

FERC Reliability Technical Conference

Panel IV: ERO Performance

Remarks of Steven Noess

Associate Director of Standards Development

North American Electric Reliability Corporation

June 10, 2014

Introduction

Acting Chairman LaFleur, Commissioners, staff, and fellow panelists. My name is Steven Noess, and I am the Associate Director of Standards Development at the North American Electric Reliability Corporation (NERC). My remarks today are centered on Electric Reliability Organization (ERO) performance, specifically as it relates to NERC's standards development activities and NERC's focus on physical security.

NERC Standards Development Process

NERC's standards development process depends upon the participation and input from stakeholders, and they have repeatedly demonstrated commitment to reliability and security through their consistent engagement and dedication toward improvement. Through collaboration among NERC staff, the NERC Standards Committee, and direct and observer participation on standard drafting teams, NERC has made significant progress in achieving the desired end-state of a comprehensive set of technically sound, results-based standards that collectively ensure the reliable operation of the North American bulk power system (BPS).

Efficiencies Gained from Recent Revisions to the Standards Development Process

NERC's standards development process is defined in the Standard Processes Manual (SPM), Appendix 3A to the NERC Rules of Procedure.¹ The SPM governs all activities of NERC related to the development, approval, revision, reaffirmation, and withdrawal of Reliability Standards, Interpretations, Violation Risk Factors (VRFs), Violation Severity Levels (VSLs), definitions, variances, and reference documents developed to support standards, and it also addresses the respective roles of the Standard Committee, drafting teams, and ballot body members in the stakeholder process. Upon FERC's approval of revisions to the SPM in June 2013, NERC, the Standard Committee, and stakeholders began implementing the approved changes, as well as additional changes that could be implemented within the construct of the SPM, into the standards development process.

The revisions to the SPM were initiated in February 2012, when the NERC Board of Trustees, in consultation with the NERC Members Representative Committee (MRC), formed the Standard Process Input Group (SPIG). The SPIG was composed of the MRC chair and vice chair, other MRC members, two members of the NERC Board, the NERC CEO, and the NERC Standard Committee chair. The NERC Board tasked the SPIG with developing process improvements in four key areas: 1) provide clarity on the reliability objectives, technical parameters, scope and relative priority of

¹ The SPM is available at: http://www.nerc.com/pa/Stand/Documents/Appendix_3A_StandardsProcessesManual.pdf.

Reliability Standards; 2) review the drafting process to ensure that Reliability Standards contain specific technical content; 3) assess Reliability Standards project management and workflow; and 4) evaluate formal balloting and commenting.

The SPIG gathered input from stakeholders and made five recommendations² to modify the way NERC develops Reliability Standards. Based on these recommendations, NERC worked with stakeholders to develop revisions to the SPM. In these revisions, NERC:

- Memorialized the intent to revise drafting team compositions to ensure they are appropriately equipped to meet reliability objectives (*e.g.*, add legal and compliance experts)
- Incorporated reference to compliance assessment tool development, such as Reliability Standards Audit Worksheets (RSAWs), cooperatively and in parallel with standard drafting
- Streamlined commenting and balloting, including provisions for:
 - Summary responses to comments and elimination of the obligation to respond in writing at every stage of the comment process;
 - Eliminating negative votes without comments in the calculation of consensus.
- Allowed quality review in parallel with standards development
- Incorporated guidance for the appropriate role and scope of Interpretations, to be consistent with guidance from the NERC Board
- Reduced the requirement for periodic reviews to be consistent with ANSI minimum requirements
- Incorporated a waiver provision to allow for modifications to the standards development process for good cause, with five days' notice and reporting of the exercise of a waiver to the Board's Standards Oversight and Technology Committee

These improvements provide a balanced flexibility to the process that enables NERC and the industry to address pressing reliability issues on accelerated timeframes if necessary. The Commission approved the proposed revisions on June 26, 2013, agreeing that these changes allow for greater flexibility and efficiency.³

