Written Testimony of Terry Turpin
Director, Office of Energy Projects
Federal Energy Regulatory Commission
before the
Energy and Natural Resources Committee
Subcommittee on Water and Power
United States Senate
April 10, 2024

Chairman Wyden, Ranking Member Risch, and members of the Subcommittee, good afternoon, and thank you for the opportunity to appear before you today.

My name is Terry Turpin and I am the Director of the Office of Energy Projects at the Federal Energy Regulatory Commission. The Office is responsible for taking a lead role in carrying out the Commission's responsibilities in reviewing infrastructure projects, including: (1) the licensing, administration, and safety of non-federal hydropower projects; (2) the authorization of interstate natural gas pipelines and storage facilities; and (3) the authorization of liquefied natural gas terminals. I appreciate the opportunity to appear before you to discuss the Commission's program regarding cybersecurity for dam structures associated with hydropower. As a member of the Commission's staff, the views I express in this testimony are my own, and not necessarily those of the Commission or of any individual Commissioner.

I. Federal and Non-Federal Roles in Hydropower Oversight

There are hydropower projects in nearly every state and on most major river systems of the U.S. with more than 100 (gigawatts) GW of electric generation capacity installed. Of this capacity, approximately 43 GW is supplied by facilities owned and operated by federal entities, principally the Army Corps of Engineers (COE), the Bureau of Reclamation (BOR), and the Tennessee Valley Authority (TVA).[1] Approximately 57 GW of hydropower generation capacity is owned and operated by non-federal parties such as private, non-utility companies; private utility companies; municipalities; electric cooperatives; private citizens; Indian Tribes; and state agencies. Under the Federal Power Act, non-federal hydropower projects must be licensed by the Commission if they: (1) are located on a navigable waterway; (2) occupy federal land; (3) use surplus water or water power from a federal dam; or (4) are located on non-navigable waters over which Congress has jurisdiction under the Commerce Clause, involve post-1935 construction, and affect interstate or foreign commerce. In accordance with the Federal Power Act, the Commission currently regulates over 1,600 non-federal hydropower projects comprised of over 2,500 dams. These projects represent most, but not all, non-federal hydropower.

[1] Megan M. Johnson, Shih-Chieh Kao, and Rocio Uria-Martinez. 2023. *Existing Hydropower Assets (EHA) Plant Database, 2023*. HydroSource. Oak Ridge National Laboratory, Oak Ridge, Tennessee, USA. https://doi.org/10.21951/EHA_FY2023/1972057

Multiple entities hold cybersecurity oversight responsibly for different components within a hydropower facility. For example, the North American Electric Reliability Corporation is responsible for setting and enforcing cybersecurity standards related to generating equipment and controls that support the Bulk Electric System. Alternatively, cybersecurity standards for the control systems related to the safe storage and conveyance of water at hydropower facilities typically falls under the purview of government agencies. For federal hydropower facilities (*i.e.* outside of the Commission's jurisdiction), the COE, BOR, and TVA establish and implement cybersecurity standards for the facilities they own and operate and the Commission has no authority regarding them. For non-federal hydropower facilities, the Commission oversees a comprehensive safety and security program, discussed below.

II. History of the Commission's Dam Safety Program

The Commission is responsible for ensuring that the water-retaining and conveyance features of licensed hydropower projects are designed, constructed, operated, and maintained using current engineering standards and meet federal guidelines for dam safety. During the nearly 60 years the Commission's dam safety program has been in existence, the principal focus has been on dam safety problems associated with: increased risk from natural hazards (*e.g.*, floods, earthquakes), the effectiveness of maintenance activities for ensuring structural integrity; the development/implementation of emergency response plans; and the efficacy of Owner's Dam Safety Programs. Dams are inspected and evaluated by Commission staff and/or independent consultants hired by the licensee on a frequency correlated to the scope of potential downstream impacts. The results of evaluations of both Commission staff and independent consultants include detailed engineering studies, recommendations for dam safety improvements, and a determination whether a dam can safely continue to operate. Each year, Commission dam safety engineers conduct approximately 2,000 inspections related to incident response, construction, and operation of dams.

Beginning in 2001, the Commission incorporated physical security review into the dam safety program. In addition to the consideration of potential downstream impacts, the agency added an assessment of a facility's vulnerability to attack (*i.e.* facility configuration, structural condition, accessibility, and attractiveness as a target). Dams with higher potential downstream consequences and higher vulnerability were required to have more stringent physical security measures than those with a lower combination of potential consequences and vulnerabilities. Security measures were developed by the licensee through conducting vulnerability assessments; developing security plans; undertaking security upgrades and modifications; and maintaining communications with law enforcement entities. FERC engineering staff reviewed the thoroughness of the vulnerability assessments and security assessments conducted by the licensees and evaluated installed physical security measures during dam safety inspections.

