACMS - Electronic Access Control or Monitoring Systems
  - PACS - Physical Access Control Systems
NERC Cybersecurity Supply Chain Risks

• At this time, NERC Staff **does not recommend** that the Supply Chain Standards be modified to include all low impact BES Cyber Systems.

• **As a best practice**, NERC staff expects entities that have medium or high impact BES Cyber Systems will voluntarily apply CIP-013-1 Requirement R1 supply chain risk management plans to low impact BES Cyber Systems.
EEI Procurement Language

Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk

Version 1.0

https://www.eei.org/issuesandpolicy/Pages/Security.aspx
NERC CIPC Supply Chain Working Group (SCWG)

• Very active
• Large membership
  ▪ Currently over 150 participants
  ▪ Partnership with industry
    o Registered Entities
    o Service Providers
    o Consultants
    o Product Providers
    o FERC, NERC, and Regional Entities
    o EEI, EPRI, and NATF
• Exceptional Experience and Knowledge
SCWG Short Papers - Security Guidelines

- Good Business Practices Provided in Short Papers
  - Use the experience and expertise of the small team and the SCWG to identify best practices and challenges to the reader.
    - What are the pitfalls the reader should know about and avoid?
    - How does the reader learn about a specific topic and move forward to implement a solid program to improve reliability?
    - **Short papers are not compliance implementation guidance.**
  - Short papers are limited to approximately 3 pages each.
    - The papers should be written to convey general guidance to the reader without having to read a lengthy document.
    - Not trying to make the reader an expert.
  - Provide the reader references – reader can research for more information.
SCWG Short Papers - Security Guidelines

- Supply Chain and Risk Considerations for Open Source Software
  - Sub-team Lead: George Masters, Schweitzer Engineering Laboratory, Inc.
- Secure Equipment Delivery
  - Sub-team Lead: Wally Magda, WallyDotBiz LLC
- Supply Chain Security Guidelines on Provenance
  - Sub-team Lead: David Steven Jacoby, Boston Strategies International
- The Supply Chain Cyber Security Risk Management Lifecycle
  - Sub-team Lead: Tom Alrich, Tom Alrich LLC
- The Vendor Risk Management Lifecycle
  - Sub-team Lead: Tom Alrich, Tom Alrich LLC
SCWG Short Papers - Security Guidelines

- Short Papers Sent to CIPC for Approval to Post
  - Vendor Identified Incident Response Measures
    - Sub-team Lead: Steven Briggs, TVA
  - Supply Chain Risks Related to Cloud Service Providers
    - Sub-team Lead: Brenda Davis, CPS Energy

- Short Paper in Development
  - Considerations for threat-informed procurement language
    - Sub-team Lead: Chris Walcutt, DirectDefense
How do we Implement the new NERC Requirements?

<table>
<thead>
<tr>
<th>Individual Companies</th>
<th>Jointly Through Collaboration</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Up to 1411 utilities gathering data for same standard</td>
<td>• North American Transmission Forum (NATF) Supply Chain Core Team</td>
</tr>
<tr>
<td>▫ Vendors are trying to engage with hundreds of companies with diverse programs and</td>
<td>▫ Cyber security criteria developed with NATF members</td>
</tr>
<tr>
<td>questions</td>
<td></td>
</tr>
<tr>
<td>• Very difficult for companies to perform individual vendor site visits to verify</td>
<td>• Future: Vendor reviews / site verifications</td>
</tr>
<tr>
<td>programs</td>
<td>▫ Certifications</td>
</tr>
<tr>
<td>▫ Utilities will struggle to travel to multiple vendors</td>
<td>▫ 3rd party assessments</td>
</tr>
<tr>
<td>▫ Vendors will struggle hosting multiple utilities</td>
<td></td>
</tr>
</tbody>
</table>
Implementation

- What if industry had standardized criteria?
  - Vendors and service providers wouldn’t be flooded with numerous questions from numerous utilities
  - Individual utilities wouldn’t have to develop their own criteria
North American Transmission Forum

