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.)
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.)?	☐	☐	☐	

FERC Hydro Cyber/SCADA Security Checklist – Form 3

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 such as 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. If yes, 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 ICS and non-ICS networks?	☐	☐	☐	If yes, how often are back-ups tested?
17. Do you have a policy to address removable and portable media?	☐	☐	☐	

FERC Hydro Cyber/SCADA Security Checklist – Form 3

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.
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 9.3a, are "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?	☐	☐	☐	

FERC Hydro Cyber/SCADA Security Checklist – Form 3

RESOURCES 23a. 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. 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?	☐	☐	☐	If yes, how often and who are they reported to?
32a. Does your risk management strategy address cybersecurity supply chain risks?	☐	☐	☐	

FERC Hydro Cyber/SCADA Security Checklist – Form 3

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?	☐	☐	☐	