FERC Hydroproject Cyber Security

[FERC 3A Section 9 versus CIP v5]

Gannett Fleming

Excellence Delivered As Promised

Presentation Goals

- Provide a clear distinction between the intent of FERC cyber security and NERC CIP cyber security
- Discuss opportunities to leverage NERC CIP to meet FERC 3A cyber security assessment requirements
- Generate discussion on the following:
  - Physical security zones needed for FERC, CIP, and Hydroproject
  - Cyber asset inventories for NERC CIP, FERC 3A, other Hydroproject
  - Annual report generation
  - Terminology confusion between FERC and NERC cyber security requirements

Outline

High-level review of Cyber Security

- **FERC 3A Section 9** – Computer Security and SCADA
  - Intent
  - Determinations – Non-Critical, Operational, Critical
  - Form 3 – Inputs and Outputs
- **NERC CIP v5**
  - Intent
  - Determinations – Low, Medium, High
- **FERC 3A Section 9 relies on NERC CIP**
  - Where are the FERC / NERC cyber security overlaps?
  - Opportunities to leverage NERC CIP to meet FERC 3A cyber security assessment requirements

Please Make Note

FERC 3A Section 9 focuses on:

- Potential downstream consequences from unintentional release of all or part of the reservoir, and
- Non-operation and loss of significant power generation.

NERC CIP focuses on:

- Reliability and the transmission of power.

Some cyber assets fall under both jurisdictions.

Terminology between FERC 3A and NERC CIP becomes confusing and needs to be fully understood.

Threats

Aurora Cyber Vulnerability

https://www.youtube.com/watch?v=bAWU5aMyAAo

March 4, 2007 - Idaho National Laboratory ran the Aurora Generator Test to demonstrate how a cyber attack could destroy physical components of the electric grid.

The experiment used a computer program to rapidly open and close a 2.25 MW diesel generator's circuit breakers out of phase from the rest of the grid and cause it to fail.

This vulnerability is referred to as the Aurora Vulnerability and is caused through bypassing protective relays.

FERC 3A Section 9 – Computer Security and SCADA

- The intent is understand the consequences of:
  - **Unintentional release** of all or part of the reservoir (presenting a hazard to downstream populations and infrastructure); and
  - **Non-operation** of a Licensed facility (loss of significant power generation).

- There are three (3) classifications: Non-Critical, Operational, Critical
- There are two (2) levels of security – Basic and Enhanced

Notes:

- Non-critical Licensees do not need to add security under Section 9
- Only Group 3 dams that are interconnected to operational or critical cyber assets of Group 1 or 2 dams will be subject to Section 9.

New Licensee Requirements

Cyber and SCADA controls:

NOT TO BE CONFUSED WITH NERC CIP

9.0 COMPUTER SECURITY AND SCADA

9.1 Introduction

Section 9.0 has been thoroughly revised and will become effective as of January 1, 2016. For purposes of these guidelines only, the emphasis on cyber security and Industrial Control Systems (e.g. SCADA) relates to two main consequences: 1) the unintentional release of all or part of the reservoir (presenting a hazard to downstream populations and infrastructure); and, 2) non-operation of a Licensed facility (loss of significant power generation). Because of this, not all Licensees are required to follow the requirements of Section 9. The flowchart below in Figure 9.1 determines asset criticality and whether the Licensee must follow Section 9. If the asset result is "non-critical" then the Licensee does not need to adhere to Section 9, although voluntary conformance may assist in the strengthening of Licensee business continuity. Details for each step are shown in Section 9.1.1.

***Note: Only Group 3 dams that are interconnected to operational or critical cyber assets of Group 1 or 2 dams will be subject to Section 9.**

FERC 3A Section 9 – Computer Security and SCADA

- **Non-critical** - Powerhouse(s) connected to one cyber asset with installed capacity less than 100 MW are non-critical.
- **Operational** - If a generating unit qualifies as having black start capability, regardless of generating capacity, it is considered Operational. Powerhouse(s) connected to one cyber asset with installed capacity equal or greater than 100 MW but less than 1,500 MW are Operational.
- **Critical** - Powerhouse(s) connected to one cyber asset with installed capacity greater than or equal to 1,500 MW are Critical.

