FERC Security Program Update and Cyber Brief

May 11, 2016

Introduction

- D2SI Security Team
  - Justin Smith and Nadim Kaade

- Cyber Security Team
  - Barry Kuehnle and Daniel Bogle

- DHS Special Guests

Discussion Points

- Ground rules
- DHS ICS-CERT Brief
- Mass Mailing
- Revision 3/3A
  - History
  - Physical Security – Minor changes
  - Cyber Security – Major changes
- Licensee Expectation – 2016 and 2017 Season
- FERC Cyber SME Collaboration
- Final Thoughts

Ground Rules

- DHS ICS-CERT – 1hr with 15mins for questions
- FERC – 45mins with 45mins for questions
- Type questions into WebEx at presentation’s end

Department of Homeland Security

Industrial Control System -
Cyber Emergency Response Team

Mass Mailing

1. Generation Capacity/Black Start Requirements (Revision 3A)
2. 2016 and 2017 Licensee Expectations
3. NERC/FERC – Duplication of Effort
4. FAQs (attached to letter) – continually updated
5. Cyber Security Checklist (attached to letter)

Revision 3/3A

History

- *April 2015* – Email about the draft and open comment period
- *August 2015* – Posted Revision 3 on ferc.gov
- *September 2015* – Notification to Licensees/Exemptees and email checklist
- *January 2016* – Revision 3 in Effect
- *March 2016* – Revision 3A, FAQs and Cyber Security Checklist posted to ferc.gov
- *April 2016* – Mass Mailing Completed

Revision 3/3A

Physical Security – Minor Changes

- Group 1, 2 dams:
  - New NTAS, National Terrorism Advisory System
  - SP requirements
- Group 1 dams:
  - VA requirements
  - Evaluate 5 DBT for each critical asset
- Group 2 dams:
  - SA requirements
  - Use of generic threat to baseline assess security

Revision 3/3A

Cyber Security – Major Changes

- All Group 1 & 2s determine cyber assets
- Complete the checklist looking for gaps
- “Enhanced” or “Baseline” measures implemented

Licensee Expectations – 2016/2017 Season

- Form 3 Cyber Security Checklist completed
  - Identify all cyber assets
  - Include all justifications to cyber asset designation
  - Assess gaps
- NERC/D2SI assets – show CIP documentation (NERC audit results)
- P & S to implement cyber & physical security measures – NLT December 2017

Licensee Expectations – 2016/2017 Season

Step 1 – Identify Cyber Asset

1. Does the facility/project utilize automated or remote 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)?

If there is a virtual (System) interconnection to other facilities, that facility is also inclusive of 9.0.

