Remarks

FERC Reliability Technical

Conference Panel IV – Grid Security

June 22, 2017

Presentations: Cybersecurity continues to be a rapidly evolving risk to the Bulk-Power System. CIP Reliability Standards are designed to mitigate the cybersecurity risks to bulk electric system facilities, systems, and equipment, which, if destroyed, degraded, or otherwise rendered unavailable as a result of a cybersecurity incident, would affect the reliable operation of the Bulk-Power System. The 2015 and 2016 cyber-attacks on the electric grid in Ukraine are examples of how cyber systems used to operate and maintain interconnected networks, unless adequately protected, may be vulnerable to cyber attack.

a. While controls in the CIP Reliability Standards reduce the risk of cyber-attacks, additional controls or modifications may further mitigate potential impacts on the operation of the Bulk-Power System. Which controls have been most effective? Are there additional controls, modifications, or voluntary actions that should be considered to improve cybersecurity? What partnerships should the Commission form or strengthen to help improve the overall cybersecurity posture of the Bulk-PowerSystem?

b. A system is only as secure as the people who run and operate it. What can the Commission do to facilitate or encourage a strong cyber workforce?

INTRODUCTION

Georgia System Operations Corporation, on behalf of NRECA, appreciates the opportunity to participate on the Grid Security Panel at today's Federal Energy Regulatory Commission (FERC) Reliability Technical Conference regarding the Bulk-Power System.

Georgia System Operations Corporation (GSOC) is a not-for-profit system operations company, operating as a cooperative. Our Members are 38 of Georgia's distribution electric membership corporations, Oglethorpe Power Corporation (OPC) and Georgia Transmission Corporation (GTC). GSOC is one of four companies — along with OPC, GTC and Smarr EMC — that this group of EMCs (the distribution Members) formed to provide and deliver wholesale electric services. GSOC was formed in 1997 when OPC spun off its transmission and system operations business units to form GTC and GSOC, respectively, although GSOC, in effect, has been managing system operations since 1990. As the system operator, GSOC ensures reliable, safe, independent system operations by controlling and monitoring electric generation, transmission and distribution assets owned by OPC, GTC, Smarr EMC, the Members and their power supply partners. As a registered Transmission Operator, GSOC complies with applicable North American Electric Reliability Corporation (NERC) reliability standards and operates within the Southeastern reliability region of the SERC Reliability Corporation (SERC). GSOC also manages the CIP role for itself and for Georgia Transmission Corporation.

GSOC is committed to ensuring the security and resiliency of the electric grid in Georgia. We implement security practices in our tools and technology and maintain a 24x7 security operations center to ensure that we remain vigilant night and day, 365 days a year. We also actively participate in industry security

activities including the Electricity Subsector Coordinating Council, the Electricity Information Sharing and Analysis Center (E-ISAC), the North American Transmission Forum, and NERC CIP standards development activities, among others.

REDUCING THE RISK OF CYBER ATTACK

Which controls have been most effective?

NERC CIP standards outline a disciplined approach to protecting the reliability and security of the Bulk Electric System. These standards mitigate the risk that operational systems will be damaged or destroyed due to a cyber-incident and ensure that we will be able to promptly recover from any damage that might occur. It has been nearly a year since the CIP version 5 standards became effective. The transition to CIP version 5 has been difficult, yet has yielded significant security benefits to the Bulk Electric System. A key aspect of CIP version 5 was the introduction of the cyber system impact categorization afforded by CIP-002, which has expanded protection to the entire Bulk Electric System while acknowledging that not all facilities have the same risk profile.

Overall, no single set of individual controls stands out as the most effective. It is the interrelated nature of the controls that together provide a defense-in-depth posture that makes the CIP standards effective. The core elements that we have found important to this defense-in-depth posture start with training and awareness. Security starts with people. Having all staff, including those not involved in operations systems or IT, keenly aware of the damage that a cybersecurity incident can cause is critically important to reducing the chance of successful cyber-attack and the consequent damage to, or mis-operation of, operational systems. Then, a defense-in-depth posture requires knowledge of the system inventory and application of the controls necessary to protect it, including network isolation, patching, malware detection, and intrusion detection. These processes mitigate risk of infection and assist in identifying where abnormal incidents are occurring. This alerts us of existing problems and provides advanced notice of those that might be on the horizon. To keep our people sharp and continually improve our processes, exercises are essential, including performance of drills that test response capabilities for cyber incidents or non-cyber incidents like natural disasters. Backup systems should be tested on a regular basis to assure they continually operate correctly in case of an emergency situation on the primary system. Worst-case scenario planning can anticipate critical response strategies if systems are compromised. This is the framework that the existing requirements provide.