Threats

2013 Unauthorized access into the SCADA systems of the Bowman Dam - Rye, New York - U.S. Indicts 7 Iranians in Cyberattacks on Banks and Dam

The attempt indicated that hackers could take control of computer-operated infrastructure.

Cyber (SCADA) Applicability

To Reiterate:

FERC Section 9 does not deal with the reliability of the electric grid.

The FERC Division of Dam Safety and Inspections (D2SI) is primarily concerned with:

- Safety of the Populations At Risk (PAR) generally downstream of the dam and other consequences (econ/mission loss)
- Requirements of your license to operate a functioning project to ensure project operations – loss of significant power generation

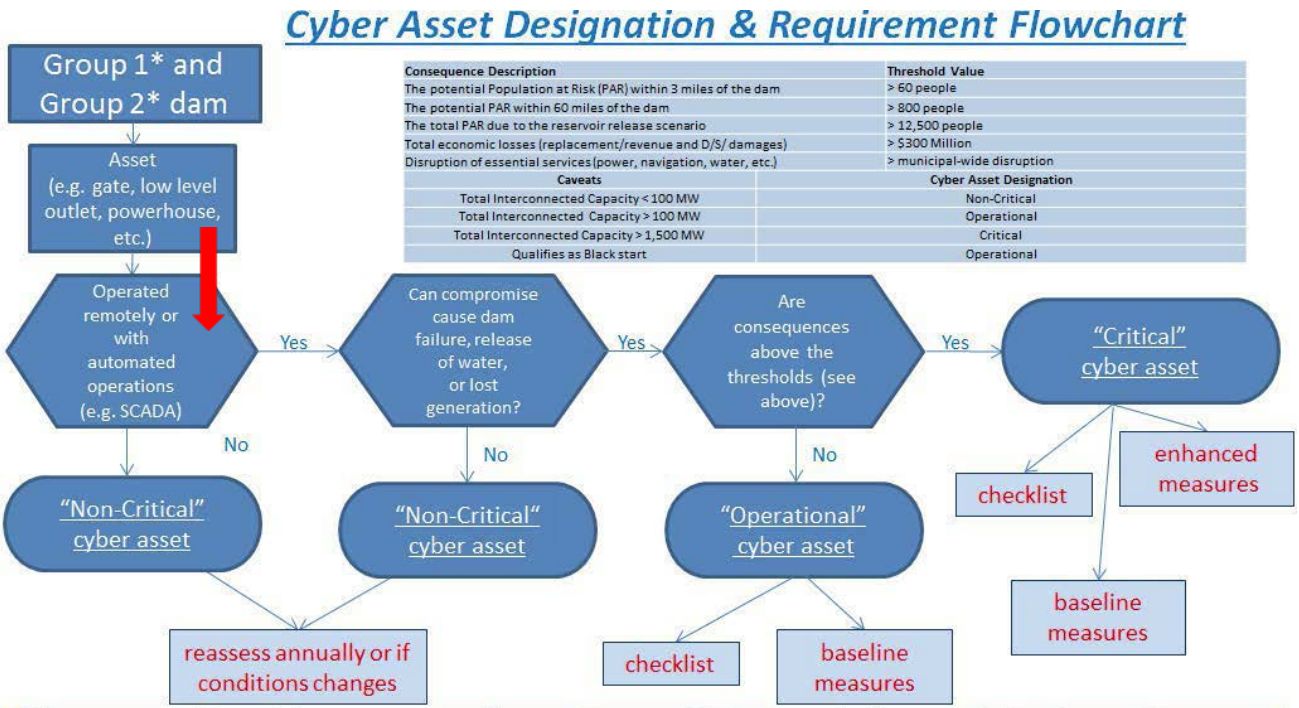
Because of this, not all Licensees are required to follow the requirements of Section 9. Licensee applicability of Section 9.0 starts with the Cyber Asset Designation Flowchart

Threats

The Bowman Avenue Dam is about 20-foot-tall and retains the Blind Brook from flooding basements and ground floors in houses downstream.

