A-4 Staff Presentation

Slide 1

FERC Cyber Security Focus Areas

Office of Electric Reliability, Office of Energy Infrastructure Security, and Office of Energy Projects

November 21, 2019

Good morning Chairman and Commissioners,

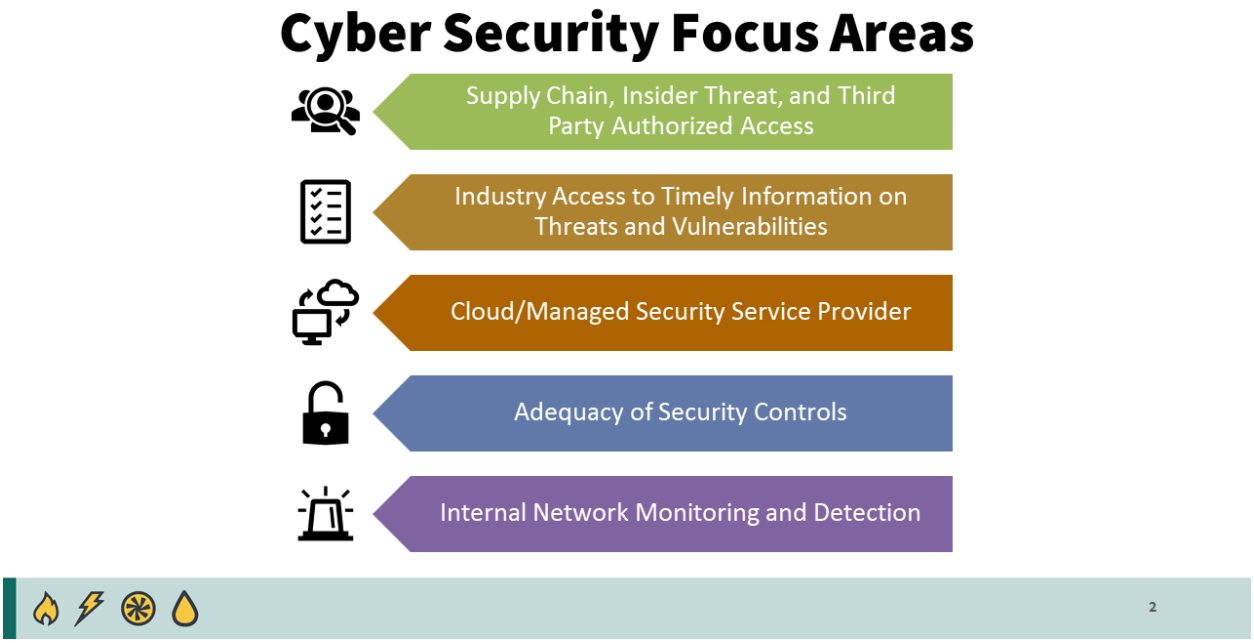
Thank you for the opportunity to present today on the Commission's cyber security focus areas and to highlight a number of the key cyber security program priorities across the Commission. Earlier this year, Chairman Chatterjee directed the Office of Electric Reliability, the Office of Energy Infrastructure Security, and the Office of Energy Projects to build on their ongoing cybersecurity efforts by identifying areas in which we may work collectively for the benefit of the Commission, consumers and regulated entities. This presentation identifies five focus areas on which Commission staff plans to strategically and collectively focus our efforts to address associated critical infrastructure risks and vulnerabilities. The nature of the Commission's work has always required significant coordination among the Commission's program offices, and these five focus areas allow greater opportunity to target that coordination in ways that will have the most impact on the security of the infrastructure we oversee.

Staff identified these five focus areas by drawing on the experience and knowledge of each of the relevant offices to determine issues that would allow staff to address the cyber security of Commission jurisdictional facilities. Staff considered known threats, observed vulnerabilities,

and potential consequences if a security incident were to occur. Staff's development of the five focus areas was informed by a review of public and non-public threat reports; a review of significant cyber security events across the globe, particularly those that impacted industrial infrastructure; the currently enforceable NERC CIP standards; and the Office of Energy Projects, Security Program for Hydropower Projects Revision 3a guidelines.

Staff will first briefly describe each of the five focus areas, and then we will provide an overview of a few key initiatives staff has undertaken to address these items.

Slide 2



This slide identifies the five focus areas, but I stress that each issue is important in its own way and these are not listed in order of importance.

Supply Chain/Insider Threat/Third Party Authorized Access

Each of these three categories relates to methods by which an attacker can bypass perimeter security controls. These categories are critical because compliance requirements and best security practices to secure an entity's systems are rendered of little value if an attacker can simply bypass those controls.

Industry Access to Timely Information on Threats and Vulnerabilities

Under this focus area we recognize that many entities have limited threat intelligence capabilities and access to information on threats, vulnerabilities, and the mitigation of risks. Improving access to that information is critical to ensuring that companies can act on relevant, time-sensitive, and well-supported information about threats and vulnerabilities.