Licensee Expectations – 2016/2017 Season

Step 2 - Critical Cyber Assets vs. Operational

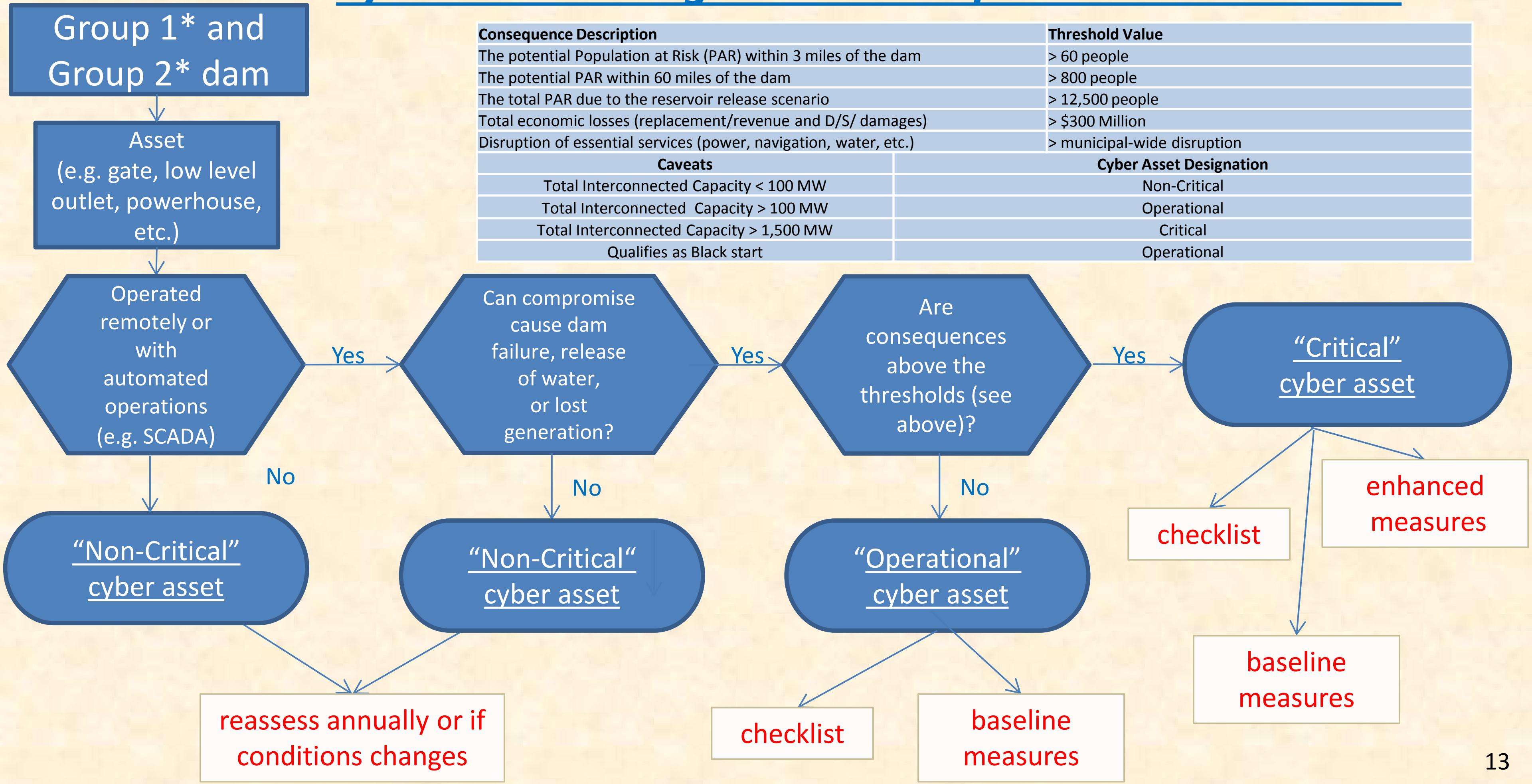
Consequence Description	Threshold Value	YES	NO
The potential Population at Risk (PAR) within 3 miles of dam	> 60 people		
The potential PAR within 60 miles of the dam	> 800 people		
The total PAR due to the reservoir release scenario	> 12,500 people		
Total economic losses (replacement/revenue and D/S damages)	> $300 Million		
Disruption of essential services (power, navigation, water, etc.)	> municipal-wide disruption	1	2,3,4

1. Powerhouse(s) connected to one cyber asset with installed capacity greater than or equal to 1,500 MW are critical. 2. Powerhouse(s) connected to one cyber asset with installed capacity equal or greater than 100 MW but less than 1,500 MW are operational. 3. Powerhouse(s) connected to one cyber asset with installed capacity less than 100 MW are non-critical. 4. If a generating unit qualifies as having black start capability, regardless of generating capacity, it is considered operational.

Cyber Asset Designation & Requirement Flowchart

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



Group 1* and Group 2* dam
Asset (e.g. gate, low level outlet, powerhouse, etc.)
Operated remotely or with automated operations (e.g. SCADA)
Yes
No
Can compromise cause dam failure, release of water, or lost generation?
Yes
No
Are consequences above the thresholds (see above)?
Yes
No
"Critical" cyber asset
"Non-Critical" cyber asset
"Non-Critical" cyber asset
"Operational" cyber asset
reassess annually or if conditions changes
checklist
baseline measures
checklist
enhanced measures
baseline measures

* Interconnected Group 3 dam assets must adhere to the most critical connected cyber asset designation requirements

Licensee Expectations – 2016/2017 Season

Cyber Asset Designation – Example #1

Setting: Group 1 dam with remote SCADA controlled spillway gate(s)

Scenario: SCADA can be compromised and the gate(s) opened to drain the reservoir the sill

Result: Depending on the consequences it's either "operational" or "critical"

Licensee Expectations – 2016/2017 Season

Cyber Asset Designation – Example #2

Setting: Group 2 dam with remote SCADA controlled spillway gate(s)

Scenario: SCADA can be compromised and the gate(s) closed to overtop and fail the dam

Result: Depending on the consequences it’s either “operational” or “critical”

