

**Remarks of Daniel P. Skaar, President and CEO
Midwest Reliability Organization**

FERC Technical Conference on Critical Infrastructure Protection Issues Identified in Order No. 791
April 29, 2014

Good morning, and thank you for the opportunity to provide comments. My name is Dan Skaar, and I am the President and CEO of Midwest Reliability Organization. I am not participating in my official capacity today so my comments do not necessarily reflect the views of the MRO Board.

The Bulk Power System (“BPS”) has become more secure as a result of the CIP Standards. Industry awareness of security matters has increased significantly over the last few years. And, state utility commissions and the National Association of Regulatory Utility Commissioners (“NARUC”) are actively promoting security for consumers at the distribution level in the United States.

We are all here because we know we have more to do. I have three suggestions for your consideration.

After World War I, the French built the Maginot line to secure its borders from invasion. They were comforted by this sophisticated, costly fixed fortification. A year after its completion, the Maginot line was rendered useless in a matter of days – bypassed and outflanked in World War II. We know the rest of the story.

Standards can be much like fixed fortifications – easily bypassed and outflanked.

My first observation is that we must prevent the CIP standards from becoming like fixed fortifications destined to turn into monuments, rather than protection.

So how do we proceed? We must be cognizant of the cost and confusion created by constantly changing the CIP standards. The CIP Version 5 standards (“Version 5”) can serve as the foundation for security provided we - the industry and regulators - are mindful of new technology and ever-changing risks to the Bulk Power System so we “future proof” the standards.

Virtualization illustrates the point. Virtualization allows one piece of hardware to run multiple operating system images at the same time - in effect, machines within a machine. This has the potential of creating mixed trust environments. Version 5 does not explicitly address this situation. Emerging communication technologies deployed in substations may pose similar challenges. Guidance and security frameworks may be necessary to complement standards in order to “future proof” them.

My second observation is that cyber security risk for our industry is about systems. It is not discrete risk; it is systems risk - a complex system of systems. Fortunately, Version 5 is more focused on systems than previous versions of the CIP standards. This is consistent with my long-held view of assessing risk on complex systems. It should be a “tops-down” exercise starting with the supervisory controls systems (ex. SCADA), focusing on the central nervous system downward to the “fingers and toes,” and recognizing the interdependencies including the cyber connections.

**Remarks of Daniel P. Skaar, President and CEO
Midwest Reliability Organization**

FERC Technical Conference on Critical Infrastructure Protection Issues Identified in Order No. 791
April 29, 2014

In the context of systems risk, we should be emphasizing the connections, such as ICCP, between neighboring entities' systems, regardless of size, just as much as connections within an entity's single system. After all, our mission is to prevent uncontrolled cascading events. We are only as strong as our weakest link. For MRO and two other Regional Entities, this is also an international endeavor because we share the interconnection with Canada. So, security interests must include our northern neighbors.

Let me describe what happens when we do not employ a "tops-down" approach to system risk. Recently, I participated in a Version 5 transition study. Thirty highly skilled people spent an hour discussing compliance around a device located inside a secured, physical perimeter that could only be reprogrammed by disassembly, re-flashing the EPROMs and then re-assembly. Reprogramming this device required physical access, specialized knowledge, and specialized equipment. There was much discussion and anxiety in the room. This was not a systems approach to risk, but rather a "fingers and toes" compliance mindset. Is it programmable? Yes. Is it a high security risk? No. In this situation, the probability for intentional, malicious manipulation is low. It is a discrete risk having little potential to contribute to an uncontrolled, cascading event.

On the other hand, an entity may have a Remote Terminal Unit ("RTU") communicating through routable protocol from a non-BPS asset. As a result, an individual may have easier access to the RTU at the substation because it is likely not governed by the CIP Standards and may create risk to the control system's front end. This clearly poses more risk than my first example, yet it probably isn't within the protection of the CIP Standards.

I want to be very clear. I am not implying that non-BPS assets or assets not designated as "critical" are not secure. Responsible Entities have obligations to customers and state regulators to maintain secure systems. But, I don't know what I don't know. And, the fact that I don't know the nature of communications with key systems, like supervisory control on the BPS, raises a concern. It may not be a risk, but it's a "known, unknown" which should be addressed in some manner.

Simply put, we must not confuse compliance with security risk causing industry to invest more in low probability matters (like the EPROM example) at the expense of higher risk items (like the RTU example). We need to find ways to optimize investments by using "tops down" approaches to system risk and if we do not address these communications interdependencies through the CIP standards, we should, at the very least, address them through guidance and security frameworks.

My third observation relates to enforcement. Cyber security is complex, requiring diverse perspectives. It is not a perfunctory legal process; it's a technical problem solving activity requiring frank engagement. We must promote problem-solving which allows entities to fix deficiencies without an enforcement proceeding. This is a rational regulatory approach. We can still have transparency without enforcement. Of course, we always have enforcement as a tool for serious

**Remarks of Daniel P. Skaar, President and CEO
Midwest Reliability Organization**

FERC Technical Conference on Critical Infrastructure Protection Issues Identified in Order No. 791
April 29, 2014

matters. But, we need to adopt a “fix it first” approach. The Reliability Assurance Initiative (“RAI”) can deliver this approach, and I am pleased that the Commission recognized in Order No. 791 the RAI efforts underway by the Electric Reliability Organization.

In summary, Version 5 can be enduring to the reliability of the Bulk Power System and be designed in a way that is valued by Responsible Entities. It should be akin to a UL listing. We can improve the value of the CIP standards by doing the following:

1. Consider methods to “future-proof” the standards so that they can adapt to new technologies and emerging threats;
2. Emphasize “tops-down” approaches in assessing security risks and recognize interdependencies; and,
3. Adopt a “fix it first” regulatory posture.

Thank you.