In addition to the revisions provided in the SPM, NERC implemented additional enhancements into the standards development process. In conjunction with implementing the changes to the SPM, in 2013, NERC spearheaded an "informal development effort," which used informal groups composed of industry subject matter experts to conduct early outreach to industry stakeholders prior to initiating formal standards development. Such early outreach encouraged stakeholder conversations to obtain inputs on the proposed standard development project. This approach has since transitioned into the fabric of formal development itself, and increased outreach throughout the standards development process is positively affecting how standard drafting teams are conducting their work.

² The SPIG's *Recommendations to Improve the NERC Standards Development Process* report is available on the NERC website at: http://www.nerc.com/pa/Stand/Standards%20Processes%20Manual%20revisions%20SPIG%20Recommen/Standards_Process_Input_Group_04.24.12_ver_8_FINAL.pdf.

³ *Order Approving Revisions to Electric Reliability Organization's Standard Processes Manual*, 143 FERC ¶ 61,273 (2013), at P 18.

The periodic reviews conducted through 2013 followed this same approach, acting as a tool for gathering stakeholder input. Recommendations from each periodic review team are implemented through subsequently-formed standard drafting teams.

Projects that were initiated and completed after FERC's approval of the SPM changes have shown significant increases in efficiency while simultaneously improving quality. Implementing the revisions within other projects that were already in process has also resulted in the same improvements.

The most significant improvement is the composite result of all the revisions – the amount of time required to develop a quality standard. As reported in the Analysis of NERC Standards Process Results, Fourth Quarter 2013 filing⁴, the baseline for the time to revise an existing standard was approximately 27 months and 40 months to develop a new standard. In contrast, the times to produce each of eight standards development projects that began formal development after implementing the revised SPM⁵ were dramatically reduced. In example, 6.5 projects -- Geomagnetic Disturbance Mitigation Phase I, Coordinate Interchange Standards (INT), Physical Security, MOD A, MOD B, PER, and one of the two standards in the VAR project (VAR-001) -- completed formal development from posting the SAR to being adopted by the NERC Board in less than seven months, and in the case of the physical security project, less than three months. The remaining standard in the VAR project (VAR-002) and the MOD C project completed formal development in ten months.

The reduction in time to develop a standard provides registered entities increased flexibility in staffing standard drafting teams due to the reduced time commitment and, with meetings held closer together in time, the standard drafting team members are able to stay focused on the standard.

This composite result is dependent upon the other revisions:

- Smaller standard drafting teams provided with the appropriate expertise have increased the ability to conduct activities and respond to stakeholders in a more-timely manner.
- Open communication and concurrent development of compliance assessment tools have addressed compliance questions and allowed for clarification of compliance intentions during standards development.
- Allowing for summary responses to comments has allowed the standard drafting teams to consider stakeholder inputs, modify the standard in response to those inputs, and repost for industry review more quickly (as short as 1.5 weeks). Summary responses are more concise while still addressing the issues, and the summaries provide visibility into the concerns in an easily digestible format.

⁴http://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/Analysis_of_NERC_Standards_Process_Results_Q4_FINAL.pdf

⁵ The eight projects were: Project 2010-01 – Training (PER), Project 2010-03 – Modeling Data (MOD B), Project 2010-04 – Demand Data (MOD C), Project 2012-05 – ATC Revisions (MOD A), 2013-03 – Geomagnetic Disturbance Mitigation, Coordinate Interchange Standards Project, Project 2013-04 – Voltage and Reactive Control (VAR), and Project 2014-04 – Physical Security.

