NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FERC Reliability Technical Conference

Panel III: ERO Performance and Initiatives

Remarks of Gerry Cauley, President and CEO
North American Electric Reliability Corporation
June 4, 2015

Chairman Bay, Commissioners, and fellow panelists, I appreciate the opportunity to address the topics identified for the third panel of today's important conference. The ERO's performance and initiatives identified for discussion today include a focus on the key enhancements to our Compliance Monitoring and Enforcement Program. Sonia Mendonca, NERC's Deputy General Counsel and Vice President of Enforcement will outline the various process improvements undertaken by NERC and the Regional Entities.

I would like to take this opportunity to commend the efforts of Sonia, her team, and the regions on this effort. This truly has been a collaborative partnership and a true reflection of the value and strength of the ERO's structure.

For my part in today's panel, I will focus on the two questions dealing with the Electricity Subsector Coordinating Council (ESCC) and the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), as well as the questions addressing geomagnetic disturbances and NERC's physical and security standards.

ESCC and the ES-ISAC

As I noted in my opening comments, never have we seen a more challenging period for reliability and security than we do today. NERC's actions on standards and information sharing are key components in responding to the numerous threats and vulnerabilities. While our standards provide an important foundation, NERC's ES-ISAC is an essential information sharing hub that provides situational awareness, incident management, coordination, and communication capabilities within the Electricity Subsector through timely, reliable, and secure information exchange.

We thank the Commission for its support of NERC's budget, which has provided for more staff and additional steps to further develop and secure the operations of the ES-ISAC. Enhancements to the portal, along with increased participation from industry, support from the ESCC, and greater coordination with both industry and government partners are contributing to the success of the ES-ISAC.

The ES-ISAC is a leading source for voluntary information sharing for many in the Electricity Subsector. It gathers information from electric industry participants across North America about security-related events, disturbances, and off-normal occurrences within the Electricity Subsector and shares that information with other electric industry participants, and key governmental entities. The governmental entities also provide

the ES-ISAC with information regarding risks, threats, and warnings that the ES-ISAC disseminates throughout the Electricity Subsector.

The ES-ISAC uses a variety of tools, programs, and activities to enhance security, such as a secure web portal, alerts, exercises, and training and education. For some companies in the Electricity Subsector, the ES-ISAC portal is the first and often primary interface with the ES-ISAC. The portal allows the ES-ISAC to reach thousands of industry members and hundreds of organizations across the subsector and is the mechanism for industry and government to contact ES-ISAC staff with questions, concerns, and security-related information in a secure manner. As a result, NERC continues to grow the ES-ISAC's capabilities by enhancing the ES-ISAC's private, secure portal to receive voluntary reports from industry members and working with various organizations (both industry and government) to obtain the data and mechanisms necessary to conduct these information sharing activities. To date, the total number of organizations inside the portal is 799; the total number of portal users is 2,835.

A recent addition to the ES-ISAC's toolset is the Cybersecurity Risk Information Sharing Program (CRISP). CRISP is a collaborative effort between critical electric power utilities and the U.S. government. Participating critical infrastructure owners and operators provide cybersecurity data in near-real-time to Pacific Northwest National Laboratory and the ES-ISAC, and in return, receive automated analytics and analysis from a team of cybersecurity specialists. The program also allows participants to receive machine-to-machine threat information and mitigation measures. CRISP represents a maturation of the private-public partnership established under the National Infrastructure Protection Plan, and benefits both industry and government. No other program shares cyber intelligence information fused with industry information in a collaborative sharing framework in the same way as CRISP.

Outside of the ES-ISAC, we receive strong support from the ESCC, a key organization representing all segments of the electricity industry. The ESCC, the only sector coordinating council exclusively comprised of chief executive officers, is an outstanding example of a strong public-private sector partnership and provides key communication with our government partners coordinating efforts related to disasters and threats to critical infrastructure. Its government counterparts include senior Administration officials from the White House, relevant Cabinet agencies, federal law enforcement, and national security organizations.

