

# FERC Security Program for Hydropower Projects



## D2SI Security Branch

**\*\*\*Webinar to Begin @ 1:30 EASTERN\*\*\***



# Discussion Points

---

- Development of the Security Branch
- Branch Members and Expertise
- Current Work
- 2020 Inspection Season
- Common Inspection Findings
- Annual Security Certifications
- Cyber Security Advisory
- OER – Low Impact BES
- Suspicious Activity Reporting
- Takeaways
- Questions



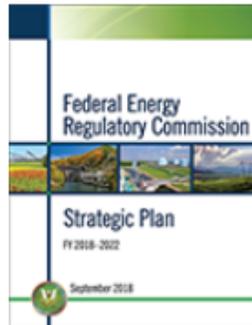
# Development of the Security Branch

[About FERC](#) >> [Strategic Documents](#) >> [Strategic Plan](#)

## Strategic Plan

TEXT SIZE

FY 2018–FY 2022



[FERC submits FY 2018–FY 2022 Strategic Plan](#) PDF

**FERC's Mission: Economically Efficient, Safe, Reliable, and Secure Energy for Consumers**  
Assist consumers in obtaining economically efficient, safe, reliable, and secure energy services at a reasonable cost through appropriate regulatory and market means, and collaborative efforts.

Fulfilling this mission involves pursuing three primary goals:

1. Ensure Just and Reasonable Rates, Terms, and Conditions
2. Promote Safe, Reliable, and Secure Infrastructure
3. Mission Support through Organizational Excellence

To view the complete plan please download the [Full Version](#) PDF



# Development of the Security Branch

## Objective 2.2: Minimize risks to the public associated with FERC-jurisdictional energy infrastructure.

The Natural Gas Act and the Federal Power Act, among other statutory authorities, charge FERC with ensuring that energy infrastructure, once authorized, continues to operate safely and reliably. Failure of LNG or hydropower infrastructure due to structural issues, unsafe operations, natural disasters, cyber and physical attacks, or other hazards can result in loss of life as well as environmental and economic consequences. In addition, the Energy Policy Act of 2005 amended the Federal Power Act to give FERC authority with respect to reliability standards for the bulk-power system and oversight of an Electric Reliability Organization (ERO). In fulfilling these responsibilities, it is critical that FERC minimize risks to the public associated with FERC-jurisdictional energy infrastructure.

FERC achieves this objective through a range of activities. FERC conducts timely safety reviews and inspections with rigorous requirements, thereby advancing the safety of non-federal hydropower projects and LNG facilities throughout their entire life cycle. FERC also oversees the development and review of mandatory reliability and security standards for the bulk-power system, as well as compliance with these standards. In addition, FERC collaborates with regulated entities and other federal and state governmental agencies to identify and seek solutions to cyber and physical threats to FERC-jurisdictional infrastructure, facilitating proactive efforts that prevent or mitigate loss or damage.



“cyber and physical attacks”



# Development of the Security Branch

## Oroville Dam Service Spillway (P-2100)

TEXT SIZE

### FERC After-Action Panel Report on Oroville Dam Spillway Incident December 6, 2018

Following the Oroville Dam spillway incident of February 2017, the Federal Energy Regulatory Commission (FERC) convened the FERC After-Action Panel to review the performance of the Commission's dam safety program at the Oroville Dam Project. This includes both work and actions by FERC staff, and the program requirements of the dam owner, such as the Part 12 process, the analysis of potential failure modes, the Instrumentation and Monitoring Program, and the owner's dam safety program.

FERC also directed the panel to identify any shortcomings in the FERC dam safety program implementation at Oroville Dam. If the panel found any shortcomings, FERC directed the panel to provide recommendations for improvements or changes that the Commission could consider making to its dam safety program to avoid future incidents.

The After-Action Panel members are Dr. Alfred Hendron, Jr., Dr. Nelson Pinto, Dr. Gabriel Fernandez, Dr. Nicholas Sitar, Charles Ahlgren, PE, and John Northrop, PE.

The Panel's final report can be found below. The Commission will begin reviewing this report and will determine how to best address the recommendations provided.

[» Report PDF](#)

d) FERC engineers should concentrate on Dam Safety issues and proper review of auxiliary/ancillary structures. This could be accomplished by creating a separate FERC division solely responsible for security aspects and other non-dam safety issues.