Licensee Expectations – 2016/2017 Season

Cyber Asset Designation – Example #3

Setting: Group 2 dam with automated SCADA spillway controls

Scenario: SCADA can be compromised so that set points are changed

Result: Depending on the consequences – either dam failure or gate release - it’s either “operational” or “critical”

Licensee Expectations – 2016/2017 Season

Cyber Asset Designation – Example #4

Setting: Group 1 dam with remote SCADA controls

Scenario: SCADA can be compromised so that operator sees high reservoir levels and opens gate(s)

Result: Depending on the consequences it's either "operational" or "critical"

Licensee Expectations – 2016/2017 Season

Cyber Asset Designation – Example #5

Setting: Group 1 dam with remote SCADA controlled gate(s) **and** powerhouse generating 1,600MW

Scenario: Gate manipulation consequences are below the threshold

Result: Gate manipulation causes "operational" and powerhouse causes "critical". Higher criticality dictates (this case – "critical")

Licensee Expectations – 2016/2017 Season

Cyber Asset Designation – Example #6

Setting: Group 1 dam with remote SCADA controlled gate(s) with county water supply intake in the reservoir

Scenario: Gate(s) opened and reservoir can be drawn below the water supply intake

Result: Gate manipulation causes "operational", but water supply could cause "critical"

Considerations: Mitigating measures (separate monitoring system or scheduled site visits) can reduce criticality

Licensee Expectations – 2016/2017 Season

Cyber Asset Designation – Example #7

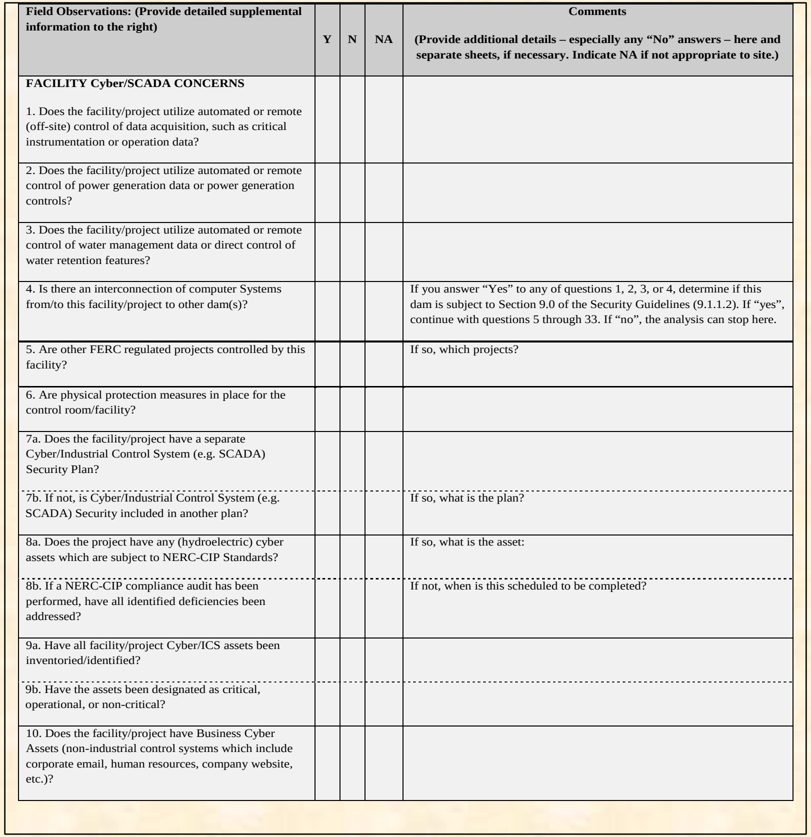
Setting: Group 1 dam with remote SCADA controlled gate(s) that also controls a Group 3 gate

Scenario: SCADA can be compromised to open spillway gates, but only Group 1 dam determines criticality through the process