Cloud/Managed Security Service Provider

This focus area acknowledges that as entities explore how to deploy cloud and managed security service providers, it is critical that they do so in a secure manner. If implemented properly, the use of a trusted third party to perform common tasks and services can yield security benefits by allowing the entity to focus on more complex issues in house and to optimize their security resources. However, more research needs to be conducted to determine if the most critical systems, such as those used for real-time operations, could be used in the cloud.

Adequacy of Security Controls

This focus area acknowledges that there are many assets connected to Commission jurisdictional facilities that are subject to either minimal or no mandatory cybersecurity controls. In particular, although Low Impact BES Cyber Systems (BCS) make up the majority of BES cyber assets, there are very few mandatory security controls required for these assets. While Low Impact BES Cyber Systems, by definition, have a lower impact on the BES, the simultaneous loss or degradation in a large number of these systems could have a significant aggregate effect. In addition, many Commission jurisdictional hydroelectric facilities connect to a Low Impact BCS facilities that are not subject to high levels of mandatory security controls. Likewise, natural gas pipelines are not subject to mandatory cyber security controls, but disruption of these pipelines could still have a significant impact on the BES.

Internal Network Monitoring and Detection

Under this focus area, we acknowledge that most cyber security efforts focus on keeping an attacker out, but once inside, attackers can loiter undetected for extended periods. Internal monitoring of the protected networks is not required by the NERC CIP standards and may not always be performed in a robust manner. Lack of monitoring and detection in these networks may miss lateral movement by an attacker.

Transition language: We will now turn to providing an overview of some key program initiatives the Commission staff is undertaking to better respond to the risks we've discussed. These initiatives are presented in three categories: First, there are a few internal efforts that are currently underway to better position the Commission to address emerging cyber security concerns. Second, we will discuss our efforts to reach out to industry and work directly with

entities to promote enhanced security. Finally, we will highlight a few specific priority initiatives that are being developed.

Slide 3

The Commission's Office of Energy Projects has taken steps to meet current and future needs in its security program for jurisdictional Hydropower Projects by establishing a new security-focused group within the Division of Dam Safety and Inspections (D2SI) composed of Physical and Cyber Security Specialists. The formation of this new group will allow D2SI dam safety engineers to focus on dam safety at jurisdictional projects while the new security group will focus on physical and cyber security concerns. The new security group will be responsible for:

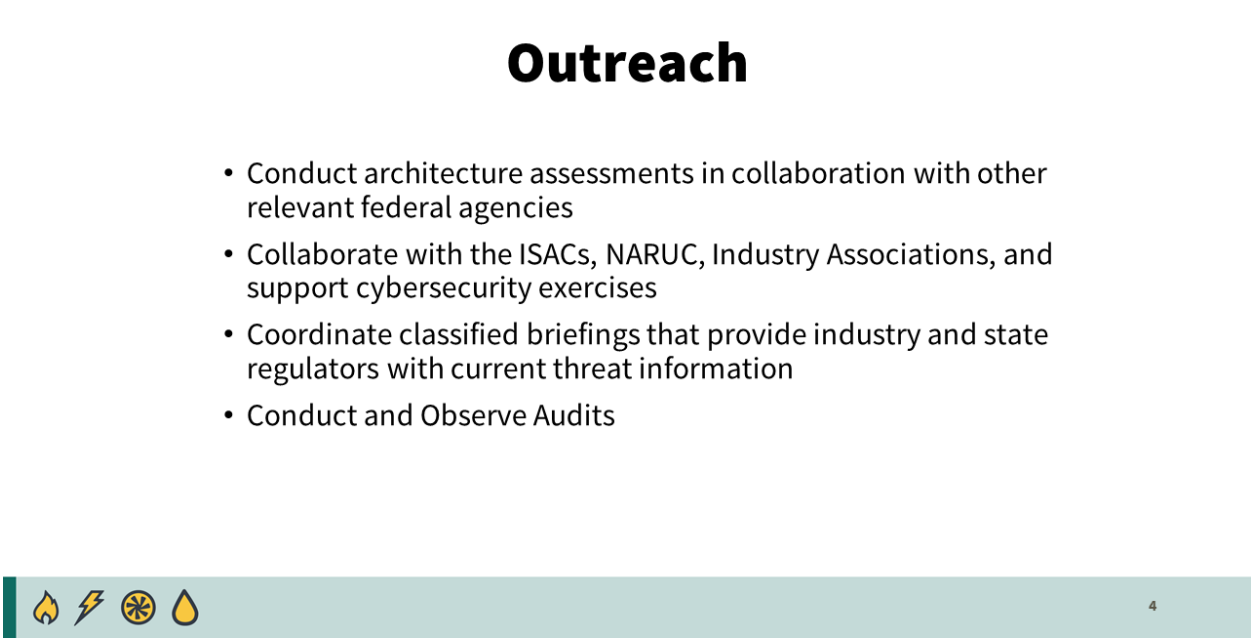
- Maintaining technical expertise, mentoring, and performing as team leaders for analyses and resolution of cyber and physical security issues for the Commission's Dam Safety Program.
- Performing special security inspections, both physical and cyber, and participating as an evaluator during security exercises.
- Conducting surveys and risk analyses to assess security needs, identifying and assessing the degree of vulnerability, and ensuring that selected protection measures are implemented effectively.