Supply Chain Activities Widely Supported

- **What is the criteria or security framework?**
  - NATF
  - CIPC SCWG
  - ISO/RTO Council

- **How is a supplier’s adherence to criteria verified and reported?**
  - NATF
  - Suppliers
  - Trades
  - Auditors/Certification Authorities

- **How does an entity determine the risk of making a purchase from the supplier?**
  - NATF
  - CIPC SCWG

- **How should an entity make the purchase?**
  - EEI
  - CIPC SCWG
  - DOE

- **How should an entity monitor the supplier/product risk after purchase?**
  - NATF
  - CIPC SCWG
North American Transmission Forum

NATF Criteria

Final Criteria Spreadsheet and Application Guide are Posted for Open Distribution

- Criteria focuses on supply chain cyber security practices
  - Criteria requires adherence to an existing cyber security framework to demonstrate broader cyber security practices
- Contains 68 criteria and 26 organizational information considerations
  - Designation of whether each criteria is required by the NERC CIP Standards or included for security practice
  - Mapping to 3 sample existing frameworks (NIST, ISO 27001, SOC2)
- Application Guide provided contains additional information
North American Transmission Forum

Projected Timeline for NATF Activities

**Summer 2019**
- Develop Criteria
  - June 2019
- Application of Criteria
  - July 2019

**Fall 2019**
- Determination of Maintenance of Criteria
  - Fall 2019
- Proof of Concept
  - September 2019

**Winter 2019**
- Common Reporting and Questionnaire Form(s)
  - By end of year 2019
- Verification of Supplier Adherence to Criteria
  - By end of year 2019
North American Transmission Forum

NATF Supply Chain Steering Team

- Chuck Abell (Ameren) (NATF Criteria Steering Team)
- Paul Ackerman (Exelon Corporation)
- James Chuber (Duke Energy)
- Tony Eddleman (NPPD) (NATF Criteria Steering Team)
- Shannon Hammett (Southern Co)
- Steve McElwee (PJM)
- Jeffrey Sweet (AEP)
- Brenda Truhe (PPL Electric Utilities) (NATF Criteria Steering Team)
  - Advisory role
North American Transmission Forum

NATF Proof of Concept

Proof of Concept for existing security framework(s)

- Collaborating with entities, suppliers and third-party assessors to develop strawman model
  - Currently being developed under limited distribution
  - Model prepared for socialization and broader input
  - Model is based on EMS/higher risk products
    - Model must provide for scalability
- Streamlining verification and reporting
- Use of established reporting systems and existing frameworks recognized by other industries
Timeline to Think About

**Spring 2019**
Drafting Risk Management Plan; Researching Industry Resources

**Fall 2019:**
Finalize Risk Management Plan; Start Discussions with Vendors & Service Providers

**Spring 2020:**
Begin using process to identify any issues before compliance date

**Summer 2019:**
Develop Cyber Security Criteria with NATF

**Winter 2019-2020:**
Determine 3rd party assessments; Develop tracking tool for compliance documentation

**Compliance Date: July 1, 2020**
Summary

• Resources are available to develop your Risk Management Plans

[**Industry can work together**] through the NATF criteria to standardize procurements from a utility perspective and a vendor perspective

• Certifications and 3\textsuperscript{rd} party assessments can improve reliability and prevent unnecessary work and stress for our industry

• If you don’t have your Risk Management Plan developed, you should start now!
Questions?
Fundamentals of IEC 61850 & Cyber Security Concerns


Deepak Maragal, PhD, PE
Manager, System Integration and Test
New York Power Authority
Agenda

• What is IEC 61850? & What NPCC?
• Communication Protocols & Applications
• Cyber Security Concerns and Threats
• Recommended Practice for Isolation
• Redundancy in networking
• Cyber Mitigation Strategies
• Why do IEC 61850?
• IEC 61850 Resources
What is IEC 61850?