# Development of the Security Branch

News Release: November 21, 2019

Item No: A-4

[Staff Presentation PDF](#)

[View Printable PDF Version](#)

SHARE [f](#) [t](#) [e](#) ...

## FERC Staff Identifies Key Cybersecurity Program Priorities

The Federal Energy Regulatory Commission (FERC) staff today detailed the depth of its continuing efforts to address cybersecurity challenges facing the nation's energy infrastructure.

Among other things, the presentation detailed several organizational changes meant to better focus the agency's resources on quickly evolving cyber challenges including creation of a new security-focused group within the Office of Energy Projects' Division of Dam Safety and Inspections. The group will address cyber, as well as physical, security concerns at jurisdictional hydropower facilities, staff said in a presentation at FERC's November open meeting. Chairman Neil Chatterjee also announced that the Commission's Office of Electric Reliability would be realigning its functions to establish one division focused exclusively on cybersecurity.

"At FERC, we are charged with overseeing the development and enforcement of cybersecurity standards for the nation's high-voltage transmission system and jurisdictional hydroelectric facilities," FERC Chairman Neil Chatterjee said. "These two developments will help FERC staff more efficiently focus its efforts on cyber security. This new security group in OEP and the realignment in OER will consolidate the cybersecurity staff into a division that focuses solely on cyber."

Drawing on the experience and knowledge of each of the relevant offices, a FERC staff presentation today identified five areas where Commission staff will strategically and collectively focus efforts to address critical cybersecurity challenges. The five focus areas are:

- Supply Chain/Insider Threat/Third-Party Authorized Access;
- Industry access to timely information on threats and vulnerabilities;
- Cloud/Managed Security Service Providers;
- Adequacy of security controls; and
- Internal network monitoring and detection.

Staff also described certain outreach activities and other initiatives they intent to prioritize throughout FY2020. In particular, staff will closely monitor supply chain security implementation and the industry's adoption of new technologies and services to address cyber infrastructure implementation, maintenance and/or management. In addition, the Office of Energy Infrastructure Security continues to build on its existing outreach initiatives, including offering voluntary network architecture assessments and the Office of Electric Reliability will continue to conduct and participate in audits.



“...creation of a new security-focused group within the Office of Energy Projects' Division of Dam Safety and Inspections.”



# Development of the Security Branch

---

- Physical Security was an easy extension
- Cyber Threat is constantly evolving
- Limited Cyber Expertise
- Cyber requirements are broad
  - Good for FERC
  - Tough for licensees
  - Difficult to audit uniformly



# Branch Members and Expertise

---

- 5 Physical Security Specialists
- 4 Cyber Security Specialists
- 1 Branch Chief
- Branch out of HQ
  - 6 in DC
  - 2 in Atlanta
  - 2 in Chicago



# Branch Members and Expertise

---

- Army Corps of Engineers
- Department of Homeland Security
- FERC-Dam Safety
- FERC-Dam Security
- FERC-OED
- FERC-OER & OEIS
- Nuclear Regulatory Commission
- Transportation Security Administration



# Current Work

---

- Training for all Branch Members
- Compiling & analyzing all checklist data
- QA/QC all cyber asset designation data



# Current Work

---

- Technical guidance for joint jurisdictional assets
- Determine extent of NERC-CIP assets
- Assess level of protection of Low Impact Cyber Assets at Hydro facilities
- Investigate Baseline Criteria for physical security
- Investigate how cyber criteria can be more prescriptive



# 2020 Inspection Season

---

- Dam Safety Engineers:
  - Will NOT assess security
  - Will report security concerns to the SB
  - Will be informed of the SB recommendations
  - Could be asked to confirm security features/documents



# 2020 Inspection Season

---

- Security Branch will:
  - NOT have new requirements
  - Ask for details within the checklists
  - Ask for details on NERC regulated projects
  - Ask for details on cyber assets



# 2020 Inspection Season

---

- Inspection frequency - *planned*
  - 9 inspectors for about 12-14 dams annually
  - Reevaluate after this year
  - Had started contacting licenses before COVID-19



# 2020 Inspection Season

---

- Inspection frequency - *actual*
  - No inspections through May 15 (except incidents)
  - Await more COVID-19 Guidance to begin inspecting
  - Will likely re-prioritize
  - May request a remote review of documents