Notably, the version 5 CIP standards introduced additional controls for interactive remote access that are consistent with a key lesson learned from the Ukraine event. CIP-005 includes requirements mandating that all Interactive Remote Access must first pass through an intermediate system and leverage multi-factor authentication. As we saw in the Ukraine event, the adversary was able to leverage legitimate credentials, obtained via phishing, to remotely access operational systems. Use of multi-factor authentication would have gone a long way in mitigating this vector of attack.

At GSOC, we have gone beyond the requirements of the CIP standards and developed a set of internal controls to ensure compliance and more aggressively mitigate security risks. We have internal controls not only for the CIP operations but also for the other BES operations. Further, we have internal controls across every department of our entire corporation addressing those risks that could subject GSOC to potential harm. We have embraced internal controls as part of our day-to-day operations to help avoid mistakes that might lead to mis-operations or permit cybersecurity breaches. Over time we

have formalized these controls and continue to test and monitor them for effectiveness. Corporate goals measuring the implementation and ongoing monitoring and testing of these internal controls were approved by our Board and are a component of our employees' performance pay.

Are there additional controls, modifications, or voluntary actions that should be considered to improve cybersecurity?

We urge restraint on pursuing the addition of new mandatory standards. We are still within the first year of the CIP version 5 standards being mandatory and have not yet reached the milestone of mandatory electronic access control and physical access control requirements for low impact BES Cyber Systems, but we note that substantial strides have already been made. Time is still needed to fully implement the version 5 CIP standards and to absorb the lessons learned from that implementation.
Further, we are motivated to protect our systems and our infrastructure without mandatory standards because, simply put, delivering reliable electricity is our business. Implementing the necessary security controls is essential to us delivering to our customers and succeeding as a business. We believe that voluntary recommendations and actions should lead before mandatory standards. Other organizations, such as the E-ISAC, are well positioned to coordinate voluntary recommendations to industry.

During this first year of mandatory compliance, we have learned that some standards, as written, are taking a disproportionate amount of effort to execute as compared to others. In particular, we highlight the CIP-007 patching and CIP-010 baseline standards. While we certainly recognize these standards are important, they are also among the most prescriptive.

We believe that an improved security benefit could be achieved with greater effectiveness if these standards focused on the security objective rather than specifying performance details. For instance, the current patch management requirement specifies a specific process to assess security patches every 35 days, implementing applicable security patches within 35 days of the determination of applicability, and documenting mitigation plans for any patches that could not be applied within that window. An equally effective alternative approach could be to focus on the security objective of a flaw remediation and vulnerability management program.

We believe that the existing CIP standards mandate the necessary elements of a solid foundational cybersecurity program. We also recognize that as the cybersecurity field continues to mature, new technologies will be introduced that could improve the overall security posture of the grid. The Commission should resist the urge to mandate such new technologies. These new advanced security technologies will, no doubt, come and go. By the time a new technology can be incorporated into a mandatory standard, it may no longer represent the state of the art. Our approach moving forward must ensure that a solid security framework is in place, but also enable us to be nimble in the face of an ever-changing threat landscape.

Some areas that exemplify this include the way the industry, and GSOC in particular, has embraced cybersecurity awareness and training. Not only are employees that are directly involved in cyber operations being trained, but all employees at GSOC receive special training and constant exercise on how to avoid being "phished" as well as awareness of other evolving cybersecurity issues. GSOC performs annual business continuity tests where all employees work from an alternate work location in a coordinated exercise to ensure that operations would not be disrupted in the event of a

cybersecurity event or other issue affecting our business operations.

As our industry embraces a culture of internal controls, we need to continue to move towards an environment where the focus of the oversight is on ensuring that controls are in place to monitor and maintain compliance and security. Deficiencies that are detected and corrected by a company's controls should not result in a violation.

What partnerships should the Commission form or strengthen to help improve the overall cybersecurity posture of the Bulk-Power System?