Panel IV

Remarks of Steven Noess, Associate Director of Standards Development

North American Electric Reliability Corporation

FERC Reliability Technical Conference

June 10, 2014

- Not considering negative votes without comments in the calculation of consensus encourages entities to provide constructive comments, providing insight into the issues for the standard drafting team.
- Coordinating quality review in parallel with standard development eliminated an additional process (that previously could require 4-6 weeks) from the process and improves focus on quality at an earlier stage.
- Granting the Standards Committee the authority to waive provisions in the SPM for good cause provides the Standards Committee the ability to respond to urgent reliability issues. A recent example, discussed later in these remarks, is the physical security standard.

Another improvement resulting from the SPM revisions, which is also associated with increased outreach and communication, is the partnership created between NERC staff, standards drafting teams, and the Standards Committee. Additionally, FERC staff has been providing early input regarding their perspectives during the development process, providing standards drafting teams the opportunity to weigh those inputs early in the process. While the results are preliminary we anticipate this open dialogue will result in FERC orders with either no directives or a significantly reduced number of directives.

The Standards Committee has also created a new subcommittee, the Process Management and Oversight Subcommittee (PMOS) that acts as an industry and standards drafting team partner. This subcommittee assigns a representative to each standards drafting teams for the purpose of oversight. This oversight includes such actions as assisting the standards drafting teams in understanding any stakeholder concerns, reaching out to stakeholders if they do not understand the actions being taken by the standards drafting team, being partners in reviewing the standards for quality, and assisting with advice on a range of topics from direction to posting schedules. This group has assisted standards drafting teams in avoiding or overcoming hurdles during the process.

The revisions made to the SPM and other changes made to the standards development process, while still in their infancy, are showing great promise as improvements to the process, both in creating efficiency and improving quality. These improvements have allowed the ERO to make significant progress towards achieving a body of steady-state standards. The 2015-2107 Reliability Standards Development Plan will reflect that most, if not all, FERC directives and recommendations for retirement (both from the Paragraph 81 project⁶ and the Independent Experts Review Panel (IERP)⁷ will be addressed in 2015, and it will provide an opportunity for a strategic review of the reliability standards.

⁶ The March 15, 2012, FERC Order Accepting with Conditions the Electric Reliability Organization's Petition Requesting Approval of New Enforcement Mechanisms and Requiring Compliance Filing, *North American Electric Reliability Corporation*, 138 FERC ¶ 61,193 at P 81 provided the opportunity for the ERO to evaluate requirements, which resulted in the Paragraph 81 project. The Paragraph 81 criteria are in the Phase I Technical Paper on the NERC website at: http://www.nerc.com/pa/Stand/Pages/Project2013-02_Paragraph_81.aspx.
⁷http://www.nerc.com/pa/Stand/Standards%20Development%20Plan%20Library/Standards_Independent_Experts_Review_Project_Report.pdf.

Reliability Issues Steering Committee (RISC) and the Standards Development Process

The RISC is an advisory committee that reports directly to the NERC Board and triages and provides front-end, high-level leadership and accountability for issues of strategic importance to BPS reliability. The RISC assists the Board, NERC standing committees, NERC staff, regulators, Regional Entities, and stakeholders in establishing a common understanding of the scope, priority, and goals for the development of solutions to address these issues. In doing so, the RISC provides a framework for steering, developing, formalizing, and organizing recommendations to help NERC and the industry effectively focus their resources on the critical means to improve the reliability of the BPS. In some cases, that includes recommending reliability solutions other than the development of new or revised standards and offering high-level stakeholder leadership engagement and input on issues that enter the standards process. In other cases, the development of a new reliability standard or modification of an existing reliability standard may be the best way to address a particular issue.

The Standards Committee works closely with the RISC and the NERC technical committees, creating an alignment of focus on specific issues. The chair of the Standards Committee is a member of the RISC, which strengthens the relationship.

Additionally, RISC is developing a triage process to address other reliability issues that are brought to the Standards Committee, whether through a Standards Authorization Request (SAR) or another mechanism. This process will include a review by the RISC to determine whether the issue is a risk to the reliability of the BPS and, if so, the priority of investing ERO and stakeholder resources to resolve the issue. This aids in focusing resources on the resolution of appropriate issues.