# 2020 Inspection Season

---

- Inspections focused on:
  - Dams without a Special Security Inspection
  - Group 1 and 2 dams, (Interconnected Group 3 dams)
  - Projects in the same vicinity
  - Keeping long-term frequency in mind



# 2020 Inspection Season

---

- Security Branch will learn:
  - Length of an inspection
  - Duration of a cyber review
  - Whether Cyber Assets & designations are correct
  - The number of NERC-CIP assets
  - Common gaps within cyber-security program
  - How effective pre-visit cyber review can be
  - Of any resources we haven't thought of



# 2020 Inspection Season

---

- All inspections = past “Special Security Inspections”
- Inspections will include physical & cyber
- Inspections could include cyber call-aheads
  - Intended to save time in the field
  - Hope to conserve licensee resources
  - Coordinate timing before the inspection
  - Multiple information sharing methods available



# 2020 Inspection Season

---

- FERC Field Inspection Process
  - Complete new DAMSVR ahead of the inspection
  - Review All Security Documentation (SP/VA/SA/IERRR)
  - Review/collect Physical Security Checklist
  - Review Cybersecurity Checklist
  - Review Cyber Asset Designation Sheet
  - Ensure procedures within the Plans are exercised



# 2020 Inspection Season

---

- Licensees/Exemptees To Continue:
  - Updating documents in compliance with Rev. 3A
  - Having security staff (physical/cyber) available for security inspections
  - To report security incidents and suspicious activities
  - Maintaining an acceptable level of physical and cyber security
  - Maintaining close relationships with law enforcement agencies/fusion centers



# 2020 Inspection Season

**Table 3.3.8 Security Group Requirements**

Requirement	Security Group 1	Security Group 2	Security Group 3
Security Assessment (SA)	Yes <sup>1</sup>	Yes <sup>1</sup>	No <sup>2</sup>
Vulnerability Assessment (VA)	Yes <sup>1,5</sup>	No <sup>2,5</sup>	No <sup>5</sup>
Security Plan (SP) <sup>3</sup>	Yes <sup>1</sup>	Yes <sup>1</sup>	No <sup>2</sup>
Internal Emergency Response	Yes <sup>4</sup>	Yes <sup>4</sup>	No <sup>2</sup>
Rapid Recovery Plan	Yes <sup>4</sup>	No <sup>4</sup>	No <sup>4</sup>
Annual Security Compliance Certification Letter	Yes	Yes	No

Caveats :