"It's ridiculous how little that dam is, how insignificant in the grand scheme of things," said Paul Rosenberg, the Mayor. "We're not talking about something vital to the infrastructure of the country."

Updated Cyber Asset Designation (Rev 3B)



Consequence Description	Threshold Value
The potential Population at Risk (PAR) within 3 miles of the dam	> 60 people
The potential PAR within 60 miles of the dam	> 800 people
The total PAR due to the reservoir release scenario	> 12,500 people
Total economic losses (replacement/revenue and D/S/ damages)	> $300 Million
Disruption of essential services (power, navigation, water, etc.)	> municipal-wide disruption

Caveats	Cyber Asset Designation
Total Interconnected Capacity < 100 MW	Non-Critical
Total Interconnected Capacity > 100 MW	Operational
Total Interconnected Capacity > 1,500 MW	Critical
Qualifies as Black start	Operational

The definition of what constitutes dam Security Groups cannot be included in this open document because the level of potential consequences defined for a specified group of dams should not be publicly revealed, but can be provided to the licensee during the security inspection.

Cyber (SCADA) Applicability

Determining if your Facility falls under the requirements of Section 9.0

- Every Group 1 and 2 dam will be required to fill out the FERC Hydro Cyber/SCADA Security Checklist, Form 3, Questions 1 – 4
  - To determine cyber asset designation, and
  - Discuss this information with the project engineer during the next Operation Inspection.

Remote Operation Determination

- Responses to the four questions on Table 9.1a determine if the dam under consideration falls under the requirements of Section 9.0

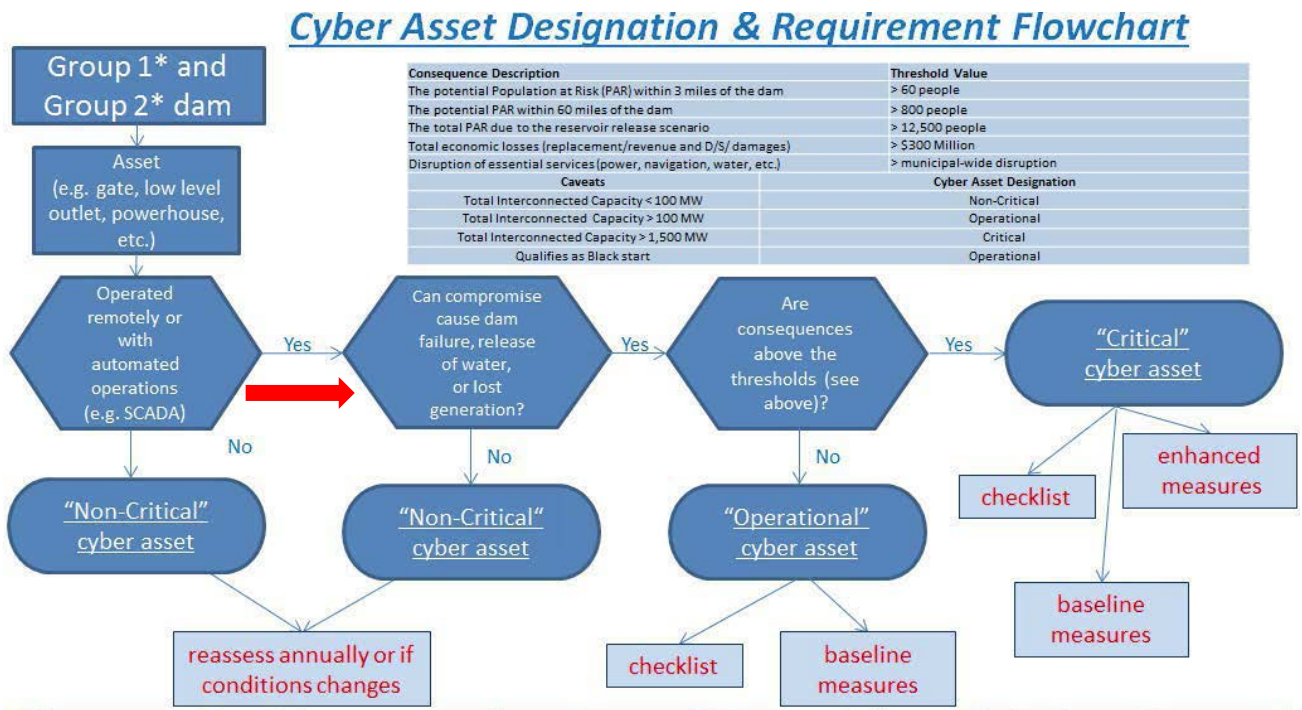
Cyber Asset Applicability (Table 9.1a)