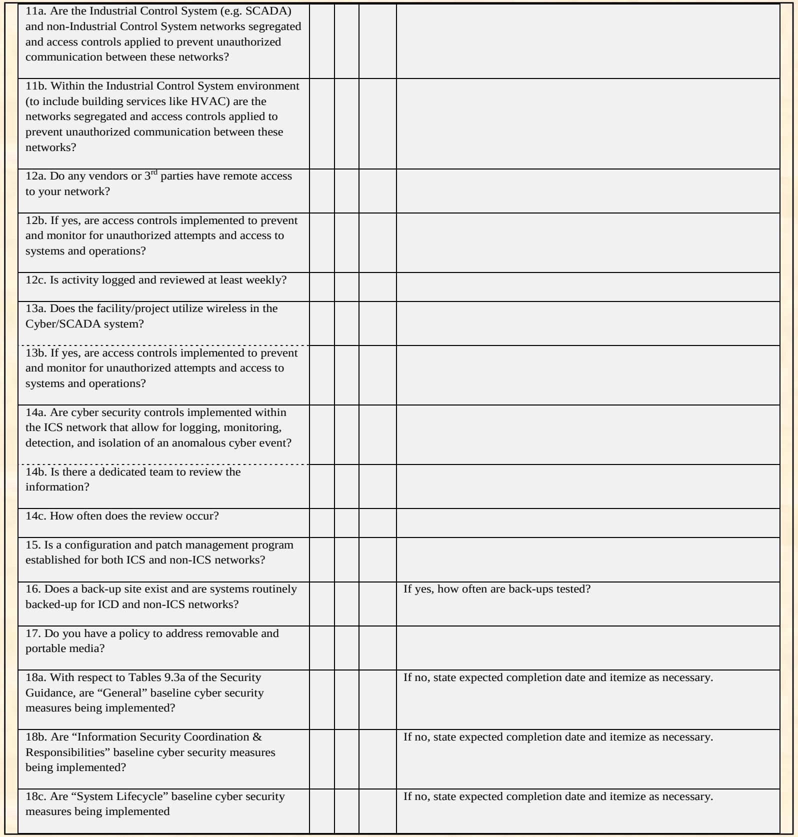
Result: Need to protect Group 3 gate like the Group 1 because of the "weakest link" mentality

Licensee Expectations – 2016/2017 Season

Question 5-33 Self-Assessment



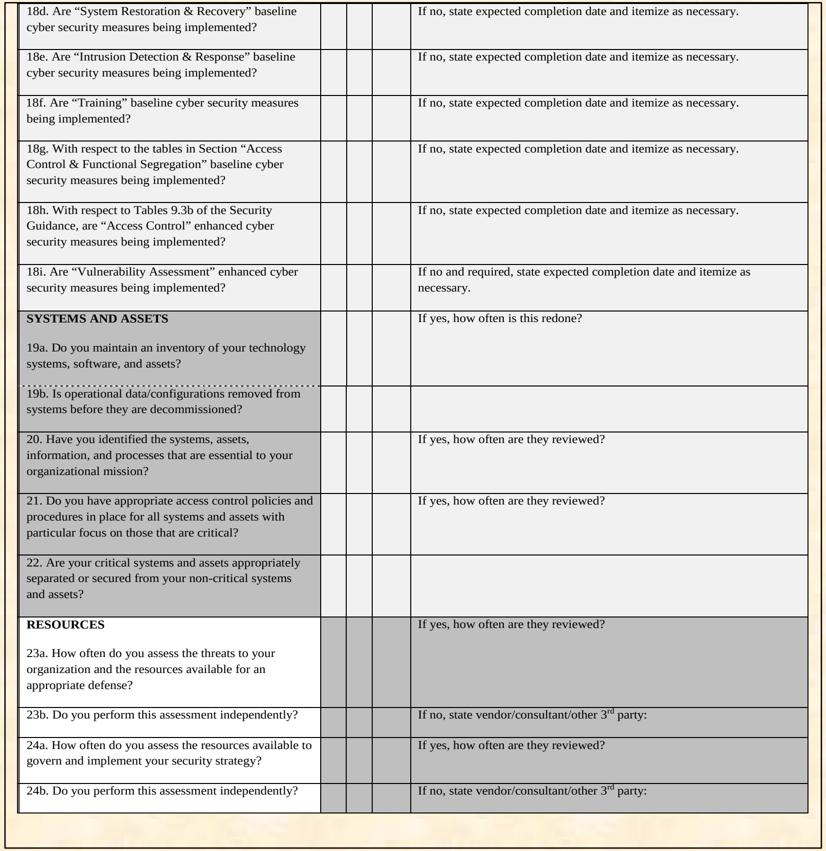
Field Observations: (Provide detailed supplemental information to the right)	Y	N	NA	Comments (Provide additional details – especially any "No" answers – here and separate sheets, if necessary. Indicate NA if not appropriate to site.)
FACILITY Cyber/SCADA CONCERNS 1. Does the facility/project utilize 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)?				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?				If so, which projects?
6. Are physical protection measures in place for the control room/facility?				
7a. Does the facility/project have a separate Cyber/Industrial Control System (e.g. SCADA) Security Plan?				
7b. If not, is Cyber/Industrial Control System (e.g. SCADA) Security included in another plan?				If so, what is the plan?
8a. Does the project have any (hydroelectric) cyber assets which are subject to NERC-CIP Standards?				If so, what is the asset:
8b. If a NERC-CIP compliance audit has been performed, have all identified deficiencies been addressed?				If not, when is this scheduled to be completed?
9a. Have all facility/project Cyber/ICS assets been inventoried/identified?				
9b. Have the assets been designated as critical, operational, or non-critical?				
10. Does the facility/project have Business Cyber Assets (non-industrial control systems which include corporate email, human resources, company website, etc.)?				



