Articles + Publications | May 5, 2026

FERC Issues Draft Revised Cybersecurity Guidance for Hydropower Projects (Section 9.0)

WRITTEN BY

Sahara Shrestha | Elizabeth J. McCormick | Dustin T. Till | Charles Sensiba | Andrea W. Wortzel

On April 17, 2026, staff of the Federal Energy Regulatory Commission (FERC or Commission) released a draft revised Section 9.0 of its *Security Program for Hydropower Guidance* addressing cybersecurity for hydropower projects. FERC staff explains that the revisions are intended to modernize the existing guidance to reflect technological advancements, lessons learned from inspections and audits, and evolving practices for protecting cyber and control-system assets. Comments on the draft are due Monday, May 18, 2026.

Background: FERC's Hydropower Security Guidance and Section 9.0

FERC administers a Security Program for Hydropower Projects that is intended to ensure that Commission?jurisdictional hydropower developments maintain appropriate physical and cybersecurity protections based on the potential consequences of a failure or malicious act. As part of this program, FERC staff has developed a written Security Program for Hydropower Guidance document that describes how licensees should identify higher?consequence developments, perform vulnerability assessments, develop and maintain security plans, and certify compliance to the Commission. Within that document, Section 9.0 is the dedicated cybersecurity section. It focuses on computer?based control systems that monitor and control dam and powerplant operations, including supervisory control and data acquisition (SCADA) systems and other industrial control system components.

Section 9.0 operates within the program's broader "Security Group" structure, under which each hydropower development is categorized as Group 1, Group 2, or Group 3 based on the overall potential consequences of a failure or attack. Group 1 and Group 2 developments are higher?consequence projects and are subject to the most stringent requirements, including application of Section 9.0. Security Group 3 developments are lower?consequence projects that generally are not subject to Section 9.0 unless they are electronically or operationally interconnected with the control systems of a higher?consequence Security Group 1 or Security Group 2 development.

Under the existing Section 9.0, FERC staff explains that licensees are expected to identify whether a hydropower development uses remote or automated operation of key dam, reservoir, or generation functions—that is, whether those functions can be monitored or controlled from a control room or offsite location using digital systems, rather than solely through local, manual operation. Where remote or automated capabilities exist, licensees are to evaluate the potential consequences if those capabilities were compromised, including whether a cyber incident could lead to unintentional reservoir release, significant loss of power generation, or other major impacts on public safety, economic activity, or essential services. Based on this consequence analysis, and using thresholds defined

in the Security Program (such as population at risk, economic loss, and service disruption), the licensee classifies each system as either an “operational cyber asset” or a “critical cyber asset.” Systems whose compromise would have lower, but still material, consequences fall into the “operational cyber asset” category and must meet baseline cybersecurity measures. Systems whose compromise would exceed the defined consequence thresholds fall into the “critical cyber asset” category and must meet both baseline and enhanced cybersecurity measures.[1]

Under the current Section 9.0, licensees record their annual evaluations and the status of required cybersecurity measures on the Hydro Cyber/SCADA Security Checklist (Form 3). Form 3 is completed once per year for each applicable development and is one of the documents FERC staff may review when assessing a licensee’s implementation of the hydropower security program.

Draft Revisions to Section 9.0

In the April 17, 2026, draft, FERC staff explains that it is revising Section 9.0 to modernize the existing cybersecurity framework considering technological changes since 2015 and lessons learned from inspections and audits under the Security Program for Hydropower. The draft retains the risk?based Security Group structure, but updates the terminology, scope, and level of detail that staff will use when evaluating cybersecurity at covered hydropower developments.