The ESCC has three main areas of focus: tools and technology, information flow, and incident response. To support the ESCC's mission, the ESCC established a Senior Executive Working Group (SEWG), consisting of Chief Operating Officers, Chief Information Officers, and other senior executives with relevant expertise in the Electricity Subsector. The SEWG meets on a monthly basis and creates ad hoc "sub-teams" to accomplish the goals identified by the CEOs and Deputy Secretaries. In parallel to this effort, the government also is organizing around these goals with a commitment to align government and industry efforts.

Together, the ESCC and the ES-ISAC enhance the subsector's security efforts. The ESCC has called for the ES-ISAC to be the central source of information sharing between the Electricity Subsector and the government. This support for the ES-ISAC's role in information sharing has led to increased awareness and improved communication on its operation and performance initiatives. Most recently, the ESCC has undertaken a strategic review of the ES-ISAC to examine existing capabilities and expertise and develop and implement a strategy to enhance these capabilities and improve security across the subsector. We are in the final stages of this review, and recommendations will be forthcoming later this month.

Geomagnetic Disturbances

NERC appreciates the recent NOPR issued by the Commission on the stage 2 GMD standard and looks forward to future discussions with the Commission on issues identified. NERC filed the completed standard in January 2015, and sees this effort as a significant milestone in addressing the risks from extreme geomagnetic disturbances. The new standard, along with the stage 1 operating procedure standard that took effect in April, employs state of the art tools and techniques to provide assurance that the bulk electric system will operate reliably during severe GMD events. TPL-007 is based on the most advanced space weather and geomagnetism information available, which was obtained through our collaborative work with space weather researchers at NASA, NOAA, the U.S. Geological Survey, and their counterparts in Canada. These organizations have leading experience in the field and have contributed vast amounts of data and rigorous analysis to establish the models and the peer-reviewed benchmark that underpins the standard[1].

NERC will continue to advance the technical capabilities of the industry to address this high-impact, low frequency risk. In addition to a proactive effort to train and prepare the industry for their obligations under the GMD standards, our work plan going forward focuses on addressing several key areas where understanding needs to progress in order to better mitigate the risks:

- Working with EPRI, researchers at USGS, and industry we will improve the earth conductivity models that are a vital component to understanding the risks of GMD events in each geographic region. In some cases, our geological researcher partners can employ techniques to measure the earth structure which will improve localized earth models. We also will work with EPRI and SUNBURST network participating entities to use modeled and collected GIC

[1] This statement highlights that the benchmark and the spatial averaging technique are peer reviewed. The commission stated in the NOPR that the spatial averaging technique used by the standard drafting team was only discussed in the white paper justification that accompanied the standard. Subsequent to our filing, a paper describing spatial averaging and the statistic derivation of the 100-year benchmark completed peer-review and was accepted for publication in a scientific journal that covers geomagnetism topics. Authors Antti Pulkkinen (SDT member), Emanuel Bernabeu (SDT member), Jan Eichner, Ari Viljanen and Chigomezyo Ngwira. *Regional-scale high-latitude extreme geoelectric fields pertaining to geomagnetically induced currents.* Accepted for publication in journal Earth, Planets and Space.

data along with magnetometer data to assess the validity of ground models in the utility's area.

- We continue to partner with Department of Energy, EPRI, and U.S. and Canadian utilities in transformer resiliency, and in increasing the availability of thermal modeling information validated by measurement data.
- NERC is collaborating with researchers to examine more complex GMD vulnerability issues such as harmonics and mitigation assessment techniques to enhance the modeling capabilities of the industry.

The new GMD standards are written in such a way that takes advantage of the emerging technical developments that NERC is pursuing through its ongoing work plan and partnerships with EPRI and other collaborators on the NERC GMD Task Force. NERC looks forward to working with the Commission and stakeholders to address the concerns raised in the NOPR so that these important standards can be implemented as soon as possible.

CIP Version 5

NERC has been actively monitoring and supporting effective implementation of the new and revised cyber security Reliability Standards, referred to as the Critical Infrastructure Protection (CIP) version 5 standards, which were approved by the Federal Energy Regulatory Commission (FERC) in Order No. 791 on November 22, 2013. The CIP version 5 standards represent a significant improvement—and change—over the currently-effective CIP Reliability Standards, referred to as the CIP version 3 standards, as the CIP version 5 standards include new cyber security controls and extend the scope of the systems that the CIP Reliability Standards protect. Using a newly formed SDT, NERC also developed responses to the directives in Order No. 791 throughout 2014 and submitted those revisions to the Commission on February 13, 2015. The revised changes have little impact on the approach to current transition activities.