Finally, as discussed immediately below, RISC also improves the standards development process by providing key insight into the prioritization process for standards development projects.

Prioritizing Standards Development Projects

In support of NERC's effort to facilitate transformation of NERC Reliability Standards to a stable set of clear, concise, high-quality, and technically sound Reliability Standards that are results-based, NERC works collaboratively with the Standards Committee and stakeholders to prepare an RSDP each year. The RSDP provides a three-year plan for standards development, and this year's 2014-2016 RSDP included prioritization criteria to assist in assigning appropriate priority to each active standards development project.

The prioritization included consideration of several specific elements, including: (1) RISC Category Rankings; (2) regulatory directives; (3) regulatory deadlines; (4) Reliability Standard requirement candidates for retirement; (5) the IERP content and quality assessments; and (6) additional considerations (fill-in-the-blank status and five-year assessment commitments). Giving primary consideration to the first three elements, NERC staff and PMOS collaborated to apply the elements to prioritize each Reliability Standard project as high, medium, low, or pending technical committee input. The same prioritization is applied to projects that have become active since completion of the RSDP.

The RISC provides input into prioritizing standards development activities by providing input to RSDP in two ways: first, by considering whether the projects identified in the plan addressed areas of risk for the BPS and second, by considering a priority rank for each of the projects. In considering whether each of the projects addressed an area of risk for the BPS, the RISC also considered whether there were outstanding FERC directives or any recommendations for retirement, either from the Paragraph 81 project or the IERP that could be addressed by the project. In reviewing the priority of each project, the RISC provided a mechanism for addressing any scheduling conflicts between projects through the development process.⁸Regulatory directives and deadlines also provide a significant input to prioritizing standards development projects for obvious reasons.

The ensuing prioritizations and other project details are then reflected on a dynamic project tracking spreadsheet⁹ to assist industry stakeholders assess approximate timing and resource allocations related to development activities. The project tracking spreadsheet provides a snapshot of projected project milestones, and it provides an executive summary-level picture of all standards development activity for the year. Since the prioritization in the 2014-2016 RSDP, prioritizations have not deviated. Furthermore, projects that began after completion of the 2014-2016 RSDP (in response to regulatory directives issued subsequent to RSDP completion, for example) have been prioritized using the same criteria.

Security Issues

Reliability and security of the grid, from both a cybersecurity and physical security perspective, are key priorities for NERC and the industry. The industry has decades of experience working to protect our shared infrastructure, and it is constantly reevaluating threats and taking steps to protect the system.

Efforts to Enhance Physical Security of the Grid

Reliability Standards are one facet of NERC's tools to address the complex, dynamic endeavor of providing a comprehensive approach to reliability. NERC also has various other tools to fulfill this mission, including guidelines, training, assessments, and alerts, all of which promotes a secure and reliable BPS for North America.

After September 11, 2001, industry developed and updated physical security guidelines to address the need for coordination and communication. These security guidelines address physical security response, best practices, and substation security. Specifically, they provide guidance on:

- Addressing potential risks
- Identifying practices that can help mitigate the risks
- Determining risk for an organization and practices appropriate to manage its risk
- Identifying actions that industry should consider when responding to threat alerts received from the ES-ISAC and other organizations
- Defining the scope of actions each organization may implement for its specific response plan
- Conducting assessment of and categorizing vulnerability and risk to critical facilities and functions

⁸ RISC reviewed and provided input on the use of RISC's rankings in project prioritization.