1 = Required

2 = Highly Recommended

3 = Address recommended security upgrades identified in the VA/SA

4 = Internal Emergency Response Required

5 = VA required to close recreation



# 2020 Inspection Season

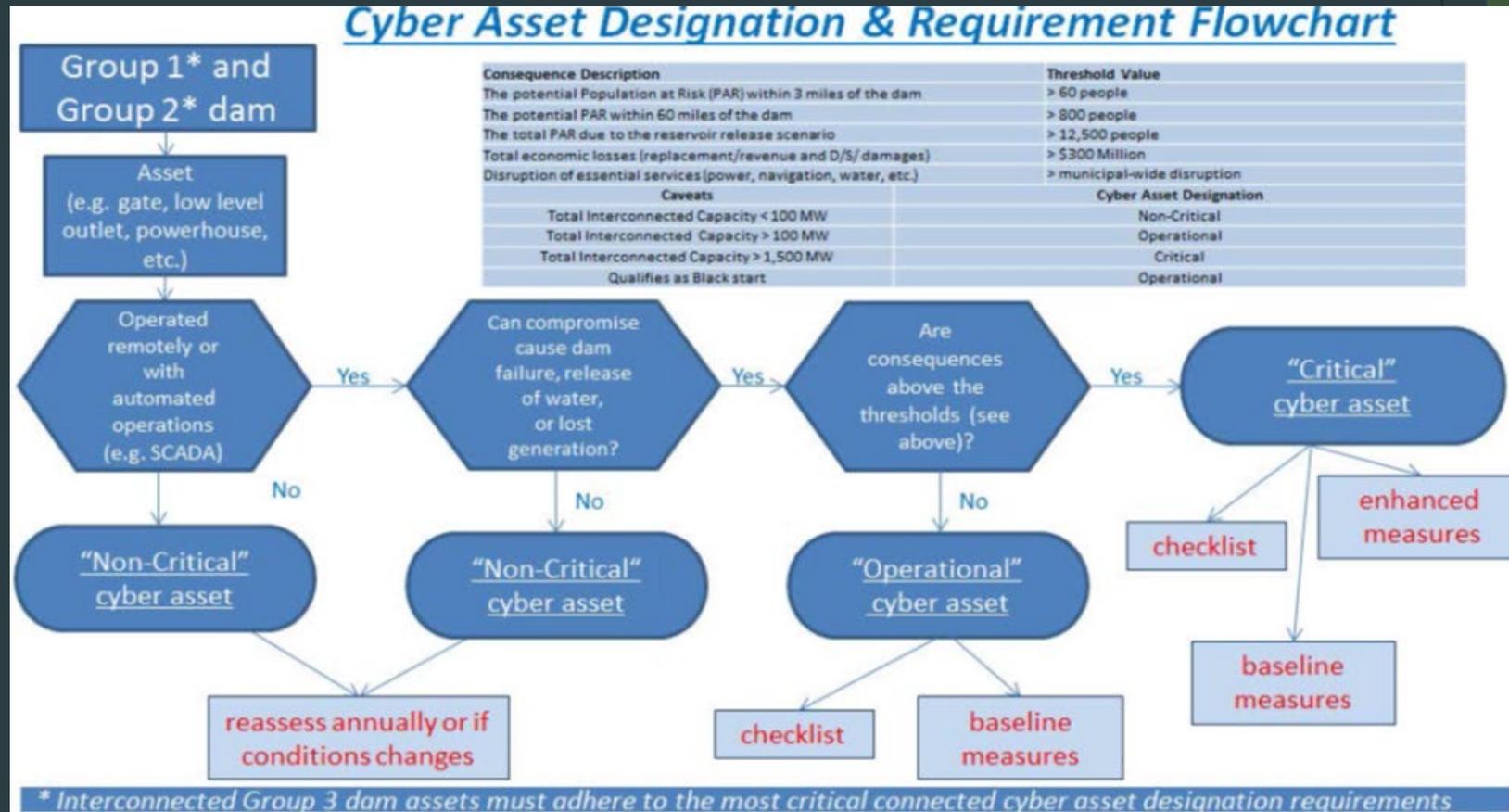
---

- Effective January 1, 2016 – Cyber Security Requirements
  - Identify cyber assets (flowchart)
  - Self-assess cybersecurity posture using cybersecurity checklist (33 questions)
  - Report cyber asset criticality
  - Implement Cybersecurity Measures (NIST 800 Series) or defer to NERC



# 2020 Inspection Season

## Cyber Asset Designation & Requirement Flowchart





# 2020 Inspection Season

## FERC Cyber Asset Designation Spreadsheet

FERC Hydro/Cyber Asset Inventory  
 CUI//CEII//SVI//PRIV

Project Number	Project Name	Dam Name	Licensee/Exemptee	Security Grp	Inspection Date	Physical Feature (e.g. spillway gate(s), powerhouse, etc)	Cyber Asset Designation (Critical, Operational, Non-Critical)	NERC Regulated	Any cyber assets operated by another entity	Status to implement	Notes
P-83	Rock Creek	Rock Creek	ABC Utility	1	June 2016	spillway gate	operational	n/a	no	complete	
P-122	Bayside	Lower Bay	X and Y Renewable	2	July 2015	powerhouse	operational	yes	no	complete	
P-122	Bayside	Upper Bay	X and Y Renewable	2	July 2015	spillway gate	operational	yes	no	complete	powerhouse & spillway gate are interconnected
P-579	North Side	North	ABC Power Co.	1	August 2016	spillway gate	critical	n/a	no	December 1, 2016	
P-580	South Side	South	ABC Power Co.	2	August 2016	powerhouse = 250 MW	critical	no	no	December 1, 2017	interconnected to P-579, would've been "operational" on it's own
P-878	Dry Creek	East Branch	OohRah Hydro Co.	2	August 2017	powerhouse	operational	yes	no	complete	
P-878	Dry Creek	West Branch	OohRah Hydro Co.	2	August 2017	spillway gate	operational	no	no	December 17, 2016	not interconnected
P-998	Eagle River	Dam 1	Lightening Speed Electric	1	September 2016	low level outlet	critical	n/a	no	December 17, 2016	
P-998	Eagle River	Dam 2	Lightening Speed Electric	2	September 2016	spillway gate	operational	n/a	no	December 17, 2016	
P-998	Eagle River	Dam 3	Lightening Speed Electric	2	September 2016	headwater gage	critical	n/a	no	December 17, 2016	mis-operation based on false readings could overtop the embankment
P-1052	Riverside	Right Side	Backup Power Co.	1	May 2017	spillway gate	non-critical	n/a	no	n/a	no remote operation
P-1052	Riverside	Left Side	Backup Power Co.	3	May 2017	powerhouse	operational	no	yes - local utility certifies compliance and we've verified that the documentation and findings meet the FERC requirement.	complete	powerhouse generation < 100 MW, but qualifies as Blackstart.

