



STACY DOCHODA – FRCC

ED SCHWERDT – NPCC

SCOTT HENRY – SERC

LANE LANFORD – TRE

DAN SKAAR – MRO

TIM GALLAGHER – RFC

RON CIESIEL – SPP

CONSTANCE WHITE – WECC

Federal Energy Regulatory Commission
Reliability Technical Conference
Docket No. AD14-9-000
June 10, 2014

Panel 4: ERO Performance

Remarks of Timothy R. Gallagher
President and CEO of ReliabilityFirst Corporation

On behalf of the Regional Entity Management Group (REMG), I want to thank the Federal Energy Regulatory Commission (Commission) and its Staff for the opportunity to participate on this panel. I am Timothy R. Gallagher, President and Chief Executive Officer of ReliabilityFirst Corporation. During the last technical conference, there was some discussion about opportunities for and improvements to the consistency and coordination of CMEP activities across all the Regional Entities (Regions). Since that conference, the Regions have made and continue to make substantial strides to promote a uniform and consistent application of these activities and to coordinate policy positions on significant matters. My comments reflect this consistency and coordination, because the views I express today are the consensus views of the entire Regional Executive Management Group.

During my participation on this panel, my comments will focus on the Regional perspective on four key topics regarding the efforts and performance of NERC and the Regions:

- Observed efficiencies in NERC's Standards Development Process;
- The positive impacts of the Reliability Issues Steering Committee (RISC);
- Trends in compliance and enforcement of Reliability Standards (Standard); and



- Potential implementation issues regarding the CIP Version 5 Standards and ongoing efforts to ensure the consistent enforcement of these Standards across the BES.

A. Observed Efficiencies in NERC’s Standards Development Process

There have been significant improvements in the efficiency of the Standards Development Process, as well as substantive improvements in the content of the Standards. This is the direct result of hard work and commitment from NERC, the Regions, and industry; clear guidance from FERC; effective leadership from the NERC Standards Committee; and guidance from the NERC Reliability Issues Steering Committee (RISC), which identifies emerging risks to the BES and utilizes those identified risks to help inform the prioritization of Standards development.

The recent development of the Physical Security Standard, CIP-014-1, provides a great example of the significant improvements that have occurred within the Standards development process. As you are aware, in early March, the Commission issued an Order under Docket No. RD14-6-000 (Physical Security Order) directing NERC to draft, within 90 days, a Reliability Standard to require Registered Entities to take steps to address physical security risks and vulnerabilities.¹ It is important to stress that the Standards Development Process was not created for speed, but rather, for deliberation and consensus-building among technical experts across the industry. Nevertheless and impressively, the Standards Development Process developed CIP-014-1 in approximately two months, which addresses all of the identified concerns in the Physical Security

¹ The development of the Physical Security Standard, CIP-014-1, also addresses the Commission’s inquiry into what efforts are being taken by NERC and the Regions to address physical security. This proposed Physical Security Standard will require Registered Entities to (1) conduct periodic risk assessments to identify facilities that are critical to the reliable operation of the BES; (2) evaluate potential threats and vulnerabilities facing those facilities; and (3) develop, validate, and implement a physical security plan or plans to protect against physical attacks on those facilities.



Order. I believe that this Standard, as well as other recently filed Standards, is emblematic of the improved quality and significant efficiency gains made in the Standards Development Process.

The next challenge facing the Standards Development Process is to shift the focus from a compliance-based mindset to a risk-based mindset. I worry that the ERO Enterprise's past zero-tolerance approach to monitoring and enforcement may have inadvertently added a focus on managing compliance risk into the development of Standards. As such, I urge the Commission to continue to be supportive of the ongoing Reliability Assurance Initiative (RAI) efforts because it eliminates the zero-tolerance mindset and focuses compliance and enforcement activities around legitimate risks. Additionally, the RAI is formalizing a standards feedback loop to leverage the Regions' real time experience with the monitoring and enforcement of Reliability Standards. This will provide improved structure to retain data and inform the Standards development process of gaps in the Standards, instances where Standards provide limited value, and potential alternatives to drafting or retiring Standards.