In 2016, the Commission's dam safety program was further expanded to address cybersecurity of the control systems used to manage operation of the water control features of a project (*e.g.*, flow bypass systems, reservoir level monitors, flow meters, piezometers, embankment movement indicators). The cybersecurity review program focused on ensuring owner/operators implemented appropriate measures around remotely operable physical features, such as spillway gates, as well as any instrumentation and digital controls needed for dam safety and/or operational decisions regarding the safe flow and storage of water.[2] Identification of remotely operated equipment and/or remotely accessible instrumentation was paired with a dam's potential downstream impacts and vulnerability to assess whether adequate levels of cyber protection were in place.

Dams with either no remote connectivity, or remote connectivity which posed no risk if compromised, were assigned a "Non-Critical" designation. Dams with remote connectivity and potential impacts to: population (less than 60 within 3 miles; less than 800 within 60 miles, or less than a total population of 12,500); economic losses ($300 million or less); disruption of essential services such as water supply for water treatment plants and irrigation (impacts affecting less than a municipal-wide area); or potential generation loss (1,500 MW or less) were designated as "Operational" assets. Dams with remote connectivity and potential impacts higher than those thresholds were designated as "Critical" assets.

Dam owners/operators subject to FERC oversight vary widely in capabilities, resources, organizational structure, and size. In recognition of this, the Commission developed cybersecurity measures drawn from a risk-based, descriptive model approach which allowed for flexibility in regulating such a diverse set of entities. As opposed to prescriptive methods, these cybersecurity measures allowed dam operators/owners the ability to implement a defense-in-depth strategy based on the unique risks and constraints they faced. This approach also allows the Commission's required measures to adapt to changes in the cybersecurity vulnerability and threat landscape. These cybersecurity measures were built on standards issued by the National Institute of Standards and Technology, approaches developed through the North American Electric Reliability Corporation standards development process, and were informed by outreach to the regulated industry.[3]

Cybersecurity measures were divided into two levels: Baseline Measures and Enhanced Measures. Baseline measures were intended to address the most common threat scenarios that might be used to compromise an operational control system. Baseline measures included providing physical security and access restrictions to control system

[2] Generation and connected transmission digital equipment controls associated with the Bulk Electric System are required to comply with the North American Electric Reliability Corporation's Critical Infrastructure Protection Reliability Standards. Accordingly, such generation and associated transmission digital equipment are not covered by FERC's dam safety requirements, but rather have oversight provided by FERC's Office Electric Reliability.

[3] Federal Energy Regulatory Commission. *Security Program for Hydropower Projects Revision 3*. https://www.ferc.gov/dam-safety-and-inspections/security-program-hydropower-projects-revision-3.

assets. Owners were directed to monitor and periodically review network connections, including remote and third-party connections. All cybersecurity procedures were to be reviewed annually and updated as necessary.

Baseline measures also included information security and coordination responsibilities such as developing a cross-functional cybersecurity team and an operational framework to ensure coordination, communication, and accountability for information security on and between the control systems and enterprise networks. Owners needed to define information and cybersecurity roles, responsibilities, and lines of communication among the operations, information technology, and business groups, as well as with outsourcers, partners, and third-party contractors. They also needed to establish and document standards for cybersecurity controls for use in evaluating systems and services for acquisition.

Additionally, baseline measures that address the system lifecycle included incorporating security into control system design and operation, whether designing a new system or modifying an existing system, to ensure creation of a sustainable and reliable system. Owner/operators were required to 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. Owners were also encouraged to implement a supply chain risk management program to ensure vendors followed practices such as software development standards to ensure trustworthy software throughout the development lifecycle. Network traffic access control and functional segregation were required to ensure segmentation of control system networks from less secure networks such as business networks and the Internet through the use of firewalls and similar network traffic access control protections.

Training was specified as an important component of a good cybersecurity program and owners were required to provide training in information security awareness, on an annual basis or as necessitated by changes in the control system, for all users before permitting access. Individuals with significant control systems security roles were to have advanced training specific to their roles.

Enhanced user access control security measures included restricting physical and logical access to control systems and control networks through the use of an appropriate combination of locked facilities, robust identity verification, secured communication gateways, access control lists, separation of duties practices, least privilege practices, and/or other secure access mechanisms and practices. Owner/operators were required to conduct a risk assessment to weigh the benefits of implementing wireless networking against the potential risks for exploitation. Owners were also directed to evaluate the need for enhanced networking control technologies for wireless networks prior to implementation. Enhanced vulnerability assessment security measures included conducting periodic vulnerability assessments of the control system security, including as appropriate in a non-production environment, not to exceed 12 months.

Owner/operators with dams considered "Non-Critical" were not required to implement these practices given their lack of remotely operable assets or lack of potential downstream impacts, but such licensees were required to re-evaluate this designation annually to monitor for changes. Dams designated as "Operational" required licensees to implement Baseline Cyber Security Measures. Operators with dams considered "Critical" were required to implement both Baseline Cyber Security Measures and Enhanced Cyber Security Measures.