Examples of cyber asset configuration to determine criticality.

**P-83- the spillway gate is operational and all gaps have been addressed and baseline measures implemented**

**P-122 - 2 dams under 1 project - a powerhouse and spillway gate are interconnected, but the powerhouse is NERC regulated. With deference to NERC requirements, we are satisfied if NERC requirements are met**

**P-579 - interconnected to P-580. 2 projects that are interconnected - the powerhouse is designated operational because it generates b/w 100MW-1,500MW, but because the spillway gate is critical, we take the higher of the two criticalities**

**P-878 - 2 dams under 1 project - the powerhouse is NERC regulated so we are satisfied if NERC requirements are met. The spillway gate at the project and is not interconnect and implementation will occur 12/2017**

**P-998 - 1 project with 3 dams with no interconnection - Dam 1 has a low-level outlet that can be remotely operated (high consequences), Dam 2 has a spillway gate that is remotely operated (low consequences), and Dam 3 has a headwater gage that is remotely read by operators who solely make decisions based on the readings and the dam's spillway gates could be shut and water levels spoofed so the operator doesn't open the gates and this embankment dam overtops and fails - freeboard is very minimal at Dam 3.**

**P-1052 - The Right Side spillway gate is not remotely operated. The Left Side powerhouse is operated by a local utility. The local utility have completed a checklist, certified compliance, and we have verified that the documentation and findings meet the FERC requirement.**

Only report physical assets controlled remotely/automation (e.g. gates, intakes, powerhouse, etc.)  
 No cyber components for control systems are to be reported (reviewed in the field instead)



# 2020 Inspection Season

- FERC Hydro Cyber/SCADA Security Checklist – Form 3
  - If no remote or automation, Section 9.0 doesn't apply.
  - If Yes to remote or automation, must answer questions 1-33.

**CUI//CEII//ISVI//PRIV**

Federal Energy Regulatory Commission  
Division of Dam Safety and Inspections  
**FERC Security Program for Hydropower Projects**  
*Revision 3B – Modified March 1, 2018*

**FERC Hydro Cyber/SCADA Security Checklist – Form 3**

Field Observations: (Provide detailed supplemental information to the right)	Y	N	NA	Comments (Provide additional details – especially any “No” answers – here and separate sheets, if necessary. Indicate NA if not appropriate to site.)
<b>FACILITY Cyber/SCADA CONCERNS</b>				
1. Does the facility/project utilize automated or remote (off-site) control of data acquisition, such as critical instrumentation or operation data?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
2. Does the facility/project utilize automated or remote control of power generation data or power generation controls?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
3. Does the facility/project utilize automated or remote control of water management data or direct control of water retention features?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
4. Is there an interconnection of computer Systems from/to this facility/project to other dam(s)?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	If you answer “Yes” to any of questions 1, 2, 3, or 4, determine if this dam is subject to Section 9.0 of the Security Guidelines (9.1.1.2). If “yes”, continue with questions 5 through 33. If “no”, the analysis can stop here.
5. Are other FERC regulated projects controlled by this facility?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	If so, which projects?
6. Are physical protection measures in place for the control room/facility?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
7a. Does the facility/project have a separate Cyber/Industrial Control System (e.g. SCADA) Security Plan?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
7b. If not, is Cyber/Industrial Control System (e.g. SCADA) Security included in another plan?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	If so, what is the plan?
8a. Does the project have any (hydroelectric) cyber assets which are subject to NERC-CIP Standards?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	If so, what is the asset:
8b. If a NERC-CIP compliance audit has been performed, have all identified deficiencies been addressed?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	If not, when is this scheduled to be completed?



