



AMPERE

FERC Order 887 on
Internal Network
Security Monitoring
(INSM)

APC SIA Meeting
October 16 2023

Introduction



- CEO, Owner, Ampere Industrial Security
- Former utility staff (telecommunications, water & electric)
- Drafter of NERC CIP standards and formal interpretations, current SCWG, SITES, and SPIDERWG contributor
- First NERC CIP auditor in North America; Manager CIP Audits and Investigations – WECC Region
- Contributor to NERC/ERO Auditor Manual and Guidance
- Speaker/contributor to multiple FERC Technical Committees, NOPRs and Orders
- Former Principal Investigator US DOE National Electric Sector Cybersecurity Organization
- EnergySec Founder, former Director, former Instructor and President Emeritus
- SANS Instructor: ICS456 - Essentials for NERC Critical Infrastructure Protection
- Contributor, DHS CISA Cross-Sector Cybersecurity Performance Goals (CPGs)
- NTIA/INL Software Bill of Materials (SBOM) Energy POC Stakeholders
- NARUC/NASEO Cybersecurity Advisory Team for State Solar (CATSS)
- DOE SETO/NREL Industry Advisory Board (IAB) for the Securing Solar for the Grid (S2G)
- DOE/NARUC Cybersecurity Advisory Group for for Distribution

What happened?



- Jan 19, 2023 - FERC issued Order 887
- *...require internal network security monitoring (INSM) for CIP-networked environments for all high impact bulk electric system (BES) Cyber Systems with and without external routable connectivity and medium impact BES Cyber Systems with external routable connectivity...*
- *...NERC directed to submit a report “that studies the feasibility of implementing INSM at all low impact BES Cyber Systems and medium impact BES Cyber Systems without external routable connectivity.” due within 12 months*

What problem does this solve?



- If we already have perimeter controls and other controls inside the ESP on the individual Cyber Assets, where is the gap?
 - MANY controls in CIP-004, 005, 007, and 010
 - Granting/revoking access controls, account review, ESP, IRA, baselines, patching, anti-malware, CVAs, logging, monitoring, change control, TCAs, RMs
- FERC says... it is designed to address situations “where vendors or individuals with **authorized access** are considered secure and trustworthy but could still introduce a cybersecurity risk” to an applicable system

What problem does this solve?



- For example, in the event of a **compromised ESP**, FERC believes that improving visibility within a network with INSM would increase the probability of early detection of malicious activities and would allow for quicker mitigation and recovery from an attack
- Some other uses:
 - Illegitimate use of legitimate credentials (insider threat)
 - Abuse of allowed/legitimate commands, scripts and software
 - Detection of data exfiltration or network exploration
- Side effect of benefit to operational visibility as well

What will be in the new standard?



- FERC directed three security objectives
 - Network baseline
 - Monitoring and detecting unauthorized activity, connections, devices, and software inside the CIP-protected network
 - Identify anomalous activity to a high level of confidence by:
 1. logging network traffic (FERC notes that packet capture is one means of accomplishing this goal);
 2. maintaining logs and other data collected regarding network traffic; and
 3. implementing measures to minimize the likelihood of an attacker removing evidence of their tactics, techniques, and procedures from compromised devices.
- Expect new terms for the glossary, **possibly**...

Areas of interest for the SDT



- What level of detail in the network baseline?
 - Which systems are talking to which systems, or
 - The above, as well as port, protocol, time of day, frequency, etc...?
- What constitutes unauthorized “activity” and “connections”
 - ...in a way that can be audited?
- For logging network traffic, what will be allowed in lieu of packet captures?
- How much of this data will need to be stored or for how long?
- Exactly which logs and other data will need to be collected and “maintained” regarding network traffic?
- Which log integrity methods will be expected?

When will it be effective?



- 15-month directive for submittal of new standard to FERC
 - Probably early Q2 of 2024
- FERC will review and respond
 - Speculation that it will take 4-6 months
 - Could be Q4 of 2024 (or later)
- Assuming approval, likely 12-18 month implementation window
 - Q1-Q3 of 2026 speculated target for auditability
- Caveat: it could be slower or it could even be faster if we have a “catalytic event”

What's next for INSM?



- SAR has been issued (Project 2023-03)
- SDT has been formed and is currently drafting
- Data requests have been issued for the medium without ERC and low impact study
 - NERC will analyze results and prepare report
 - Provide study to FERC for review, await FERC's response
- Some working groups may produce guidance in tandem with, or even get ahead of the SDT

What are the next steps for you?



- Start planning now; **this will take more time** than you expect
 - Will any network outages be needed?
- May require upgrades to the network (e.g.: spans or taps)
- What are you buying?
 - Will the supply chain issues impact the timing, availability, etc?
 - Don't forget about CIP-013
 - What if everyone else in the industry is also buying at the same time?
- Use the opportunity to upgrade or refine your network
 - Regulatory-driven costs are easier to get budget
- How much capacity will you need for packet captures?
 - Cloud may or may not be an option
- How will you be enforcing log integrity and immutability?
- Review the NERC [INSM Practice Guide](#)

Questions?



Email: pmiller@amperesec.com

Email: cmathis@amperesec.com

Web: www.amperesec.com

LinkedIn: <https://www.linkedin.com/in/millerpatrickc/>

Twitter: [@patrickcmiller](https://twitter.com/patrickcmiller)

Mastodon: [@patrickcmiller@infosec.exchange](https://mastodon.exchange/@patrickcmiller)

Podcast: [Critical Assets Podcast](#)