

**Opening Remarks by  
Kevin B. Perry, Director, Critical Infrastructure Protection  
Southwest Power Pool Regional Entity**

**Federal Energy Regulatory Commission Technical Conference on  
Critical Infrastructure Protection Issues Identified in Order No. 791**

**Need for Additional Definitions or Controls for CIP Reliability Standards**

**April 29, 2014**

**Introduction**

Good afternoon. My name is Kevin Perry. I am the Director of Critical Infrastructure Protection at the Southwest Power Pool Regional Entity. Thank you for inviting me to speak on the need for additional definitions or controls for CIP Reliability Standards. While the CIP Version 5 standards represent a significant and positive improvement in overall security of the Cyber Assets supporting the reliability of the Bulk Power System (BPS), there are several issues of vagueness or outright gaps that should be addressed. I will briefly address each of the significant issues in my remarks.

**Would versus Could**

First, the language of the CIP Version 5 standards and definitions uses the term “would,” such as “would within 15 minutes...” or “would affect...” I believe the language needs to be prospective. From a risk perspective, if something “could” happen, then entities should assume that under the right conditions it “would” happen and require the protective controls be implemented. The use of “would” implies certainty and registered entities may argue over that distinction in asserting certain BES Cyber Systems are not subject to the CIP standards.

**Definition of BES Cyber Asset**

Looking at the definitions, a BES Cyber Asset is defined as “A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, mis-operation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System.” While the definition of BES Cyber Asset appears to be precisely worded, it is long, convoluted, and confusing. The linkage of the Cyber Asset to the destruction, degradation, or rendering unavailable of a Facility, system, or equipment, that in turn would affect the reliable operation of the Bulk Electric System “when needed” sets a bar that could result in not all BES Cyber Assets being identified. The failure, mis-operation, or even intentional operation of a BES Cyber Asset could potentially impact the reliability of the BPS without such extreme consequences being present. The reference to affecting the reliable operation of the Bulk Electric System, “when needed,” is also problematic in that this condition is not clearly defined and is open to debate as to its meaning. While I contend that an N-100 contingency might be when the proper operation of the BES Cyber Asset is needed, I expect that some registered entities may attempt to demonstrate the lack of impact through less comprehensive engineering studies rather than assuming there may be a scenario in which the

proper operation of the BES Cyber Asset may be the only thing between BPS reliability and the initiation or furtherance of a cascading outage. I suggest that a better definition might be one where the Cyber Asset is a BES Cyber Asset if it performs, supports, or affects the performance of one or more BES Reliability Operating Services and it does so in real-time, currently defined as within 15 minutes of its required operation. I am not as concerned about the fifteen-minute threshold. Fifteen minutes may seem arbitrary and in some instances it may be hard to demonstrate, but it is based in Operations and Planning standards concepts, and it is how the CIP Standard discriminates between BES Cyber Assets with real-time impact and those without. Most Cyber Assets with real-time impact are expected to operate in far less time than the fifteen minutes specified in the definition and are clearly BES Cyber Assets. Similarly, many Cyber Assets without a real-time impact are also clearly non-impacting.

### **Interconnectivity**

The interconnectivity of BES Cyber Systems remains an issue. I believe the CIP Version 5 criteria for categorizing BES Cyber Assets fails to address connectivity as instructed by Order 761. The Generator Operator and Balancing Authority control centers are both subjected to an aggregate 1500 MW threshold to satisfy the minimum criteria for identifying the control center BES Cyber Systems as medium impacting and subjecting them to meaningful protective controls. Only the BES Cyber Systems of a Transmission Operator control center are unconditionally established as medium impacting if they do not satisfy any criteria making them high impacting. Balancing Authority control centers, and to a lesser extent Generator Operator control centers, are directly or indirectly interconnected with each other and with Reliability Coordinator and Transmission Operator control centers through the use of ICCP (Inter-control Center Communications Protocol) and possibly other protocols. This interconnectivity spans BPS Interconnection boundaries, essentially exposing all of North America to the risk of compromise and misuse of the control center BES Cyber Systems. To exacerbate the risk further, at least one Regional Transmission Organization, or RTO, has expanded its use of ICCP to include market participants that are not even subjected to the CIP standards. The principles of mutual distrust are ineffective because the ICCP communications are necessary and must be allowed into the adjacent control center's network. To minimize the risk, I suggest that inter-control center communications, including ICCP, File Transfer Protocol (FTP), and web services be treated in a similar manner as interactive remote access. Such access should be terminated in a DMZ outside of the ESP and the traffic into the ESP strictly controlled. These protections should be required even for control centers containing Low impacting BES Cyber Systems.

