FERC Podcast Transcript
September 6, 2019

Energy Cybersecurity

Craig Cano: Welcome to Open Access, I'm Craig Cano. Our topic today is cybersecurity, and FERC's role in identifying and addressing cyber threats to energy facilities under the Commission's jurisdiction. Joining us are Andrew Dodge, director of FERC's Office of Electric Reliability, and Joe McClelland, director of FERC's Office of Energy Infrastructure Security. Gentlemen, welcome to the podcast.

Craig Cano: Andy, let's start with you. Tell us what the Office of Electric Reliability does?

Andy Dodge: The Office of Electric Reliability oversees the development and review of mandatory reliability and security standards. We ensure that users, owners, and operators of the bulk power system comply with the electric system reliability standards approved by the Commission. In addition, the Office monitors real-time events on the bulk power system and will lead, or join in, inquiries and investigations of blackouts, near-misses and other events to determine if reliability standards were violated, if changes to standards are needed or if the standards are adequate to ensure reliability.

Craig Cano: Turning to you Joe, what role does the Office of Energy Infrastructure Security play regarding potential cyber risks to FERC-jurisdictional facilities?

Andy Dodge: Our office provides the second half of a "two-fold" approach: We help the Commission to seek, identify and communicate comprehensive solutions to potential risks to FERC-jurisdictional facilities from cyber attacks and physical threat risks. To do that, we work collaboratively with our federal partners, the states and the energy industry by participating in assessments, interagency initiatives, workshops and classified briefings.

Craig Cano: Andy, the Commission recently revised the Critical Infrastructure Protection standard on incident reporting. Tell us about that.

Andy Dodge: The CIP standards involve various reliability requirements that have the goal of protecting the cyber and physical security of the nation's electric grid. But the

Commission was concerned that the current reporting requirements might understate the true scope of cyber-related threats facing the grid because the responsible entities were only required to report cyber incidents if the incidents compromised or disrupted one or more reliability tasks. For example, by causing an electric system outage.

So, the Commission directed this change to strengthen grid cybersecurity by requiring entities with cyber systems subject to reliability standards to timely report compromises and attempted compromises to their Electronic Security Perimeter and associated Electronic Access Control and Monitoring Systems.

The newly approved standard, known as CIP-008-6, will enhance the reporting of cybersecurity incidents by requiring responsible entities to report cyber incidents that have compromised a system without necessarily impacting a reliability task. In addition, responsible entities must report attempted cyber incidents.

Reporting on incidents that compromise or attempt to compromise an entity's cyber systems will increase awareness and understanding of the scope of cyber related threats facing the Bulk Electric System, providing a more accurate picture of the rapidly changing threat landscape that will better prepare entities to protect their critical infrastructure from cyber security threats and vulnerabilities.

Craig Cano: So how will the revised standard help to improve the reliability and security of the grid?

Andy Dodge: By broadening the mandatory reporting of cyber security incidents, we are helping to provide a more accurate picture of the rapidly changing cyber threat landscape. One goal is to create a more extensive baseline understanding of the nature of cyber threats and vulnerabilities. Mandating the reporting of cyber events involving attempts to compromise BES Cyber Systems and specifying the minimum content, dissemination, and filing deadlines for the reports will enhance the reliability of the grid by providing a more accurate picture.

Craig Cano: How does an entity know if its systems are compromised or have experienced an attempt like you mention?

Andy Dodge: That's a great question. We understand responsible entities are already monitoring their networks and employ many security controls, some that are mandatory and most that are voluntary based on best security practices and an entity's unique needs, architecture configuration, and core functions that alert them attempts on their system.

The enhanced reporting requirements will ensure a better baseline understanding of how the threat landscape may exploit vulnerabilities of cyber systems that operate the Bulk Electric System.

Craig Cano: Will that be a burden on industry?

Andy Dodge: We take that question very seriously and it's one of the measures staff researches and analyzes when proposing any action on rulemaking. There are requirements within the CIP Reliability Standards that already require entities to track data on compromises or attempts to compromise their systems, so the revised Reliability Standard will not significantly increase the reporting burden on entities because it builds off the currently effective reporting threshold by expanding it to address some reliability gaps.

Craig Cano: Who will receive the reports from the responsible entities?

Andy Dodge: Once the Reliability Standard goes into effect, and under the timeline set by the Commission we anticipate that date will be January 1 of 2021, responsible entities will be required to send the reports and updates to the Electricity Information Sharing and Analysis Center as well as the Department of Homeland Security, and also to the Commission in the form of an annual summary report.

Craig Cano: So, they won't be sending these cybersecurity incident reports directly to FERC?

Andy Dodge: That is correct. Though we are the federal regulator, we are not the correct audience for this information. These incident reports on compromises and attempted compromises need to get in to the hands of industry and quickly. However, I should say that the North American Electric Reliability Corp. – which is the FERC-certified electric reliability organization – will file an annual, public, and anonymized summary of the cybersecurity incidents with the Commission.

Craig Cano: Andy has described for us how the reliability standards work to ensure that companies can identify, assess and protect against cyber threats. But Joe, what are threats that you and your team see out there?