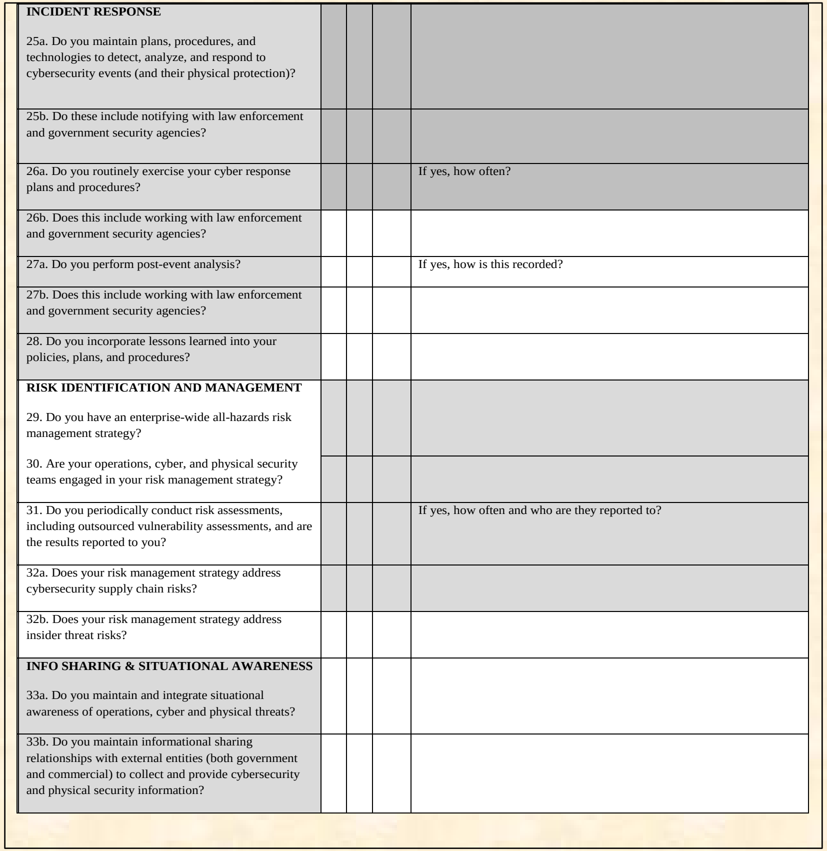
11a. Are the Industrial Control System (e.g. SCADA) and non-Industrial Control System networks segregated and access controls applied to prevent unauthorized communication between these networks?				
11b. Within the Industrial Control System environment (to include building services like HVAC) are the networks segregated and access controls applied to prevent unauthorized communication between these networks?				
12a. Do any vendors or 3rd parties have remote access to your network?				
12b. If yes, are access controls implemented to prevent and monitor for unauthorized attempts and access to systems and operations?				
12c. Is activity logged and reviewed at least weekly?				
13a. Does the facility/project utilize wireless in the Cyber/SCADA system?				
13b. If yes, are access controls implemented to prevent and monitor for unauthorized attempts and access to systems and operations?				
14a. Are cyber security controls implemented within the ICS network that allow for logging, monitoring, detection, and isolation of an anomalous cyber event?				
14b. Is there a dedicated team to review the information?				
14c. How often does the review occur?				
15. Is a configuration and patch management program established for both ICS and non-ICS networks?				
16. Does a back-up site exist and are systems routinely backed-up for ICD and non-ICS networks?				If yes, how often are back-ups tested?
17. Do you have a policy to address removable and portable media?				
18a. With respect to Tables 9.3a of the Security Guidance, are "General" baseline cyber security measures being implemented?				If no, state expected completion date and itemize as necessary.
18b. Are "Information Security Coordination & Responsibilities" baseline cyber security measures being implemented?				If no, state expected completion date and itemize as necessary.
18c. Are "System Lifecycle" baseline cyber security measures being implemented				If no, state expected completion date and itemize as necessary.