⁹ http://www.nerc.com/pa/Stand/Project%20Tracking%20Spreadsheet/2014%20Project_Tracking_Spreadsheet.xlsx

In April of last year, NERC, industry, and our federal partners responded to a physical attack against a substation in California. Immediately after the event, the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) issued an alert to inform industry of the event and provide advice on steps to mitigate and protect against such attacks. In addition, the ES-ISAC, the Department of Energy, FERC, the Department of Homeland Security, and the FBI developed an outreach effort to raise awareness of the event, inform industry of mitigation activities, and provide a forum for industry to meet with state, local, and federal authorities to discuss physical security concerns for their regions. This was an unprecedented public-private partnership effort to address physical security concerns and involved U.S. and Canadian interests.

Physical Security Standard

Most recently, NERC developed a physical security standard (CIP-014-1), which FERC ordered on March 7, 2014, with a filing deadline of June 5, 2014. Through our industry process, NERC completed the standard and filed it to FERC for approval on May 23, 2014. This standard will address physical security threats and vulnerabilities for the most critical facilities and will focus on risk management activities and foundational physical security practices.

In the order, FERC stated that the proposed Reliability Standard(s) should require entities to take at least the following three steps:

- Perform a risk assessment to identify facilities that, if rendered inoperable or damaged, could result in instability, uncontrolled separation, or cascading failures on the BPS.
- Evaluate the potential threats and vulnerabilities to those identified facilities.
- Develop and implement a security plan designed to protect against physical attacks to those identified facilities based on the assessment of the potential threats and vulnerabilities to their physical security.

Additionally, FERC directed that the proposed standard(s) should also: (1) include a procedure that will ensure confidential treatment of sensitive or confidential information; (2) include a procedure for a third party to verify the list of identified facilities and allow the verifying entity, as well as FERC, to add or remove facilities from the list of critical facilities; (3) include a procedure for a third party to review the evaluation of threats and vulnerabilities and the security plan; and (4) require that the identification of the facilities, the assessment of the potential risks and vulnerabilities, and the security plans be periodically reevaluated and revised to ensure their continued effectiveness.

The Physical Security Standard Drafting Team developed the proposed physical security Reliability Standard, CIP-014-1, through the standards development process. CIP-014-1 requires entities to identify critical facilities as defined in the order, to evaluate the threats and vulnerabilities to those facilities, and to implement security measures to prevent or mitigate against physical attacks to those identified facilities. The revised SPM, which I discussed earlier, provided necessary mechanisms to enable the industry to efficiently complete the standard within the required timeframe. To facilitate the 90-day timeline, the Standards Committee approved waivers to the SPM to shorten certain posting periods related to the standard's development. The Standards Authorization Request was posted, under a Standards Committee-approved waiver, for a seven-day informal comment period from March 21-28, 2014. A NERC-led industry technical conference on April 1, 2014, provided industry input regarding applicability, identification of critical facilities, evaluation of threats and vulnerabilities, development and implementation of physical security plans, and a proposed implementation plan for the standard.

The standard was posted under a Standards Committee-approved waiver for a 15-day concurrent comment and initial ballot period from April 10-24, 2014. The initial ballot results indicated a quorum of 88.60 percent and an industry approval of 82.07 percent. The final ballot was posted, under a Standards Committee -approved waiver, for a five-day period from May 1-5, 2014. The final results indicated a quorum of 92.53 percent and an industry approval of 85.61 percent. The NERC Board of Trustees adopted the standard on May 13, 2014, and it was filed to FERC by NERC on May 23, 2014.

The proposed physical security standard enhances physical security measures for the most critical facilities and lessens the overall vulnerability of the BPS. As the industry implements CIP-014-1, NERC is committed to continuing its long-standing dedication to enhancing physical security, and NERC will continue to monitor and assess implementation on an ongoing basis to confirm progress in securing the most critical facilities on the North American BPS.