Joe McClelland: As Chairman Chatterjee noted in testimony before the House Energy and Commerce subcommittee on energy earlier this summer, the nation's critical infrastructure is increasingly under attack by foreign adversaries, and this evolving

threat landscape demonstrates the importance of an unwavering focus on the security of the nation's critical energy infrastructure. Widespread disruption of electric service can undermine the security of the United State — our government, the military, and the economy — as well as endanger the health and safety of all of us.

According to a January 2019 report by the Office of the Director of National Intelligence (and I quote here), "China, Russia, Iran, and North Korea increasingly use cyber operations to threaten both minds and machines in an expanding number of ways — to steal information, to influence our citizens, or to disrupt critical infrastructure." The report goes on to quote specific nation/state capability including that "China has the ability to launch cyber attacks that cause localized, temporary disruptive effects on critical infrastructure — such as disruption of a natural gas pipeline for days to weeks — in the United States" and that "Russia has the ability to execute cyber attacks in the United States that generate localized, temporary disruptive effects on critical infrastructure…" and that they are "mapping our critical infrastructure with the long-term goal of being able to cause substantial damage."

Of course, these threats are joined by other threats from a host of actors such as from supply chain compromises, insider attacks, ransomware campaigns, internet-of-things vulnerabilities, and many more.

Craig Cano: How does FERC work with its federal and state partners and the energy industry in addressing these threats?

Joe McClelland: I'm glad you asked that question because this is a multi-layered effort that requires many players. We engage with our partners in numerous ways to address both cyber and physical security issues for critical energy infrastructure. These initiatives include such things as voluntary architecture assessments of interested entities, classified briefings for state and industry officials, collaborative work with the NERC Electricity Information Sharing and Analysis Center and others to rapidly issue bulletins and alerts, and joint security programs with other government agencies and industry.

Craig as you aware, the Commission has varying degrees of authority over several different types of energy infrastructure in addition to the Bulk Power System including oil and natural gas pipelines, LNG terminals and hydroelectric facilities. We share jurisdiction with other agencies such as TSA and Coast Guard as well as the Sector Specific Agency for Energy, which is the Department of Energy. It is important that we carefully coordinate our actions leveraging resources and expertise wherever possible. Therefore, it is very important that we participate in interagency and intelligence-related coordination and collaboration efforts with all of the appropriate federal and state

agencies, as well as the industry representatives on cyber and physical security matters related to FERC-jurisdictional energy facilities.

The responsibility for securing critical infrastructure is shared by industry and government authorities at the federal and state levels, so we believe it is imperative that we continue to strengthen these partnerships.

Craig Cano: Joe, you said a couple of things there that I'd like to follow up on. First, you mentioned voluntary architecture assessments — what are they?

Joe McClelland: Voluntary architecture assessments are an important part of our office's work. As every industry member has customized computer networks sometimes with tens-of-thousands of pieces of interconnected equipment, it is important to review the system in detail to identify any vulnerabilities that may exist in the context of current cyber threats. As with FERC, other federal agencies such as DHS, TSA, the Coast Guard, and DOE have also determined that assessments like these are an important way to address specific cybersecurity problems.

Our office sends a team of cybersecurity subject matter experts to spend 2-3 days at the company's facility reviewing their facilities for things like inventory management, system connectivity, network traffic analysis, security protocols, employee training, backup and restoration systems, and other key items. Wherever there is overlapping jurisdiction such as with natural gas pipelines or LNG terminals, the other federal agencies (in these cases TSA and Coast Guard) are included in the assessment.

The company representatives are briefed on the results of the assessments at the conclusion of the assessment; including any recommendations for mitigating actions. We have seen substantial improvements to the security posture of these organizations as a result of these engagements.

Craig Cano: You also mentioned interagency collaboration. Can you give us an example?

Joe McClelland: Yes. In addition to the architectural assessments, on March 28 of this year FERC and the Department of Energy held a joint technical conference with federal, state, and industry officials, to discuss investment incentives for cyber and physical security. Among the participants were representatives from the Department of Homeland Security, the Department of Defense and the National Counterintelligence and Security Center from the Office of the Director of National Intelligence.

The conference looked at the current threats against energy infrastructure, best practices for mitigation, the adequacy of current incentives for investing in physical and

cyber security protections, and cost recovery practices at both the state and federal level. The transcript from the conference is available on the Commission's web site for anyone who missed the event. It makes good reading.

Craig Cano: What was one of the key takeaways for you from the conference?

Joe McClelland: Craig, one of the key takeaways was the importance of public/private cooperation and partnership focused on securing critical infrastructure. We routinely work with the states on an individual, regional and national level, industry associations and stakeholder groups, the Information Sharing and Analysis Centers and others to conduct open and classified briefings, help produce bulletins and alerts, and to assist with table-top security exercises to help keep the states and industry informed of, and able to, address cybersecurity threats.

Again, it's important for us all to work together in a thoughtful way to ensure that all of these important issues are addressed effectively.

Craig Cano: Well on that, I going to have to wrap this up. Thanks to our guests Andy Dodge and Joe McClelland. Improving the cybersecurity of the energy facilities under the Commission's jurisdiction is, and will remain, one of the Commission's most important responsibilities.