Based on its prior experience, NERC understood that myriad issues can arise as entities transition to new or revised versions of Reliability Standards. If these issues are not properly understood and addressed through guidance documents, training, and other outreach efforts, entities may not correctly implement the required security controls, which could result in reliability issues as well as a spike of noncompliance upon the effective date of the new or revised Reliability Standards. Therefore, in October 2013, NERC initiated a program, working collaboratively with Regional Entities and industry participants, to support transition from the CIP version 3 standards to the CIP version 5 standards in a manner that is timely, effective, and efficient. The transition program is designed to accomplish the following objectives:

1. *Implementation Readiness* – Improve industry's understanding of the technical security requirements of the CIP version 5 standards and help ensure that industry is technically ready to implement the CIP version 5 standards upon their effective date.

2. *Compliance and Enforcement Expectations* – Clarify expectations for compliance and enforcement of the CIP Reliability Standards to provide industry: (i) a clear path and approach to transition from CIP version 3 standards to CIP version 5 standards; (ii) an understanding of the application of NERC's risk-based approach to compliance and enforcement to CIP version 5 standards.
3. *Resource Requirements* – Provide industry and Regional Entities an understanding of the technical and compliance-related resources and efforts needed to transition and comply with the CIP version 5 standards.
4. *Consistent and Reasonable Enforcement* – Ensure that the ERO Enterprise enforces the CIP version 5 standards consistently, reasonably, and transparently.

The transition program consists of the following key elements to support accomplishing the programs objectives:

- **Implementation Study**. A study in which six industry volunteer entities implemented elements of the CIP version 5 standards in an accelerated time frame to help the ERO Enterprise understand the challenges Responsible Entities may face transitioning to CIP version 5, identify topics requiring guidance, and provide feedback and guidance to other entities based on lessons learned from the study. This study was completed on June 30, 2014, and NERC published a final report summarizing the Implementation Study in October 2014.
- **Guidance Documents (Lessons Learned and FAQs)**. Working with representatives from the Regional Entities, implementation study participants, and other industry stakeholders, NERC has been developing documents to provide guidance to industry on the implementation of various CIP version 5 requirements. The guidance documents are based on topics identified during the implementation study as well as questions that other stakeholders have brought to the ERO Enterprise's attention during the CIP version 5 transition period. The guidance documents are intended to provide stakeholders an understanding of effective approaches for implementing various CIP version 5 requirements and they are designed to highlight ways in which entities may implement the CIP version 5 standards consistent with the language of those standards. Each of these guidance documents goes through a process of broad stakeholder review before the ERO finalizes the document.
- **Compliance and Enforcement Expectations**. Communicating to the Regional Entities and Responsible Entities the expectations for compliance and enforcement of the CIP Reliability Standards. In particular, communicating expectations related to: (1) how the ERO Enterprise will view compliance and enforcement during the transition period to ensure that entities have the flexibility to begin implementing CIP version 5 in a manner and time frame that best suits their needs; and (2) the ERO Enterprise's application of its risk-based approach to compliance and enforcement to the CIP version 5 standards.

- **Outreach and Communications**. Keeping stakeholders informed of developments related to the implementation of CIP version 5 and inviting stakeholder input throughout the transition period. Among other things, representatives of NERC staff, Regional Entity staff, implementation study participants, and other stakeholders have weekly conference calls to discuss issues related to CIP version 5 implementation, including the topics for and the status of guidance documents. This same group also meets in-person on a monthly basis. Among other things, as part of its outreach efforts NERC intends to provide sample CIP version 5 implementation reviews to as many Responsible Entities as possible during 2015. Additionally, throughout 2015, NERC has been and will continue conducting a series of in-person workshops to provide entities focused input and guidance on CIP version 5 implementation issues.
- **Training**. To provide timely training to Regional Entities and industry on CIP version 5 implementation. NERC is holding a series of ERO Enterprise CIP auditor training workshops to help ensure a consistent, reasonable, and transparent approach to auditing the CIP version 5 standards under the revised Compliance Monitoring and Enforcement Program (CMEP).