Table 9.1a

Project Name:		
REMOTE OPERATION DETERMINATION	**YES**	**NO**
1. Does the facility/project utilize automated or remote (off-site) control of data acquisition, such as critical instrumentation or operation data?	✓	
2. Does the facility/project utilize automated or remote control of power generation data or power generation controls?	✓	
3. Does the facility/project utilize automated or remote control of water management data or direct control of water retention features?	✓	
4. Is there an interconnection of computer Systems from/to this facility/project to other dam(s)?	✓	
○ **Note:** If there is a virtual (System) interconnection to other facilities that falls under Section 9.0 of the guidelines, that facility is also inclusive of 9.0.		

Any "Yes", continue with criticality determination.

Updated Cyber Asset Designation (Rev 3B)



Consequence Description	Threshold Value
The potential Population at Risk (PAR) within 3 miles of the dam	> 60 people
The potential PAR within 60 miles of the dam	> 800 people
The total PAR due to the reservoir release scenario	> 12,500 people
Total economic losses (replacement/revenue and D/S/ damages)	> $300 Million
Disruption of essential services (power, navigation, water, etc.)	> municipal-wide disruption

Caveats	Cyber Asset Designation
Total Interconnected Capacity < 100 MW	Non-Critical
Total Interconnected Capacity > 100 MW	Operational
Total Interconnected Capacity > 1,500 MW	Critical
Qualifies as Black start	Operational