Partnerships

NERC also works closely with stakeholders and our government partners on security matters on a regular basis through both formal and informal structures. NERC works closely with the Electricity Sub-sector Coordinating Council (ESCC), which coordinates policy-related activities and initiatives to improve the reliability and resilience of the BPS. Gerry Cauley, NERC's President and CEO, is a member of the ESCC. The roles of the ESCC are to represent the electricity sector, to build relationships with government and other critical infrastructure sectors, and to participate in joint initiatives as part of the "partnership framework" envisioned by the National Infrastructure Protection Plan and Energy Sector-Specific Plan. This past year, the ESCC underwent changes to broaden membership to 30 CEO-level representatives, formally recognizing the significant increased CEO interest and participation on cybersecurity issues. The ESCC's focus to address physical security and cybersecurity issues, working alongside our government partners, remains unchanged.

NERC also continues to provide leadership to significant DHS-affiliated public-private partnerships. These groups are the Cross-Sector Cyber Security Working Group, which was established to coordinate cross-sector initiatives that promote public and private efforts to help ensure secure, safe, and reliable critical infrastructure services; and the Industrial Control Systems Joint Working Group, which is a cross-sector industrial control systems working group that focuses on the areas of education, cross-sector strategic roadmap development, and coordinated efforts to develop better vendor focus on security needs for industrial control systems.

NERC's Critical Infrastructure Protection Committee (CIPC) focuses on both physical security and cybersecurity issues impacting the BPS. The committee consists of both NERC-appointed regional representatives and technical subject matter experts. CIPC coordinates NERC's security initiatives and serves as an expert advisory panel to the NERC Board, standing committees in the areas of physical security and cybersecurity, and the ES-ISAC. To address issues related to cybersecurity and physical security, CIPC establishes working groups or task forces comprised of subject matter experts who review and examine specific issues and develop reports and recommendations. CIPC also coordinates with government individuals and entities to hold joint briefings and participate in other activities to address security policy matters. NERC also collaborates with the Industrial Control Systems Cyber Emergency Response Team to share threat, vulnerability, and security incident information.

In 2012, CIPC reorganized and expanded to allow it to produce more deliverables. This reorganization established new subcommittees and created new task forces and working groups to address emerging issues and initiative requests from the NERC CEO and Board. The reorganization included forming task forces to address cybersecurity-related subjects identified in the 2010 *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System* report. One CIPC task force, the Cyber Attack Task Force (CATF), considered the impact of a coordinated cyber-attack on the BPS and developed flexible options for detecting, operating, and recovering from such an attack. A key component of the resulting CATF report was the development and use of an attack tree tool that provides key insight into the attack surface of the interconnected BPS of North America.

Following NERC Board approval of the CATF report, CIPC established a HILF Implementation Task Force to review the recommendations in this and other related reports, and to determine which recommendations CIPC should address. The HILF Implementation Task Force determined that CIPC should continue its analysis of cyber attack trees and analyze issues relating to information sharing, security clearances, security metrics, and physical security guidelines. CIPC established task forces for all of these issue areas, and most groups have completed their reviews and issued recommendations.

Conducting Outreach, Training, and Education Activities

In addition to collaborating with industry and government partners, NERC regularly conducts outreach to and training for our partners. We do so through assessments, exercises, webinars, and guidelines.

GridEx II

In 2011, NERC facilitated the first-ever GridEx for the electricity sector in North America. NERC now holds a biennial distributed play exercise and executive tabletop discussion to:

- Exercise the current readiness of the electricity industry to respond to a security incident, incorporating lessons learned
- Review existing command, control, and communication plans and tools for NERC and its stakeholders
- Identify potential improvements in cybersecurity and physical security plans, programs, and responder skills
- Explore senior leadership policy decisions and triggers in response to a coordinated cyber and physical event of national significance with long-term grid reliability issues

NERC held GridEx II on November 13-14, 2013, where more than 230 organizations participated in the distributed play session. Additionally, a group of senior industry and government executives participated in a tabletop session based on the distributed play scenario but greatly expanded in scope. The exercise built upon the objectives and findings from the 2011 GridEx recommendations and simulated a coordinated cyber and physical security attack to offer participants a worst-case scenario to review their existing command control and communication plans and to identify potential areas for improvement. The exercise was the most comprehensive effort to date that addressed both cyber and physical security. NERC released reports in March 2014 detailing lessons learned and recommendations. These reports are posted on NERC's website.