Abandoning the zero tolerance mindset, in conjunction with a formalized standards feedback loop, will better focus and ensure the development of Standards that address critical risks to reliability and resiliency. The timing is critical, given the rapidly changing nature of our industry and the constantly evolving risks to the BES.

B. The Positive Impact of the RISC

The RISC, an advisory committee that reports to the NERC Board of Trustees, uses ERO-wide reliability and resiliency data and analytics to prioritize the most critical risks facing the BES. The RISC then strategically focuses the activities of NERC, the Regions, and the industry around these high-priority risks. Presently, RISC's most notable impact is the guidance it provides on the



development of Standards. I am hopeful that the RISC will continue to play a major role in the continuing evolution of the RAI.

It is only logical that the RISC's ongoing identification of high-priority risks should help focus the Regions' monitoring and enforcement activities. For example, the RISC identified workforce capability and human error as a high-priority risk to the BES; and then identified Standards related to this risk (*e.g.*, the PER Standards - Personnel Performance, Training, and Qualifications). In turn, the Regions should allow this identified risk to inform their respective compliance monitoring and enforcement activities, and serve as an input to the scope and the frequency of their audits. This agile approach seems much preferable to developing an Actively Monitored List and auditing the Standards on a set, mechanical schedule.

C. Trends in Compliance and Enforcement of Reliability Standard Requirements

Over the past two years, the Regions have seen approximately twice as many violations of the Cyber Security Standards than of the Operations & Planning Standards.² I believe this is largely rooted in the fact that the CIP standards are relatively new and have undergone numerous revisions. Throughout this time of change, I have seen the industry's sincere commitment to both understanding and effectively implementing the CIP standards. In fact, the Regions' respective staffs have shared with each other numerous experiences where Registered Entities with significant issues in the CIP area have responded by working with their respective Region and emerging as industry leaders in CIP compliance.

² The list of the top ten most violated Reliability Standards has also remained steady over the past two years, with CIP-007 being the most violated Standard, followed by CIP-006, CIP-005, PRC-005, CIP-004, CIP-002, CIP-003, VAR-002, CIP-009, and FAC-008.



As to the general trends in the compliance monitoring and enforcement areas, I would like to note the following. First, in the compliance monitoring area, we are actively moving away from scripted audits and towards truly risk-based audits. The Regions continue to better leverage the significant amounts of data and analytics they have developed over the years to identify risks to reliability and resiliency, and to focus audits and other compliance monitoring activities around these risks.

In the enforcement area, self-reporting continues to be strong across all the Regions. NERC and the Regions, in conjunction with industry, recently developed a self-reporting guide that focuses on improving and streamlining the content of self-reports. Additionally, the Regions have begun to exercise and test enhanced enforcement discretion in various RAI pilots commissioned and overseen by NERC. Examples of this enhanced enforcement discretion include allowing Registered Entities with strong internal controls to self-log violations of certain Standards (subject to spot checks); and case-by-case enforcement discretion for lesser risk matters.

In the mitigation area, the Regions are actively encouraging Registered Entities to focus their mitigation activities on comprehensive corrective actions to improve the management practices and internal controls implicated in the root cause of a violation. I encourage NERC and the Commission to support this proactive and capability-focused approach to mitigation, as it better ensures the long-term reliability and resiliency of the BES. To the industry's credit, most Registered Entities voluntarily choose to implement systemic, reliability-focused initiatives in their mitigation plans. I applaud and encourage these efforts, but note to NERC and the Commission that the coordination and review of these comprehensive mitigation activities requires additional Regional resources.



D. Issues Discovered During the Initial Effort to Implement the CIP Version 5 Standards

As an initial point, I want to commend the Commission's direction to remove the "identify, assess, and correct" language from the CIP Version 5 Standards. The Regions do not support the codification of discretion into these or any other Standards because it renders compliance obligations vague and ambiguous for the industry to follow, and for the Regions to monitor and enforce. Worse yet, the codification of discretion in the Standards may also impair the Regions' ability to apply discretion in the RAI because codified discretion language in some Standards implies that there is no ability to exercise discretion where it is not codified. Simply put, the exercise of discretion is a tool for informed decision-making to utilize in the compliance monitoring and enforcement space. It must be based on the facts and circumstances at issue, and as such, should not be written in a vacuum and codified into the Standards.