Gannett Fleming

Excellence Delivered As Promised

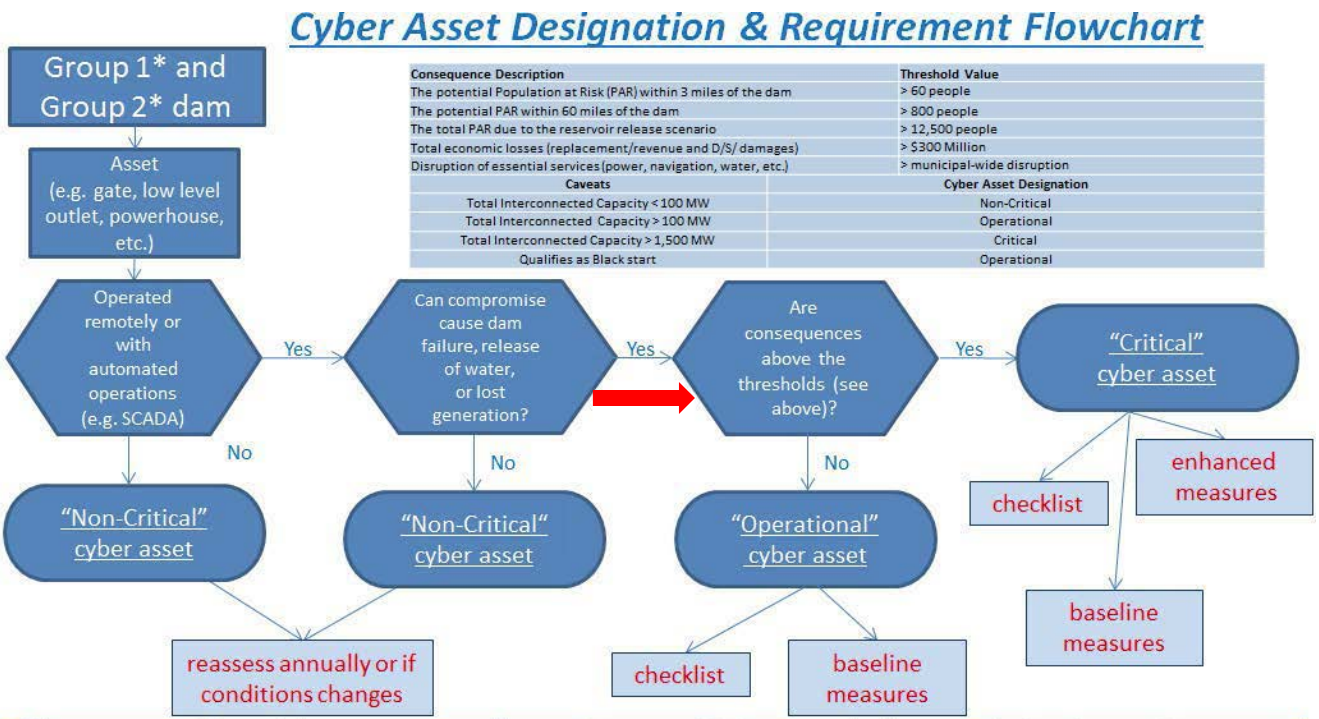
Cyber Asset Applicability (Table 9.1b)

Table 9.1b

Project Name:		
Cyber/SCADA Consequence Determination	**YES**	**NO**
1. Releasing the reservoir,		
2. Losing power generation,		
3. Loss of other associated dam/reservoir mission(s) such as navigation, water supply, etc.		
4. For gate loss and downstream flow considerations, assume all gates are fully open, with no remediation response for 48 hours		
5. For dam failure potential, consider if cascading actions from operational loss could cause the dam to fail (e.g., similar to the 2009 Sayano–Shushenskaya* hydroelectric power station accident, if taken to dam failure).		

A "Yes" answer to questions 1 through 5 means the new regulations apply.
The Facility is now considered either Operational or Critical, as determined through Table 9.1c

Updated Cyber Asset Designation (Rev 3B)



Consequence Description	Threshold Value
The potential Population at Risk (PAR) within 3 miles of the dam	> 60 people
The potential PAR within 60 miles of the dam	> 800 people
The total PAR due to the reservoir release scenario	> 12,500 people
Total economic losses (replacement/revenue and D/S/ damages)	> $300 Million
Disruption of essential services (power, navigation, water, etc.)	> municipal-wide disruption

Caveats	Cyber Asset Designation
Total Interconnected Capacity < 100 MW	Non-Critical
Total Interconnected Capacity > 100 MW	Operational
Total Interconnected Capacity > 1,500 MW	Critical
Qualifies as Black start	Operational

Cyber Asset Applicability (Table 9.1c)

Follow Section 9.0 (Cyber/SCADA) requirements if any potential Consequence arising from compromise of the Cyber/SCADA System is greater than the following values the asset is critical. (Consider Consequences for all potential loss of services (power, water, etc.) and the potential for either full or partial uncontrolled release of the reservoir. Each scenario may generate different Consequence values and should correlate with DAMSVR (or similar methodology) results.)			
Consequence Description	**Threshold Value**	**YES**	**NO**
The potential Population at Risk (PAR) within 3 miles of dam	> 60 people		
The potential PAR within 60 miles of the dam	> 800 people		
The total PAR due to the reservoir release scenario	> 12,500 people		
Total economic losses (replacement/revenue and D/S damages)	> $300 Million		
Disruption of essential services (power, navigation, water, etc.)	> municipal-wide disruption	1	2,3,4

A "Yes" answer response means the Facility is now considered Critical.