# 2020 Inspection Season

- FERC Hydro Security Inspection Form
  - Evaluate the capability to detect, assess, delay, respond, and communicate against a threat.

**CUI//CEII//PRIV**  
**FERC HYDRO SECURITY INSPECTION FORMS (version 5 – 8/31/2015)**  
 Division of Dam Safety and Inspections  
**FERC SECURITY CHECKLIST (v5)**  
 Field Security Inspection Form 1

Project No.: \_\_\_\_\_ Project Name: \_\_\_\_\_ Dam: \_\_\_\_\_  
 Owner: \_\_\_\_\_ Security Group: \_\_\_\_\_ Date: \_\_\_\_\_  
 Inspector: \_\_\_\_\_ Accompanied by: \_\_\_\_\_

Field Observations: (Provide detailed supplemental information to the right)	Y	N	NA	Comments (Provide additional details – especially any “No” answers – here and separate sheets, if necessary. Indicate NA if not appropriate to site.)
<b>DETECTION AND ASSESSMENT</b>				
1. Is the site manned? Dam?				Days/week _____ Hours/day _____
Powerhouse?				Days/week _____ Hours/day _____
2. Are there surveillance cameras in use? Dam?				
Powerhouse?				
Other?				
How are they viewed/checked?				
3. Is the frequency of walking inspections appropriate (safety and/or security)?				Note the frequency of these inspections:
Personnel control/ID badges used?				
<b>DELAY</b>				
4. Is the dam site fenced with gates/doors locked (if appropriate to the site)?				
5. Is access restriction to the dam/facilities appropriate and in-place? Foot?				
Vehicle?				
Boat?				
6. Are spillway/gate controls secured against unauthorized access?				
7. Are powerhouse doors/windows locked?				



# 2020 Inspection Season

---

- Security Inspections Have & Will Focus On:
  - Assess physical security at all critical assets (e.g. dam, spillway, intake, powerhouse, valves, etc.)
  - Assess cybersecurity at powerhouse control rooms/ remotely operated control centers
  - Look for vulnerabilities at structures and within the security system



# 2020 Inspection Season

---

- Things we look for:
  - At the perimeter
    - Signage on fencing
    - Cameras at perimeter
    - Top guard is intact and faces 45° outward
    - Large gaps bottom of fence line and between gates
    - Ability to shimmy across the ledge of a dam
    - Cut/damaged fence fabric
    - Loose fencing
    - Trees overhanging or are growing within fence
    - Clear Vegetation at least 10' on either side of fence
    - Loose hardware on fence and gates



# 2020 Inspection Season

---

- Things to look for:
  - Access Points
    - Card readers, PIN pad, at pedestrian/vehicle gates
    - Turnstiles
    - Mechanical Bollards/Barrier Systems
    - Locked vehicle/pedestrian gates/maglocks
    - Guard shack (ID checks, visitor logs)
    - Piggybacking/tailgating procedures
    - Camera systems
    - Sensors
    - Restricted areas
    - Signage



# 2020 Inspection Season

---

- Things to look for:
  - Around the Powerhouse
    - Cracked doors and windows
    - Metal grating on windows at eye level
    - Roll-up bays protected (summer heat)
    - PLCs should have pass code or physically protected
    - Physical protection of control room
    - Secured access points (including roof hatch)
    - Cameras/sensors inside and out
    - Exposed wiring in conduits and junction boxes locked
    - Exposed propane tanks
    - Gaps on doors to pick lock/deadbolt



# 2020 Inspection Season

---

- Things to look for:
- At the spillway gates and dam crest
  - Local controls for motors locked
  - Exposed communication and power source protected
  - Maintenance hatches locked
  - Gate control house locked and alarmed
  - Metal grating on windows at eye level
  - Camera system
  - Access to trunnion pins
  - Detection on spillway deck and dam crest
  - Locked gates
  - Fencing with top guard



# 2020 Inspection Season

---

- Things to look for:
- Intake Structures/Gates
  - Fenced off/gated/locked
  - Camera system
  - Sensors on doors
  - Exposed wiring protected
  - Gate control house locked/alarmed
  - Metal grating on windows at eye level
- Waterside of the Dam and Powerhouse
  - Boat barriers
  - Boat booms (public safety and line of demarcation)
  - Signage