Cyber Risk Preparedness Assessments (CRPA)

The ES-ISAC developed the CRPA program to assess, through exercises, an entity's current cybersecurity capabilities and the adequacy of existing reliability mechanisms. By conducting these assessments, the ES-ISAC targets areas for improvement and identifies best practices that it can then share with industry. Since 2010, over a dozen entities have participated in the CRPA program and have responded positively to the impact the CRPAs have on strengthening their operations, and ultimately helping to protect the BPS.

The CRPA program continued to mature in 2013 with the addition of the ES-C2M2 key practice areas informing and complementing the CRPA program. The program used the ES-C2M2 to shape the analysis of the exercise and focus the post-exercise discussion and report around the response capabilities as defined through the ES-C2M2. As part of the ES-ISAC's strategy to support adoption of the CRPA methodology more broadly across the industry, the ES-ISAC hosted a workshop in 2013 to provide training and templates for industry to use in support of their own exercise programs. The CRPA also supported the GridEx II exercise, providing documentation and training to exercise participants on using the ES-C2M2 in assessing their organization's response capabilities.

Security Readiness Program (SRP)

NERC conducts SRPs, which consists of visits to registered entities to focus on the sufficiency of industry implementation of the CIP Standards. An SRP visit both examines CIP Version 3 compliance in a retrospective review and helps registered entities address transitioning from CIP Version 3 and CIP Version 5 in a prospective view. While compliance with CIP Version 3 and its risk-based assessment methodology remains mandatory until March 31, 2016, many registered entities are concerned about how to transition their compliance and security efforts to Version 5 to meet the April 1, 2016, compliance deadline. Registered entities are exploring how to best manage the transition process to CIP Version 5 while remaining compliant with CIP Version 3. NERC invites Regional Entity representatives to participate in SRP discussions; however, no content from those discussions may be used during a subsequent audit or compliance action unless that content reveals an imminent threat to the BES. NERC staff, Regional Entity representatives, and outside consultants sign non-disclosure agreements to ensure strict confidentiality of all discussions and materials.

Security Briefings and Guidelines

Another example of NERC's outreach and training efforts included a classified briefing campaign in 2013. The ES-ISAC, DHS, DOE, and FBI collaborated to host a series of briefings focused on tactics and tools of emerging cyber threat actors. Similar to the 2014 physical security outreach campaign, this campaign included a multi-city tour across the United States and was developed following a NERC alert that detailed how attackers use common tools to infiltrate critical infrastructure networks and gain access to control system networks. The briefings were designed to raise awareness within the control systems community to better protect the BPS.

In addition, NERC's CIPC holds security briefings and workshops throughout the year to educate industry about items, such as physical security assessments and penetration testing. CIPC also developed physical security guidelines for the electricity sector to assist entities in responding to a physical security situation. The guidelines also include a reference document that any entity can adapt to its specific physical security policies and procedures.

Panel IV

Remarks of Steven Noess, Associate Director of Standards Development

North American Electric Reliability Corporation

FERC Reliability Technical Conference

June 10, 2014

Grid Security Conference (GridSecCon)

Finally, NERC hosts its annual GridSecCon, which brings together cybersecurity and physical security experts from industry and government to share emerging security trends, policy advancements, and lessons learned related to the electricity sector. GridSecCon 2013 included discussions focused on industry being transformational, strategic, and tactical in its approach to securing systems. Specifically, participants were asked to consider different information sharing techniques; determine if their organizations are resilient through self-assessments; test response activities through exercises; work to ensure that security is built into operations; and enhance the workforce by recruiting, training, and retaining individuals who can address these and other issues. Additionally, almost 200 stakeholders attended credentialed training sessions in cyber and physical security.