First, the draft updates several core definitions that frame how Section 9.0 applies. FERC staff proposes to define “control systems” to include supervisory control and data acquisition (SCADA) systems, process control systems, and distributed control systems that monitor and control generation, water management, and related functions at a development. The draft defines “remote operations” as access from external locations to non?public computing resources inside a protected network, and defines “automated operations” as a form of remote operation when systems execute control actions based on programmed logic without direct, local human intervention. The draft also defines “cyber asset” and “cyber system” to include both individual devices and groups of interconnected hardware and software that together perform operational functions, and revises “interconnection” so that it encompasses both physical networking and virtual or logical connections between developments.

Second, the draft adds clearer text on how Section 9.0 can apply to lower?consequence Security Group 3 developments when they are interconnected with higher?consequence Security Group 1 and 2 projects. In particular, the draft explains that when a Security Group 3 development is electronically or operationally interconnected with the control systems of a Security Group 1 or Security Group 2 development, systems at the Security Group 3 development may fall within Section 9.0 and be classified as operational or critical cyber assets based on the consequences they could cause at the interconnected higher?risk development.

Third, the draft also expands the description of the “baseline” and “enhanced” cybersecurity measures that apply to covered systems. For baseline measures, the draft provides additional detail on FERC staff’s expectations for managing user access, segmenting control networks from business networks, exercising incident?response processes on a regular basis, and reviewing external and third?party network connections. It adds new emphasis on configuration and patch?management practices for control?system components, supply?chain risk management for hardware and software, planning for end?of?life or unsupported equipment, and use of multi?factor authentication for remote access into control?system environments. For enhanced measures, which continue to apply only to critical cyber assets, the draft offers a more granular description of what FERC staff

expects, including tighter logical and physical access controls, more detailed logging and correlation of cyber events with physical access records, and more frequent or in?depth technical vulnerability assessments, preferably conducted outside of live production environments.

Finally, the draft makes the self?assessment and oversight process more explicit. It states that licensees should be able to answer “yes” to all Hydro Cyber/SCADA Security Checklist (Form 3) questions that correspond to required baseline and enhanced measures, and that any “no” answer should be accompanied by a plan and schedule to implement the missing measure. The draft also describes in more detail how FERC staff intends to use Form 3 information in inspections, stating that cyber specialists and regional engineers will focus on control?system assets that affect dam operations, remote operation of project facilities, and power generation, and will review how licensees manage network segregation, remote access, and identified vulnerabilities. In addition, the draft notes that, where a facility is subject to North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection standards, staff will consider how a licensee’s Section 9.0 activities align with those existing obligations.

Status of Section 9.0 as Guidance

The draft revised Section 9.0 continues to appear as part of FERC staff’s Security Program for Hydropower Guidance, rather than as a codified regulation. The draft itself does not identify new, stand-alone regulatory requirements or specify penalties tied to particular baseline or enhanced measures. Instead, it describes how FERC staff intends to evaluate cybersecurity at licensed hydropower developments and how staff expects licensees to document and assess their own programs.

At the same time, because the Security Program and Section 9.0 are used in license administration and inspection by FERC staff, the more detailed language in the draft may, in practice, influence what staff treats as the minimum acceptable cybersecurity posture under existing license and Federal Power Act obligations. Stakeholders may wish to address this point in comments, including whether the draft appropriately distinguishes between recommended practices and expectations that FERC staff may later seek to enforce in the context of hydropower security oversight.

Comments on the draft revised Section 9.0 are due Monday, May 18, 2026, by 5:00 p.m. Eastern Time. A copy of the draft, issued in Docket No. AD26-6-000, is available here.

---

[1] In the existing Section 9.0, “baseline” measures are the minimum set of cybersecurity practices that apply to all covered systems. They include core controls such as managing user access to control systems, segmenting control networks from business networks, maintaining backups and recovery procedures, monitoring for suspicious activity, and providing basic security training. “Enhanced” measures build on the baseline for higher?risk systems and involve additional safeguards and scrutiny, such as tighter access controls, more detailed logging and monitoring, and more frequent or in?depth reviews of vulnerabilities and configuration changes.

RELATED INDUSTRIES + PRACTICES

- Hydropower