Licensee Expectations – 2016/2017 Season

Question 5-33 Self-Assessment



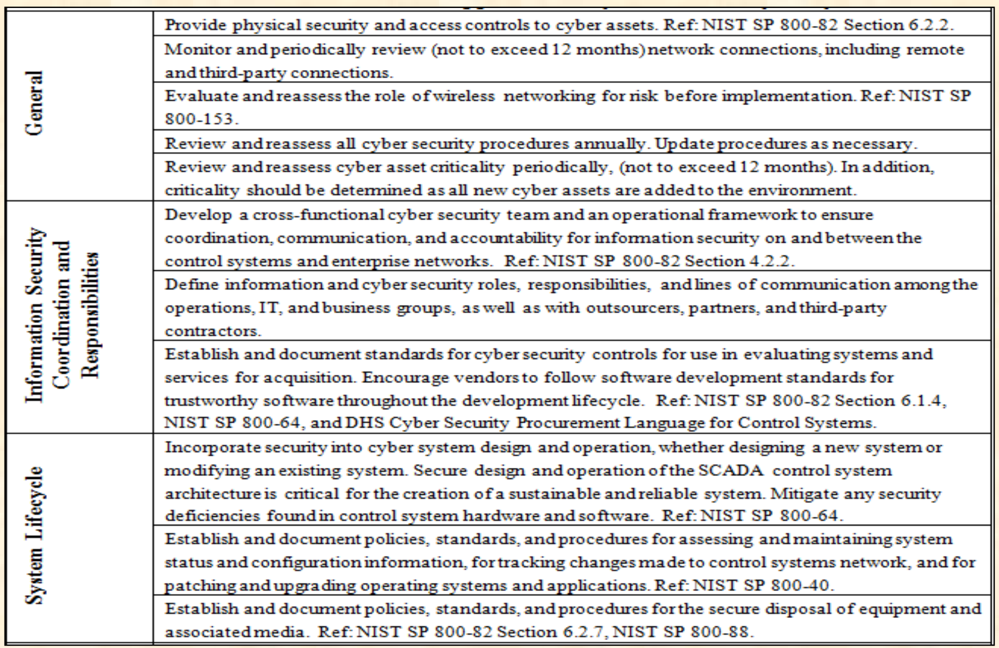
18d. Are “System Restoration & Recovery” baseline cyber security measures being implemented?				If no, state expected completion date and itemize as necessary.
18e. Are “Intrusion Detection & Response” baseline cyber security measures being implemented?				If no, state expected completion date and itemize as necessary.
18f. Are “Training” baseline cyber security measures being implemented?				If no, state expected completion date and itemize as necessary.
18g. With respect to the tables in Section “Access Control & Functional Segregation” baseline cyber security measures being implemented?				If no, state expected completion date and itemize as necessary.
18h. With respect to Tables 9.3b of the Security Guidance, are “Access Control” enhanced cyber security measures being implemented?				If no, state expected completion date and itemize as necessary.
18i. Are “Vulnerability Assessment” enhanced cyber security measures being implemented?				If no and required, state expected completion date and itemize as necessary.
SYSTEMS AND ASSETS 19a. Do you maintain an inventory of your technology systems, software, and assets?				If yes, how often is this redone?
19b. Is operational data/configurations removed from systems before they are decommissioned?				
20. Have you identified the systems, assets, information, and processes that are essential to your organizational mission?				If yes, how often are they reviewed?
21. Do you have appropriate access control policies and procedures in place for all systems and assets with particular focus on those that are critical?				If yes, how often are they reviewed?
22. Are your critical systems and assets appropriately separated or secured from your non-critical systems and assets?				
RESOURCES 23a. How often do you assess the threats to your organization and the resources available for an appropriate defense?				If yes, how often are they reviewed?
23b. Do you perform this assessment independently?				If no, state vendor/consultant/other 3rd party:
24a. How often do you assess the resources available to govern and implement your security strategy?				If yes, how often are they reviewed?
24b. Do you perform this assessment independently?				If no, state vendor/consultant/other 3rd party:



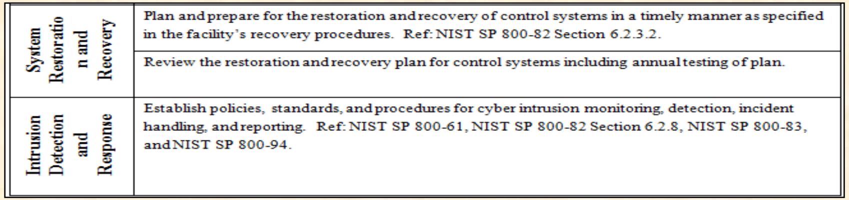
INCIDENT RESPONSE 25a. Do you maintain plans, procedures, and technologies to detect, analyze, and respond to cybersecurity events (and their physical protection)?				
25b. Do these include notifying with law enforcement and government security agencies?				
26a. Do you routinely exercise your cyber response plans and procedures?				If yes, how often?
26b. Does this include working with law enforcement and government security agencies?				
27a. Do you perform post-event analysis?				If yes, how is this recorded?
27b. Does this include working with law enforcement and government security agencies?				
28. Do you incorporate lessons learned into your policies, plans, and procedures?				
RISK IDENTIFICATION AND MANAGEMENT 29. Do you have an enterprise-wide all-hazards risk management strategy?				
30. Are your operations, cyber, and physical security teams engaged in your risk management strategy?				
31. Do you periodically conduct risk assessments, including outsourced vulnerability assessments, and are the results reported to you?				If yes, how often and who are they reported to?
32a. Does your risk management strategy address cybersecurity supply chain risks?				
32b. Does your risk management strategy address insider threat risks?				
INFO SHARING & SITUATIONAL AWARENESS 33a. Do you maintain and integrate situational awareness of operations, cyber and physical threats?				
33b. Do you maintain informational sharing relationships with external entities (both government and commercial) to collect and provide cybersecurity and physical security information?				

Licensee Expectations – 2016/2017 Season

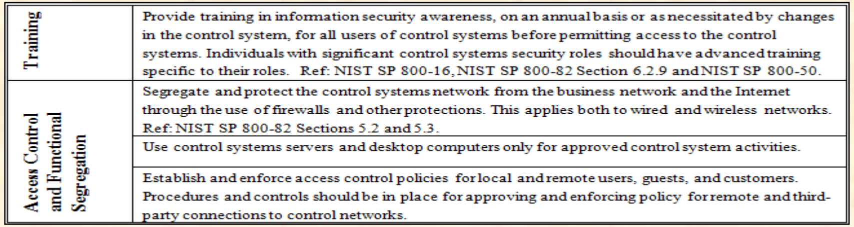
Baseline Cyber Security Measures



General	Provide physical security and access controls to cyber assets. Ref: NIST SP 800-82 Section 6.2.2.
	Monitor and periodically review (not to exceed 12 months) network connections, including remote and third-party connections.
	Evaluate and reassess the role of wireless networking for risk before implementation. Ref: NIST SP 800-153.
	Review and reassess all cyber security procedures annually. Update procedures as necessary.
	Review and reassess cyber asset criticality periodically, (not to exceed 12 months). In addition, criticality should be determined as all new cyber assets are added to the environment.
Information Security Coordination and Responsibilities	Develop a cross-functional cyber security team and an operational framework to ensure coordination, communication, and accountability for information security on and between the control systems and enterprise networks. Ref: NIST SP 800-82 Section 4.2.2.
	Define information and cyber security roles, responsibilities, and lines of communication among the operations, IT, and business groups, as well as with outsourcers, partners, and third-party contractors.
	Establish and document standards for cyber security controls for use in evaluating systems and services for acquisition. Encourage vendors to follow software development standards for trustworthy software throughout the development lifecycle. Ref: NIST SP 800-82 Section 6.1.4, NIST SP 800-64, and DHS Cyber Security Procurement Language for Control Systems.
System Lifecycle	Incorporate security into cyber system design and operation, whether designing a new system or modifying an existing system. Secure design and operation of the SCADA control system architecture is critical for the creation of a sustainable and reliable system. Mitigate any security deficiencies found in control system hardware and software. Ref: NIST SP 800-64.
	Establish and document policies, standards, and procedures for assessing and maintaining system status and configuration information, for tracking changes made to control systems network, and for patching and upgrading operating systems and applications. Ref: NIST SP 800-40.
	Establish and document policies, standards, and procedures for the secure disposal of equipment and associated media. Ref: NIST SP 800-82 Section 6.2.7, NIST SP 800-88.