Critical Infrastructure Protection Reliability Standards—Version 5 Implementation

Version 5 of NERC's Critical Infrastructure Protection (CIP) Reliability Standards represent significant improvement and change over previous versions of the CIP standards. Development of CIP Version 5 was informed by implementation experience with previous versions, and they tailor security requirements to risks to the BPS.

NERC is committed to working with industry to ensure smooth transition toward Version 5, and NERC has been collaborating with Regional Entities and responsible entities by establishing a transition program to support implementation of Version 5 in a manner that is timely, effective, and efficient. The transition program has the following goals:

- Goal 1 - Improve industry's understanding of the technical security challenges that need to be addressed to comply with the CIP Version 5 standards. This includes working closely with industry to confirm understanding of new or different components of Version 5 compared to Version 3.
- Goal 2 - Provide industry with a clear path and approach to transition from Version 3 to Version 5 that includes expectations for compliance and enforcement.
- Goal 3 - Understand the effort and required resources needed for the transition.

To achieve the goals, NERC has implemented several program elements related to outreach, communication, and training, to include periodic guidance documents to keep industry informed during the transition period. NERC believes that the topics identified during the transition should be closely examined and the risks understood so that registered entities across North America can recognize and apply appropriate security measures and mitigation actions.

Another key component of the transition program is a Version 5 implementation study, which includes six volunteer entities that agreed to work with NERC and the Regional Entities to implement the CIP Version 5 standards on an accelerated basis. Participants were selected because of their history of successful CIP Version 3 compliance, effective management practices, and willingness to commit the resources required to support transition. The study has been focusing on technical solutions and processes necessary to meet the requirements of the CIP Version 5 standards.

In addition, study participants are working to identify any issues or challenges to implementation, along with recommending potential solutions, especially related to the three goals of the transition program described earlier. The main effort of the implementation study is scheduled to end on June 30, 2014, though certain aspects will continue through to the effective date of CIP Version 5. NERC and the Regional Entities will use the information from collaborating with study participants to prepare a report containing key conclusions, lessons learned, and recommendations in support of transition to Version 5.

NERC will also continue working with the Commission's staff and other industry stakeholders to collectively evaluate and identify means to resolve any issues that may emerge during transition. Some of the topics identified during transition are as follows, and NERC is working with Regional Entities and stakeholders to evaluate them:

- **Substation BES Cyber Assets** – CIP Version 5 introduced many critical communication network components such as SCADA to RTU communication, connectivity to relays, and other intelligent electronic devices that reside inside of substations. Many of these systems and networks were not covered in Version 3 because non-routable connections were not clearly in scope. Version 5 requires both routable or IP connections in addition to serial, non-routable connectivity.
- **Programmable vs Non-programmable** – The study participants are helping to evaluate and provide guidance to help industry better understand what distinguishes certain systems and networks as programmable versus non-programmable, which informs applicability of the CIP Version 5 standards. The question of what constitutes a programmable device impacts both BES cyber assets and the networks that protect them. NERC and study participants will be working closely to develop additional clarifications.
- **Virtual Servers and Virtual Local Area Networks** – These are not terms explicitly covered in CIP Version 5; however, the industry's use of such dynamic technologies is increasing. As a result, we will work with stakeholders to monitor such technologies' impact on CIP Version 5 implementation and evaluate whether additional guidance is necessary.
- **Protecting Data in Motion** – In support of NERC's continuing work on communications security, NERC will engage the industry to evaluate the performance impact of deployed encryption, PKI-based authentication, or VPN security to determine their impacts on network and operational performance.

Conclusion

Through both Reliability Standards and other ERO tools, including a significant focus on security issues, NERC and the electric industry share FERC's commitment to ensuring the reliable operation of the North American BPS. Thank you for the opportunity to share NERC's perspectives on this important set of topics.