The participants of the Bulk Electric System have a very productive partnership with the Federal government through the Electricity Subsector Coordinating Council (ESCC). The ESCC is the principal liaison between leadership in the federal government and in the electric power sector, with the mission of coordinating efforts to prepare for national-level incidents or threats to critical infrastructure. It consists of electric utility executives who share experience and knowledge concerning electric utility operations. The ESCC facilitates and supports policy- and public affairs-related activities and initiatives designed to enhance the reliability and resilience of the electric grid. These activities include all hazards, steady-state preparation, and emergency preparedness, response, and recovery for the nation's electricity sector.

The ESCC has recently endorsed the E-ISAC's Long Term Strategic Plan. This plan reflects priorities identified by the NERC Reliability Issues Steering Committee. The effort will identify, prioritize and assure effective and efficient mitigation of risks to the reliability and security of the North American grid. The ESCC is also a key coordination point between the electricity sector and other critical infrastructures such as telecommunications, oil & natural gas, financial services, transportation, and water. The ESCC is working in coordination with the E-ISAC to bring these sectors together to improve cross-sector awareness and facilitate cross-sector exercises. Exercises such as GridEx IV planned for November of this year, are just one example of how the electricity sector is committed to improving resiliency and ensuring cyber-preparedness.

We agree that mandatory standards are a core component to a secure and resilient grid. However, industry is engaged in many activities above and beyond mandatory standards aimed at improving the overall cybersecurity posture of the Bulk Electric System. We encourage FERC to collaborate with the ESCC to determine the best way to engage with supporting industry's commitment to a secure and resilient grid.

<u>BUILDING A STRONG CYBER WORKFORCE</u>

A system is only as secure as the people who run and operate it. What can the Commission do to facilitate or encourage a strong cyber workforce? We suggest that FERC assist in encouraging new cyber graduates to work in the electricity sector. Current federal programs cover tuition or forgive student loans in exchange for federal service. FERC should consider a similar model, supported by federal funding, for cyber positions within the electricity sector.

Security training is necessary and expensive. The security landscape is evolving and the cyber workforce must continually update their skillset in order to remain effective. FERC should support efforts for the industry to receive training from other federal agencies with advanced security expertise, such as the

Department of Energy, Department of Homeland Security, and the Department of Defense.

As the cyber workforce develops within the electricity industry, satisfying, rewarding, and challenging work is vital to its development. The protection of our nation's electric grid is a worthy effort that can and should attract top talent. We must engage this workforce in the implementation of a comprehensive defense in depth security program. To do so, we must have standards that allow these professionals to focus on security objectives rather than administrative compliance activities. We must ensure that they have the necessary opportunities for training. Then we must continually exercise our response capability. Leveraging government and other partnerships is key to that effort. The E-ISAC is one such partnership that makes our workforce more effective by facilitating the sharing of information pertaining to physical and cyber threats, vulnerabilities, incidents, protective measures and practices amongst our workforce. The E-ISAC also provides rapid response through the ability to effectively contact and coordinate directly with the workforce of member companies. It also coordinates and participates in governmental critical infrastructure exercises such as the DOE's office of Electricity Delivery and Energy Reliability Clear Path exercise held on May 31 and June 1 this year and the upcoming GridEx IV exercise in November.

CONCLUSION

GSOC appreciates the focus and effort of the Commission to improve the security posture of the grid. The existing CIP standards mandate the necessary elements of a solid foundational cybersecurity program. GSOC takes cybersecurity seriously and has embraced the FERC, NERC and SERC reliability standards programs, taking significant steps to implement version 5 of the CIP Standards, including an internal controls framework to ensure they are effectively maintained.

While we are identifying lessons learned thus far from implementation, we also believe that time is still needed to fully implement the CIP version 5 standards and absorb the lessons learned from that implementation. Once fully implemented, careful steps, if needed, should be considered to improve the existing standards to focus on the security objective rather than specifying process details.

The defensive posture and capabilities of today's electric utilities can be improved by embracing cyber and physical security, and by participating in groups like the E-ISAC, regional entities and NERC grid training exercises to hone prevention, response, and recovery mechanisms.

Finally, we would like to thank the Commission for the opportunity to participate in this panel on such an important topic.