New Substation Protocol
Relay Evolution
IEC 61850 Standard Defines

Nomenclature & Data Model

- Most-all substation equipment & functions: XCBR, PIOC, CILO
- Similar to DNP3: (Quality + StVal/CtlVal) lot more abstraction

Standard Protocols

- Ethernet only protocols: GOOSE, Sample Values
- IP protocol: MMS (IEC61850 part 8-1 maps services to MMS)

Engineering process

- Hierarchical Top-down approach: Classification defined
- Std. data structure and Std. configuration files: SCD, CID, IID,
IEC 61850 Standard

Functions
- Definitions & Nomenclature
- Parameters & Attributes

Communication
- Medium
- Protocols
- Security
- Time Synchronization

Architecture
- Substation design approaches
  - Top-down
  - Bottom-up
What encompasses IEC 61850?

Design (PRC)
Operation (O&P)
Control (PRC & CIP)
Upgrades (PRC & CIP)
Monitoring (O&P, CIP)
Protection (PRC)
Security (CIP)

COMPLIANCE
1) Logs & Evidence
2) Internal Controls
3) 

New Way of LIFE
Types of Communication Protocols

Multicast (Ethernet)
Publisher <-> Subscriber/s

Client-Server (IP)
Server -> Client/s
Protocol Stack

802.1Q VLAN tagging
- Permits Isolation
- Application handled

802.1P VLAN priority
- Traffic flow prioritization
- Handled at Network switch
Typical IEC 61850 Substation Architecture
Cyber Concerns & Threats: Network

Critical
- Communication network more critical than relays

Access
- Physical access to network require same scrutiny as relays

Attacks
- Layer-2 spoofing, Layer-3
- Network Overload (Intentional & Malicious)
Cyber Concerns & Threats: Relays

- Communication capabilities similar to network switches
- Need for Access Control & Remote Access – RADIUS/LDAP
- Layer-2 spoofing, Layer-3, DOS
- Communication port monitoring
Cyber Concerns & Threats: Architecture

Traffic
- High Speed Critical traffic and Slow traffic
- (Layer-2 → Multicast) vs (Layer-3 → Client-Server & File Transfer)

Redundancy
- Communication circuits less reliable than wires

Functions
- Protection ↔ Control ↔ Monitor
Recommended Practice: Isolation

Relay with multiple network ports

• Physically Isolate traffic
  i. Tripping/status between relays
     • GOOSE
  ii. Data from field devices (merging units)
     • SV : mesh
     • SV : point-point
     • GOOSE
  iii. Connection to Station concentrator/HMI
     • MMS
Different Network Architectures

Flat network
Not expandable
Single point of Failure
Unreliable

Ring network
Automatic failover
Failover in ms
Simple design

Complex networks
Multiple rings
Failover in seconds
Design is complex
Redundancy protocols (Layer 2) evolution

- STP
- RSTP (all switches support)
- extended RSTP (proprietary)
- PRP & HSR
- SDN & IEEE TSN
Cyber threat mitigation strategies

**Reliability**
- Design main & failover configurations: PRP/HSR/RSTP
- Consider total bandwidth (SV) and device capability

**Isolation**
- If possible, physically isolate MMS with GOOSE & SV traffic
- Build layer-2 isolation with VLANs

**Security**
- Block unused ports at switch
- Allow only authorized & RBAC secure access to switches (SNMP) and to relays (MMS)

**Monitoring**
- Monitor Continuous state of GOOSE & SV subscription via LGOS & LSVS functions (logical node)
- Check network behavior and events via SNMP
What to Adopt in Design

• IEC 62351: Cyber security standard for IEC 61850
  • RBAC (few manufacturer support)
  • TLS 2.0 Encryption for MMS communication (manufacturer support awaited)

• IEC 61850: Models and Nomenclature
  • Models and parameters for most Power System Functions & Devices
  • Object models for Network switch & Syslog (work in progress)
# Communication Protocols & Applications