The initial implementation efforts for the CIP Version 5 Standards are progressing well thus far. The CIP Version 5 Implementation Study (Implementation Study), in which six entities implement the CIP Version 5 Standards in an accelerated timeframe, resulted in valuable lessons learned that will be publicly posted with other guidance that will assist Registered Entities in their implementation efforts. The Regions will work with NERC to use these lessons learned to create a guidance document for each CIP Version 5 Standard.³

The Implementation Study resulted in the identification of three key potential implementation concerns with CIP-002-5. First, CIP-002-5 defines BES Cyber Assets as those Cyber Assets that, "if rendered unavailable, degraded, or misused, would adversely impact the reliable

³ However, I must note that implementation efforts for the CIP Version 5 Standards cannot truly begin in earnest until the Standards Drafting Team completes its drafting and balloting activities, the NERC Board of Trustees approves the CIP Version 5 Standards, and NERC files the CIP Version 5 Standards with the Commission at the end of 2014.



operation of the BES within 15 minutes of the activation or exercise of the compromise.” This new definition of BES Cyber Assets may bring more assets into the scope of the CIP Standards, and Registered Entities should be prepared to involve a larger group of subject matter experts in their CIP-002-5 identification and categorization efforts.

Second, CIP-002-5, Attachment 1, “Impact Rating Criteria,” Section 2.5 requires Registered Entities to declare transmission facilities at a single station or substation that meet certain line and voltage criteria as Medium assets. There is a concern that this criterion also brings into scope as a Medium asset any Facility attached at the far end of a transmission line connected to the station or substation at issue (such as a relay). Therefore, NERC or Commission guidance to clarify this criterion would be helpful.

Finally, CIP-002-5, Attachment 1, “Impact Rating Criteria” Section 2.1 requires the identification of shared BES Cyber Systems (for each group of generation units) that could, within 15 minutes, adversely impact the reliable operation of any combination of generation units that in aggregate equal or exceed 1500MW in a single Interconnection. In response to this requirement, Registered Entities are considering “disaggregating” generation units at generation stations to take generation stations out of scope. This issue merits discussion on whether this approach is “gaming the system;” or is in fact increasing reliability and resiliency by decreasing the number of generation units with a “common mode” impact.

E. Ongoing Efforts to Ensure the Consistent Enforcement of the CIP Version 5 Standards Across the BES

It is important that NERC and the Regions address the concerns I just discussed regarding CIP-002-5 in a consistent manner. This is particularly critical given that CIP-002-5 determines



which assets are subject to the CIP Version 5 Standards, and as such, is integral to every other CIP Version 5 Standard.

I must note here that it impossible to expect identical outcomes in compliance and enforcement decisions from the Regions, due to the limitless variation in the facts and circumstances of each violation and because the risk posed by a violation varies based on the characteristics of the Registered Entity and of the Region's footprint. Instead, one should assess whether the Regions act in a fair manner that 1) is consistent with the risk posed by each violation and Registered Entity, and 2) incents appropriate behaviors to improve the reliability and resiliency of the BES.

Having said that, the ERO has taken and is taking numerous actions to ensure consistency in the enforcement of the CIP Version 5 Standards. The Regions recently adopted standardized audit practices, which will enhance consistency in audits of CIP Version 5 Standards and in audits of all the other Standards. The ERO has a number of working groups that enhance communication and consistency across NERC and the Regional Entities. The working groups have already discussed the CIP Version 5 Standards, and will discuss them more in the future. The Regions regularly reach out to NERC staff to address consistency issues as they arise, and NERC and the Regions conduct internal training to increase the consistency of CMEP implementation. Finally, as I discussed earlier in these comments, the Regions plan to work with NERC to create a guidance document for each CIP Version 5 Standard.

This concludes my remarks.

Thank you.