These efforts build upon the Commission's Security Program for Hydropower Projects that was established in 2001 with Cyber security guidance that became effective January 2016.

The Office of Electric Reliability has also recently realigned the functions of its office and has focused one of those functions exclusively on cybersecurity.

The Commission's program offices collectively work on these issues allowing the Commission and its staff to work toward providing regulated entities with consistent, well-sourced information on these risks, whether through, for example, a hydroelectric dam security inspection, a compliance audit, a voluntary network assessment or other means.

Slide 4



Picking up on that last theme, a major focus of our efforts to promote enhanced security is to improve and build-upon our existing outreach initiatives.

Commission staff in our Office of Energy Infrastructure Security offer voluntary network architecture assessments of electric, hydroelectric, natural gas, and liquefied natural gas facilities in collaboration with other relevant federal agencies including DHS, TSA, and Coast Guard.

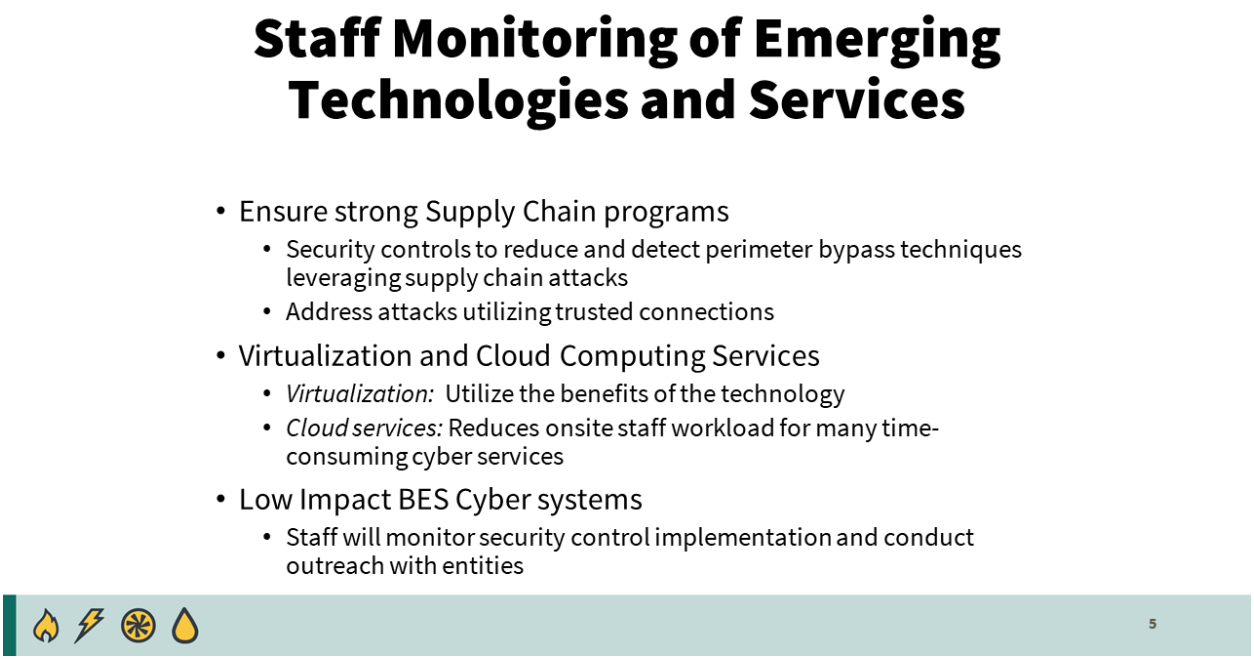
Commission staff also coordinates with the information sharing and analysis centers (ISACs), state regulatory commissions and associations, industry associations, and supports relevant

cybersecurity exercises to develop, improve, and distribute valuable threat, vulnerability, and mitigation information.

Commission staff also coordinates and participates in classified briefings in collaboration with the Department of Energy and the Office of the Director of National Intelligence that provide industry and state regulators with current threat information.

Commission staff also provides relevant threat and risk mitigation information during both the Commission-led CIP compliance audits and routine observations of audits performed by NERC and the Regional Entities.

Slide 5



In closing, I would like to highlight a few key issues that Commission staff will be closely monitoring in light of the identified focus areas. Staff will continue to monitor entities' supply chain security implementation and use of trusted connections. Additionally, staff will monitor entities' adoption of new technologies and services to address cyber infrastructure implementation, maintenance, and/or management. These technologies and services include virtualization of systems and use of cloud computing services. Staff will continue to gather information and work with regulated entities on these issues as well as potential modifications to the CIP standards, such as the security controls for Low Impact BES Cyber Systems.

Thank you again for the opportunity to present today. The team is available to answer any questions you may have.