FERC Security Program for Hydropower Projects
Revision 3A – March 30, 2016

Table 9.1c has been modified to include two threshold values to establish if a remotely controlled cyber asset that controls generation is designated as:

- Critical
- Operational
- Non-critical

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**

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.

FERC Security Program for Hydropower Projects
Revision 3 – August 31, 2015

The Division of Dam Safety and Inspections (D2SI), Office of Energy Projects, has finalized revisions to its Security Program for Hydropower Projects. The program is largely updated to address cyber security associated with Industrial Control Systems (e.g. Supervisory Control and Data Acquisition – SCADA). The new Section 9 discusses applicability of cyber security baseline and enhanced measures as well as a self-assessment checklist. With respect to physical security, revisions include selection of a design basis threat to establish baseline security effectiveness as well as additions to the Vulnerability Assessment, Security Assessment, Security Plan, and Annual Security Compliance Certification Letter. A summary of changes to the entire program is described by following this link: Revisions

Emails received during the open comment period highlighted concerns over when compliance is to begin under the new program, potential overlap with NERC-CIP requirements, and how the new cyber security requirements impact Security Group 3 dams. Each of these is discussed below:

1. Revision 3 will go into effect January 1, 2016. However, compliance will not be assessed until the annual dam safety inspection at which time documentation is to be presented and discussed with the inspecting engineer.

2. The FERC Office of Electric Reliability requires certain owners, operators and users of bulk power systems to comply with the North American Electric Reliability Corporation's (NERC), Critical Infrastructure Protection Standards (NERC-CIP). These standards focus on the reliability/transmission of power within the Bulk Electric System (BES) and not the potential downstream impacts (population at risk and economic damages) caused by misoperation/failure of water retention features. However, it is possible that a specific cyber asset may fall under both jurisdictions. In this case, the asset must meet NERC-CIP requirements in order to fulfill D2SI's criteria. The CIP standards being met for the specific cyber asset are to be referenced in the security plan(s) and discussed with the project engineer during the dam safety inspection. If a compliance inspection has been performed, the inspection results, any deficiencies identified, and corrective actions taken should also be available for review during the dam safety inspection in order to confirm compliance to Section 9 and prevent duplication of effort.

3. Group 3 dams will only be required to implement cyber security measures if interconnected to a Group 1 or Group 2 dam which has "critical" or "operational" cyber assets.

One significant change incorporated into Revision 3 since the draft version was available for comment deals with determining criticality of a cyber asset which in turn determines the extent of cyber security measures to be implemented. Specifically, cyber assets are to be identified as non-critical, operational, or critical. Each determination carries as increased level of cyber security measures.