Dam owner/operators needed to implement measures appropriate to the dam designation by the end of calendar year 2018. Licensees were required to submit a letter to the Commission by December 31, 2018, and each year thereafter, certifying compliance with both physical and cybersecurity requirements. Owner/operators needed to maintain documentation regarding vulnerability assessments, security practices, and network architecture at the facility site for review by FERC engineers during any dam safety inspection. During the dam safety inspection, FERC engineers would review measures taken by the licensee regarding remotely operable water conveyance and monitoring equipment.

III. Current Security Program

Following a spillway failure at the Oroville dam in February 2017, the Commission convened an independent panel to review the performance of the Commission's dam safety program.[4] The panel's conclusions, issued December 2018, included a recommendation to remove security inspections from the duties of traditional dam safety engineers and hire technical staff to assess security aspects of the Commission's jurisdictional facilities. Separating these functions would position the Commission to improve the breadth and scope of all dam inspections. Existing civil engineers would remain focused on evaluating dam structure integrity and performance and conducting review of auxiliary/ancillary structures, while security issues would be addressed by cyber-and physical- security specialists. By 2020, the Commission had created and staffed a security branch composed of four cybersecurity specialists and five physical security specialists.

Security specialists monitor open-source information, unclassified government issuances and classified intelligence to discern pertinent security related events, incidents and trends. Staff also reviews alerts from the E-ISAC (NERC), FBI Cyber Outreach, FEMA (DHS), HSIN (DHS), ICS-CERT, US-CERT, and Shields Up & Shields Ready (CISA) to ensure that FERC licensees are made aware of potential threats or vulnerabilities.

Dam owner/operator's implementation of physical and cybersecurity measures are reported to the Commission in an Annual Security Compliance Certification (ASCC). Staff review each ASCC to assess the status of an operator's efforts regarding: vulnerability/security assessments; documentation of cyber assets and associated criticality designations; implementation of cybersecurity controls; the posture of on-site security; and

[4] Federal Energy Regulatory Commission. *Oroville Dam Service Spillway (P-2100).* https://www.ferc.gov/dam-safety-and-inspections/oroville-dam-service-spillway-p-2100.

identification of contacts for security alerts. The accuracy and completeness of these submittals, along with an entity's size and criticality of remotely controlled assets, factor into which owners/operators and dams are identified for either a physical security inspection or a cybersecurity audit.

During the scheduled audit, FERC security branch auditors facilitate a discussion with the owner/operator's staff on the project's critical features and potential impact to population, economy, and disruption of essential services. The overview helps focus efforts on what cybersecurity measures would be most effective for those features and assets to mitigate a failure path that could lead to downstream consequences. After auditors have established an understanding of the physical project operations and potential impacts, they review network architecture diagrams with the dam owner/operator staff. This allows the entire team to understand project digital communication paths, logical interconnections, and system designs. The network architecture review enables identification of the types of network protection and monitoring the organization has in place, how critical systems are segmented from less critical systems, and how communications and data flow are secured. Review of the network diagrams permits auditing of the cybersecurity policies, management practices, and other administrative controls that are employed to ensure protections are implemented and remain in place. Written cybersecurity policies and procedures are reviewed and referenced as needed during the audit to support evidence of mitigation implementation and to identify any areas for improvement. In addition, a select set of assets are physically inspected to verify security posture based on the documentation provided and the information gathered during owner/operator staff interviews. These assets generally include the organization's main operations, dispatch and/or control center that monitors or operates multiple hydropower facilities.

Following each audit, formal recommendations are issued for follow-up by the dam owner/operator and security branch staff tracks resolution of those recommendations. When instances arise where needed measures require multi-year capital improvement projects (such as upgrading all physical and digital networking devices for improved reliability), dam owners/operators propose a risk-based plan and schedule of milestones along with temporary mitigation measures. Identified milestones are tracked with letters of confirmed completion throughout the project's duration. At any point during the implementation process, a progress audit can be conducted to validate completed milestones and progress.

IV. Conclusion

Since 2016, the Commission has incorporated review of licensee's cybersecurity measures into its program for ensuring the safety of non-federal hydropower projects. The Commission's focus has been on ensuring that the wide range of dam owners/operators understand the measures needed to protect the control systems used to manage operation of the water control features at jurisdictional projects and that these licensees are aware of potential threats or vulnerabilities. Beginning in FY 2022, the Commission undertook audits of owner/operators with remotely operable assets designated as “Critical” to assess compliance with the Commission’s physical and cybersecurity standards. By the end of FY 2024, staff of the security branch will have performed 271 physical security inspections and completed cybersecurity audits covering the owner/operators responsible for 37% of the installed non-federal hydropower generation capacity.