Collectively, these elements are helping to ensure that each of the objectives of the transition program is satisfied and that entities can confidently transition to implementing the CIP version 5 standards upon their effective date.

Physical Security Standard

Similar to the work in supporting transition to CIP Version 5, NERC is prioritizing support for the industry's successful implementation of the Physical Security Reliability Standard, CIP-014-1. On November 20, 2014, FERC issued Order No. 802, approving Reliability Standard CIP-014-1 and directing NERC to remove the term "widespread" from Reliability Standard CIP-014-1 or, alternatively, to propose modifications to the Reliability Standard that address the Commission's concerns. Through its standards development process, NERC developed revisions to the Reliability Standard and subsequently filed those revisions with the Commission on May 15, 2015. The revised changes have little impact on the approach to supporting implementation activities of CIP-014-1. Implementation of the standard presents a number of considerations related to risk management and compliance expectations due to the flexibility provided in the standard. To that end, NERC is conducting several activities to support increased understanding of the various requirements in CIP-014-1 and to promote transparency and confidence in industry's implementation of the standard.

During the implementation period for CIP-014-1, with the support and engagement of industry stakeholders and the Regional Entities, NERC is issuing guidance documents, providing training to industry and ERO compliance and enforcement staff, and conducting other outreach efforts to improve industry's understanding of the requirements of CIP-014-1 and help ensure that industry is technically ready to implement the various requirements in the standard according to the time frame provided in the

implementation plan. These activities are also designed to ensure the ERO Enterprise enforces CIP-014-1 consistently, reasonably, and transparently.

The following outlines NERC's key activities for supporting effective and efficient implementation of CIP-014-1.

- **Guidance.** While CIP-014-1 contains a Guidelines and Technical Basis section to assist registered entities in implementing the requirements, NERC understands that the industry would benefit from additional guidance, especially related to the performance of the risk assessment to identify critical facilities. Accordingly, NERC has been collaborating with industry participants and Regional Entities to develop additional guidance on CIP-014-1. More specifically, NERC is developing a package of publicly available documents, the first of which was released on February 9, 2015, for the Regional Entities outlining the ERO's compliance and enforcement expectations for CIP-014-1. Additionally, NERC is collaborating with certain reliability-focused industry groups in developing guidance for successful implementation of specific requirements in CIP-014-1, some of whom are already developing guidance for their members.
- **Monitor and Assess Implementation.** NERC management, per the NERC Board of Trustee's instruction, will monitor and assess implementation of CIP-014-1. Specifically, NERC management intends to monitor the general number and characteristics of assets identified as critical and the scope of security plans developed to meet the requirements in CIP-014-1, including the timelines provided for implementation of the various security and resiliency measures included in the plan. Following the effective date of CIP-014-1, NERC intends to report quarterly to the Board in response to the Board's request.
- **Outreach and Communications.** During the implementation period, NERC is providing regular communications and outreach on key information to support industry's implementation of the standard. NERC presented a webinar to industry on December 18, 2014, where it provided information related to implementation support as discussed in these materials. NERC will conduct additional webinars, workshops, or technical conferences going forward based on feedback from industry and in conjunction with Regional Entity outreach activities.
- **Training**. Throughout 2015, NERC will provide training to Regional Entity staff to support consistency of approach in compliance monitoring and enforcement expectations around CIP-014-1. Initial coordination to ensure auditor training and consistent application of CIP-014-1 began in Atlanta, Georgia, during the week of September 15, 2014. Additional training and coordination continues as part of NERC's regular CIP compliance monitoring and enforcement staff training to help ensure a consistent, reasonable, and transparent approach to monitoring CIP-014-1 under the risk-based Compliance Monitoring and Enforcement Program.

Collectively, these elements will help ensure a more common understanding of implementation expectations for CIP-014-1 throughout 2015.

Conclusion

I appreciate the Commission's focus on these key issues. NERC takes seriously its efforts on enhancing security and appreciates the Commission's focus on our standards, their implementation and compliance as well as our information sharing efforts