### **Communication Networks**

As I discussed this morning during the Communication Networks session, I believe that an appropriate subset of the CIP Version 5 Standards should be extended to the communication network infrastructure outside the ESP where the registered entity has administrative management control over the hardware. While no one expects the registered entity to impose the CIP standards on a commercial carrier, such as AT&T, the registered entity can certainly apply some aspect of the CIP Version 5 standards to the equipment it manages.

### **Transient Devices**

The Commission noted its concern in Order 791 with the uncontrolled use of transient devices within the Electronic Security Perimeter and directed NERC to develop appropriate controls. A standards drafting team is working on the issue now and I expect that basic security controls such as up-to-date

patches and anti-malware will be required. What I do not think is being addressed is the exclusionary language found in the definition of a BES Cyber Asset. That definition declares “A Cyber Asset is not a BES Cyber Asset if, for 30 consecutive calendar days or less, it is directly connected to a network within an ESP, a Cyber Asset within an ESP, or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.” I view a transient device as a Cyber Asset connected to the network for an express, limited, short duration purpose and disconnected immediately upon completion of that purpose. It should not linger on the network any longer than absolutely necessary and should not be a device that is regularly and routinely connected to the network. Under the current definition, I can envision a registered entity having a transient device that is continuously connected to the network for 30 calendar days, briefly disconnected, and reconnected for another 30 days, leveraging the 30-day timeframe to circumvent the application of more stringent cyber security controls.

## **Virtualization**

Probably the greatest challenge, one that is not addressed in the CIP standards, is the rapidly expanding use of virtualization. At audit, I am seeing virtual Local Area Networks defined in switches and routers where some VLANs are within the ESP and some are not. I am seeing the deployment of virtual computing environments where the hypervisor is managing Cyber Assets inside an ESP, perhaps even Critical Cyber Assets, and Cyber Assets outside the ESP. And I am seeing shared storage, typically large scale Storage Area Network devices, again hosting storage for Cyber Assets within an ESP and for Cyber Assets outside the ESP. These mixed trust environments pose a risk to the BES Cyber Systems running on them. I am not opposed to virtualization, but I do believe that mixed trust should not be permitted. The CIP V5 standards need to clearly require Protected Cyber Asset treatment for the Hypervisor and any virtual non-BES Cyber System that is running or can run on the virtual system. The same should be true for any shared storage devices. And a network device running Virtual LANs should either be an Electronic Access Point with strong access controls, or should either host ESP traffic or non-ESP traffic, but not both.

Another virtualization issue is the emerging use of cloud computing. The CIP standards tangentially address use of the cloud with the need to protect information about BES Cyber Systems. The concern is beyond that however. There has been discussion about performing certain engineering functions, including transmission planning studies, in the cloud. What is to prevent real-time operations tools, such as power flow, state estimator, and contingency analysis from being shifted to the cloud? In the cloud, the user loses control over the computing and storage resources being utilized, and that gives me a reason to be concerned. Hopefully the definition of BES Cyber System and the application of the CIP standards to those systems are sufficient to discourage use of the cloud in support of Control Center operations. Only time will tell.

## **Summary**

There are many more improvements that could be made to tighten up the CIP Version 5 standards, but I will limit myself to the most important in the interest of time. In summary, they are the use of “would” versus “could” in the standards and definitions language; the definition of BES Cyber Asset; the issues around interconnectivity, especially through the use of the ICCP protocol; critical communication network equipment; transient devices; and the rapid growth in the use of virtualization.

Thank you for the opportunity to provide opening remarks for this technical conference. I look forward to the discussion to follow.