System Restoration and Recovery	Plan and prepare for the restoration and recovery of control systems in a timely manner as specified in the facility's recovery procedures. Ref: NIST SP 800-82 Section 6.2.3.2.
	Review the restoration and recovery plan for control systems including annual testing of plan.
Intrusion Detection and Response	Establish policies, standards, and procedures for cyber intrusion monitoring, detection, incident handling, and reporting. Ref: NIST SP 800-61, NIST SP 800-82 Section 6.2.8, NIST SP 800-83, and NIST SP 800-94.

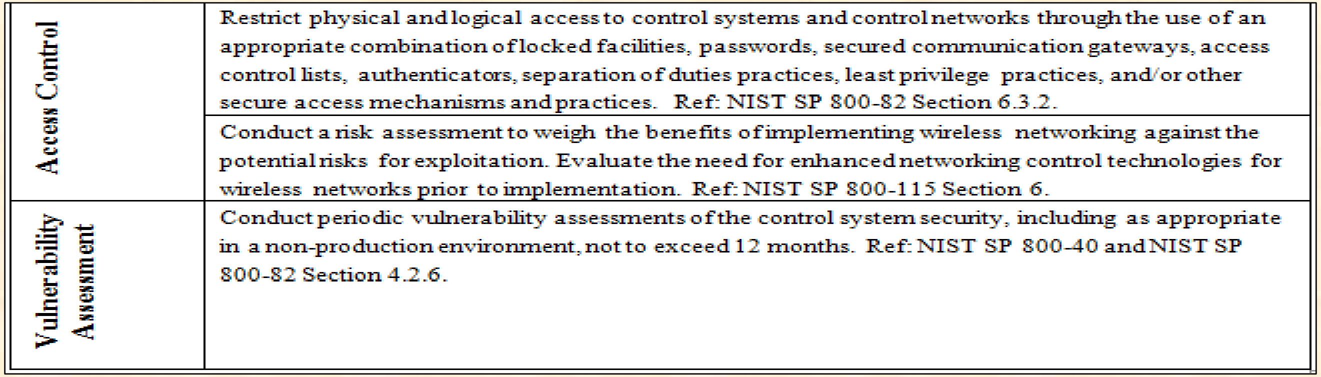


Training	Provide training in information security awareness, on an annual basis or as necessitated by changes in the control system, for all users of control systems before permitting access to the control systems. Individuals with significant control systems security roles should have advanced training specific to their roles. Ref: NIST SP 800-16, NIST SP 800-82 Section 6.2.9 and NIST SP 800-50.
Access Control and Functional Segregation	Segregate and protect the control systems network from the business network and the Internet through the use of firewalls and other protections. This applies both to wired and wireless networks. Ref: NIST SP 800-82 Sections 5.2 and 5.3.
	Use control systems servers and desktop computers only for approved control system activities.
	Establish and enforce access control policies for local and remote users, guests, and customers. Procedures and controls should be in place for approving and enforcing policy for remote and third-party connections to control networks.

National Institute of Standards and Technology
http://csrc.nist.gov/publications/PubsSPs.html

Licensee Expectations – 2016/2017 Season

Enhanced Cyber Security Measures



Access Control	Restrict physical and logical access to control systems and control networks through the use of an appropriate combination of locked facilities, passwords, secured communication gateways, access control lists, authenticators, separation of duties practices, least privilege practices, and/or other secure access mechanisms and practices. Ref: NIST SP 800-82 Section 6.3.2.
	Conduct a risk assessment to weigh the benefits of implementing wireless networking against the potential risks for exploitation. Evaluate the need for enhanced networking control technologies for wireless networks prior to implementation. Ref: NIST SP 800-115 Section 6.
Vulnerability Assessment	Conduct periodic vulnerability assessments of the control system security, including as appropriate in a non-production environment, not to exceed 12 months. Ref: NIST SP 800-40 and NIST SP 800-82 Section 4.2.6.

National Institute of Standards and Technology
http://csrc.nist.gov/publications/PubsSPs.html

FERC Cyber SME Collaboration

- Checklist/FAQs
- Licensee phone calls:
  - Identify cyber assets
  - Determine NC/Operation/Critical
  - Technical cyber details

Final Thoughts

- Licensee Expectations
  - Form 3 Cyber Security Checklist
  - P&S to implement
  - Compliant to Section 9 no later than December 2017
- Mass Mailing
- FAQ’s and Form 3 Distribution

Questions??