**GOOSE**  
(Ethernet Protocol-Layer 2)  
- Multicast  
- Event based: 0-1ms  
- Repetition: 4/8/16ms  
- Binary & Magnitudes  
- Real time events  
- Trips/Alarms/Status

**SV**  
(Ethernet Protocol-Layer 2)  
- Multicast  
- Continuous stream  
- 80/256 Samples per cycle per stream  
- Real time continuous time varying signal (A/D samples)  
- Voltage & Current data

**MMS**  
(Internet Protocol-Layer 3)  
- Client-Server (sessions)  
- Response time: ms-seconds  
- Services defined  
- Read/Write/directory  
- Read event data (file),  
- Read/Change settings  
- Operate breaker/switch: SBO with/without security
Traditional Substation & Commissioning

Oops!

MISTAKE!
IEC 61850 Substation & Commissioning
Why do IEC 61850?

IEC 61850

Safety
No CT opening

Self-Monitoring
Comm. & Devices

Functionality

Flexibility
Commission, Maintain, Test

Time & Cost
No drill # of cables & wire checks
What NPCC can contribute?

• Standards & Guidelines
  A. Design
  B. Communication Networks
  C. Access Control
  D. Monitoring

• Establish Compliance Requirements

• Extend CIP Guidelines: GOOSE/SV → Think beyond Routable
  A. A malicious Breaker Failure/bus-diff Ethernet message can trip multiple circuit breakers
  B. Blockage or interruption of SV stream would jeopardize 1st order high speed protection
  C. Cyber attack on IEEE 1588 (PTP) timing packets can cause miss-operations & trip plant

• Harmonize efforts with other committees
IEC 61850 Resources

- IEC TC57: Working Group 10

- UCAIUG

- IEEE PSRC H30
  - IEC 61850 User Feedback Forum

- IEEE PSCC S8: P2658
  - Guide on Cybersecurity Testing in Electric Power System
Questions?

Topics of interest on IEC 61850 in next meeting?

Deepak.Maragal@nypa.gov
Ph: 914-287-3874
Critical Infrastructure Protection Standards Update

NPCC Fall Workshop
November 21, 2019
Agenda

• CIP Modifications SDT
• BCSI SDT
• Incident Reporting and Response Planning
• Low Impact
• Supply Chain Risk Management
• Communications between Control Centers
CIP Modifications SDT

• Virtualization: A Case For Change
  – Whitepaper posted

• Backwards compatibility

• Option of moving to virtualization

• New posting (November?)
BCSI SDT

• BCSI = BES Cyber Systems Information
• SDT = Standards Development Team
• Explicitly allow BCSI in the cloud
• CIP-004 & CIP-011
• Key management
• Posting (November?)
Incident Reporting and Response Planning

- CIP-008-6
- Applicable January 1, 2021
- Reportable Cyber Security Incident
  - See NERC Glossary
  - Entity defines “attempt to compromise” (Part 1.2)
- Submit notification to NCCIC & E-ISAC
- Mature cyber security program probably includes PCAs
Low Impact

• CIP-003-7 applicable January 1, 2020
  – Program must be in place by January 1, 2020
  – Policy required
  – New Attachment 1 requirements for
    • Transient Cyber Assets (TCAs)
    • Removeable Media (RM)
  – New definition – Malicious Code Risk Mitigation
Low Impact (continued)

- CIP-003-8 applicable April 1, 2020
  - Managing vendor TCAs & RM
  - Going to v8 should be compliant with v7

- Can leverage High / Medium controls for Lows
Supply Chain Risk Management

• CIP-013, CIP-005 and CIP-010
• Applicable July 1, 2020
• proposed Compliance Implementation Guidance
  – NATF
• CIPC Supply Chain WG posted 7 Guidelines
• Recommend consulting procurement & legal
Communications between Control Centers

- CIP-012
- FERC NOPR (Notice of Proposed Rulemaking)
- Control Center definition for this Standard
- Responsible Entities
  - BA, GOP, GO, RC, TOP, TO
- For “real-time data specification elements” see TOP-003 and IRO-010
Questions