# Common Inspection Findings

---

- Documents are outdated
- Documents are descriptive not prescriptive
- Plans are not site-specific
  - Threat Level Planning Procedures are not unique for projects with multiple developments



# Common Inspection Findings

---

- NERC-CIP audit results unavailable
- Cyber assets lack designation information
- Threat not properly assessed (5 DBTs not evaluated)
- Recommendations not addressed/documentated



# Common Inspection Findings

---

- Labeling
  - Security Documents (SP, VA/SA, IERRR) should be labeled on every page as:
    - Header: **CUI//CEII/PRIV**
    - Footer: **Security Sensitive Material**
  - Cybersecurity Documents should be labeled on every page as:
    - Header: **CUI//CEII/ISVI/PRIV**
    - Footer: **Security Sensitive Material**



# Annual Security Certifications

---

- Annual Certifications - Due by December 31<sup>st</sup> each year
- 2019 Overdue certifications were requested by email
  - pdf. format and password protected
  - separate email with password
- All pages of the certification should be labeled on every page as:
  - Header: **CUI//CEII/PRIV**
  - Footer: **Security Sensitive Material**



# Annual Security Certifications

---

- Use template provided by FERC
- Annual Certifications to include:
  - At least two security contacts
  - Dam Name and Number
  - SP/VA/SA/IERRR - Updates/Reviews should indicate month/day/year.
  - Compliance to Section 9.0 Cyber Security



# Annual Security Certifications

---

- **DO NOT** e-file Annual Certification
- **DO NOT** e-file or mail Plans or Assessments
- Planning to host a November 2020 Webinar
  - Many certifications lack detail
  - Will walk through template
  - May request more information



# Cyber Security Advisory

---

Increased cyber events due to COVID-19, including:

- Ransomware activity
- Phishing activity
- Watering hole attacks



# Cyber Security Advisory

---

## FBI Guidance for Ransomware Mitigation

1. RDP accounts for 70-80% of network breaches
2. Be careful of phishing attacks
3. Install software and operating system updates
4. Use complex passwords
5. Monitor your network
6. **Have a contingency plan and backups**



# Cyber Security Advisory

---

## Cyber Security Feed

- E-ISAC (NERC)
- FBI Cyber Outreach
- FEMA (DHS)
- Homeland Security Information Network (HSIN, DHS)
- ICS-CERT (CISA)
- US-CERT (CISA)



# Low Impact BES Cyber Requirements

---

CIP-003-8 - Cyber Security  
Security Management Controls



# Some Definitions – From NERC Glossary

---

- ▶ **Cyber Assets** - Programmable electronic devices, including the hardware, software, and data in those devices.
- ▶ **BES Cyber Asset** - 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. Each BES Cyber Asset is included in one or more BES Cyber Systems.
- ▶ **BES Cyber System** - One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.
- ▶ **CIP Exceptional Circumstance** - A situation that involves or threatens to involve one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death; a natural disaster; civil unrest; an imminent or existing hardware, software, or equipment failure; a Cyber Security Incident requiring emergency assistance; a response by emergency services; the enactment of a mutual assistance agreement; or an impediment of large scale workforce availability.
- ▶ **CIP Senior Manager** - A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC CIP Standards, CIP-002 through CIP-011
- ▶ **Cyber Security Incident** - A malicious act or suspicious event that:
  - ▶ Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter or, Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System.



# Low Impact BES Cyber Requirements

---

► R1.

Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics:

1.1 – not being discussed as it only applies to Med and High Impact BES Cyber Systems

1.2. For its assets identified in CIP-002 **containing low impact BES Cyber Systems**, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls;

1.2.4. Cyber Security Incident response;

1.2.5. Transient Cyber Assets and Removable Media malicious code risk mitigation; and

1.2.6. Declaring and responding to CIP Exceptional Circumstances.



# Low Impact BES Cyber Requirements

---

▶ R3.

Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change.



# Low Impact BES Cyber Requirements

---

## ▶ R4.

The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator.



# Some Definitions – From NERC Glossary

---

▶ Transient Cyber Asset - A Cyber Asset that is:

1. capable of transmitting or transferring executable code,
2. not included in a BES Cyber System,
3. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and
4. directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a:
  - BES Cyber Asset,
  - network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or
5. PCA associated with high or medium impact BES Cyber Systems.

Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

▶ Removable Media - Storage media that

- (i) are not Cyber Assets,
- (ii) are capable of transferring executable code,
- (iii) can be used to store, copy, move, or access data, and
- (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a Protected Cyber Asset. Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.



# Low Impact BES Cyber Requirements

---

▶ R2.

Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in **Attachment 1**.



# Attachement 1

---

Required Sections for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple-impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.



# Attachment 1

---

Section 1. **Cyber Security Awareness:** Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).



# Attachment 1

---

Section 2. **Physical Security Controls:** Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BES Cyber Systems within the asset, and (2) the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any



# Attachment 1

---

Section 3. **Electronic Access Controls:** For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to:

3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:

- i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);
- ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and
- iii. not used for time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR61850-90-5 R-GOOSE).

3.2 Authenticate all Dial-up Connectivity, if any, that provides access to low impact BES Cyber System(s), per Cyber Asset capability.



# Attachment 1

---

Section 4. **Cyber Security Incident Response:** Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

- 4.1 Identification, classification, and response to Cyber Security Incidents;
- 4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;
- 4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;
- 4.4 Incident handling for Cyber Security Incidents;



# Attachment 1

---

## Section 4. Cyber Security Incident Response (continued)

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by:

- (1) responding to an actual Reportable Cyber Security Incident;
- (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or
- (3) using an operational exercise of a Reportable Cyber Security Incident; and 4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.



# Attachment 1

---

Section 5. **Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation:** Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets or Removable Media. The plan(s) shall include:



# Attachment 1

---

## Section 5. Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation(continued)

5.1 For **Transient Cyber Asset(s) managed by the Responsible Entity**, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per Transient Cyber Asset capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.



# Attachment 1

---

## Section 5. Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation(continued)

5.2 For Transient Cyber Asset(s) managed by a party other than the Responsible Entity, if any, the use of one or a combination of the following prior to connecting the Transient Cyber Asset to a low impact BES Cyber System (per Transient Cyber Asset capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the party; or
- Other method(s) to mitigate the introduction of malicious code.

5.2.2 For any method used pursuant to 5.2.1, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.



# Attachment 1

---

## Section 5. Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation(continued)

5.3 For **Removable Media**, the use of each of the following:

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System.



# References

---

<https://www.nerc.com/pa/Stand/Reliability%20Standards%20Complete%20Set/RSCompleteSet.pdf>

[https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary\\_of\\_Terms.pdf](https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf)



# Suspicious Activity Reporting

---

- Report security incidents
- Continue reporting as you were
  - Regional Engineer
  - Project Engineer
  - Regional Security Contact
- Add [justin.smith@ferc.gov](mailto:justin.smith@ferc.gov) and/or 202-502-6426



# Takeaways



- NO NEW Security RQTs for 2020
- Dam Safety Engineers will not assess security
- Past Special Security Inspections = SB Inspections
- Mitigate ransomware with backups & contingency planning
- Continue updating your security documents & completing annual checklists
- Submit your annual certifications on time



# Questions

---

Licensee Question: *When do you anticipate the next revision to the Hydropower Security Program?*

Answer: *A revision is not immediately planned. The SB needs more experience in the field. Also, any proposed changes would need licensee/exemptee feedback.*



# Questions

---

Licensee Question: *Is the new cybersecurity team planning to preform audits in 2020 that are not associated with the Security Inspections?*

Answer: *Only if requested by a licensee/exemptee.*



# Questions

---

Licensee Question: *Will someone from the cyber team be part of all future Security Inspections?*

Answer: *We will assess the need for each project individually.*



# Questions

---

Licensee Question: *How do you want us to handle/address the current requirement for the mandatory Physical & Cyber Security Checklists and Cyber Asset Designation Sheet?*

Answer: *These documents must continue to be reviewed/updated annually and stored in the same manner as previous years. Documents must be available for the SB inspections. If your project is not inspected by the SB, the documents may be requested for review by the Project Engineer on behalf of the SB and this will be communicated prior to the inspection.*



# Questions

---



FERC Security Program for Hydropower Projects Revision 3A:  
<https://www.ferc.gov/industries/hydropower/safety/guidelines/security.asp>

Request for DAMSVR:  
<https://www.ferc.gov/industries/hydropower/safety/guidelines/security/damsvr-req.asp>