Cyber Asset Consequence Description (Rev 3B)

- If any Cyber/SCADA Consequence values are equal to or lower than the values shown in the above table, then the facility is only required to implement Baseline cyber security measures

- If any Cyber/SCADA Consequence value is greater than the values in the above table, then the facility is required to implement Baseline and Enhanced cyber security measures.

Summary of Licensee Responsibilities

- **Non-Critical Cyber Assets**
  - Re-evaluate cyber assets annually
- **Operational Cyber Assets***
  - Must complete Questions 5 – 33 of the FERC Hydro Cyber/SCADA Checklist [Form 3]
  - Provide a plan and schedule to all negative responses
  - Develop Baseline cybersecurity measures.
- **Critical Cyber Assets***
  - Must complete Questions 5 – 33 of the FERC Hydro Cyber/SCADA Checklist [Form 3]
  - Provide a plan and schedule to all negative responses
  - Develop Baseline and Enhanced cybersecurity measures.

****All interconnected facilities also apply.***

FERC Security Measures for Cyber Assets

Hydroproject operators will need complete the following to reduce risk:

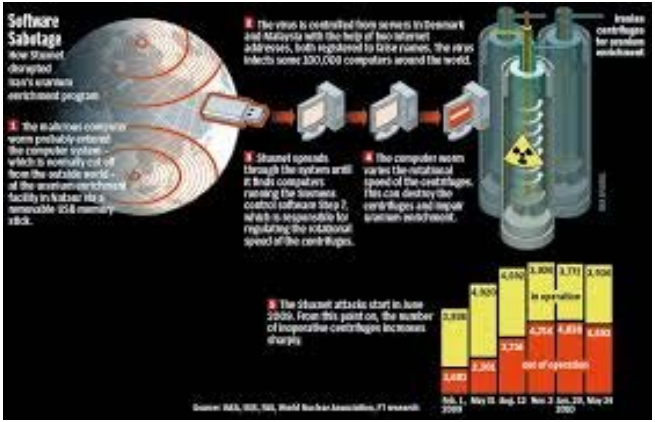
1. **Checklist** - FERC Hydro Cyber/SCADA Security [Form 3]

2. **Baseline** Cyber Security Measures [Operational Assets]
   - Baseline measures should be applied to all cyber assets or cyber systems.
   - See Table 9.3a pages 43 – 44 of D2SI Rev 3A

3. **Enhanced** Cyber Security Measures [Critical Assets]
   - Baseline measures plus Enhanced measures to all cyber assets or cyber systems.
   - See Table 9.3b pages 43-44 plus page 45 of D2SI Rev 3A

Most FERC licensed hydro generation facilities must also comply with NERC CIP v5.

Threats



Stuxnet is a malicious computer worm [malware] believed to be a jointly built American-Israeli cyber weapon. Although neither state has confirmed this openly, anonymous US officials claimed the worm was developed to sabotage Iran's nuclear program with what would seem like a long series of unfortunate accidents.

Stuxnet – Derailing the Iranian Nuclear Program

Stuxnet specifically targets programmable logic controllers (PLC), which allow the automation of electromechanical processes. Specifically, Stuxnet targets centrifuges used to produce the enriched uranium that powers nuclear weapons and reactors.

FERC Section 9 Meets NERC CIP Version 5

FERC Section 9

- Focuses on the potential downstream consequences from unintentional release of all or part of the reservoir and non-operation and loss of significant power generation.
- FERC Section 9 is all about cyber asset protection.

NERC CIP

- Focuses on reliable operation of the Bulk Electric System.
- CIP v5 is all about cyber asset protection.

Note: Some cyber assets will fall under both FERC / NERC jurisdictions.

If this is the case, the FERC cyber security must meet NERC CIP requirements in order to fulfill D2SI's criteria.

Where is the FERC / NERC cyber security overlap?

- **FERC** –
  - There are three (3) classifications: Non-Critical, Operational, Critical
  - There are two (2) security levels: Basic and Enhanced
- **NERC CIP –**
  - There are three (3) classifications: Low Impact, Medium, High
  - There are three (3) security levels: Low (CIP-003), Medium, and High
- Some of the CIP BES Cyber Assets are the same as the FERC Critical Assets
- Some of the CIP BES Cyber Systems are the same as the FERC Critical Cyber Systems
  - All FERC Critical Cyber Systems and NERC BES Cyber systems, and associated cyber assets, need to be protected by cyber and physical security

Where is the FERC / NERC cyber security overlap?

- FERC Form 3 relies on NERC CIP to address many of the 33 category questions
- NERC CIP cyber and physical security requirements meet the FERC requirements
  - Documentation is needed to explain which protection meets specific regulatory requirements – nothing fancy but needs to be explained
- Usually, a NERC CIP Physical Security Perimeter (PSP) is the same as or a subset of a FERC protected area
- A full cyber asset inventory serves multiple purposes
  - FERC 3A critical cyber systems and associated critical cyber assets
  - NERC CIP BES Cyber Systems and associated BES Cyber Assets
  - Hydroproject or facility cyber asset management

Where is the FERC / NERC cyber security overlap?

- Corporate Business Network(s) - Does not include corporate business network(s) unless proper cyber security access controls are not implemented between the networks. [Read as audit scope creep]

How to maximize compliance and minimize operational impact

- Create a complete cyber asset inventory
- Perform the **NERC** CIP-002-5.1a BES Cyber System Categorization process
- Identify the **FERC** critical operational cyber systems and associated cyber assets (best to do a full inventory of cyber assets)
- Identify which cyber asset belongs to which cyber system
- Identify if the cyber system meets the criteria for being a NERC CIP BES Cyber System or a FERC Critical Cyber System, or both
- Update your cyber asset inventory list to reflect each association
- Determine the smallest physical security perimeter to protect NERC BES Cyber Systems and associated BES Cyber Assets
- Determine if an additional physical security perimeter is required to protect FERC Critical Cyber Systems and associated Critical Cyber Assets

How to maximize compliance and minimize operational impact.

- Validate that the physical security perimeters completely protect both NERC and FERC in-scope cyber assets and associated networks.
- Validate any external connectivity from the facility; ensure appropriate devices are installed and configured to restrict access and inbound/outbound data traffic
- Determine what physical security controls are operationally efficient that meet both NERC and FERC requirements
- Document, document, document…
- Ensure that the FERC 3A, Form 3 is completed with an associated Plan to resolve any cyber security gaps
- Ensure that all NERC CIP documentation and evidence is on file; complete your RSAWs ahead of time
- Test your compliance by performing regular mock audits

Gannett Fleming

Excellence Delivered As Promised

Questions?

References – FERC Revision 3A

Federal Energy Regulatory Commission Division of Dam Safety and Inspections FERC Security Program for Hydropower Projects Revision 3A (March 30, 2016)

https://www.ferc.gov/industries/hydropower/safety/guidelines/security/security.pdf

Revision 3 to Revision 3A Changes

https://www.ferc.gov/industries/hydropower/safety/guidelines/security/summary-changes.pdf

Frequently Asked Questions

https://www.ferc.gov/industries/hydropower/safety/guidelines/security/faq.pdf