Introduction

Good morning. 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 adequacy of the CIP Version 5 standards for the protection of Bulk Power System Communication Networks.

The Need for Protection

The CIA triad (in other words, confidentiality, integrity and availability) is one of the core principles of information security. In the electricity sector, I believe integrity and availability are critical. Without timely, accurate data, the ability to maintain situational awareness and to control the Bulk Power System is severely hampered, placing the reliability of the BPS in jeopardy. Confidentiality, while important, is not as critical. While not necessarily easy to do, it is possible to intercept and manipulate data via a man-in-the-middle attack. Data can be changed or replayed to make the operator assume incorrect operating conditions and to respond improperly. DNP3, a protocol commonly used to communicate data between the control center and the field assets, is vulnerable to buffer overflow and other injection attacks, irrespective of whether the data is transmitted via a routable protocol. Data can also be manipulated or control command sequences inserted to cause the unintended operation of field equipment. The ability to intercept and manipulate data has been demonstrated in a variety of classified and unclassified settings. And, the data can be intercepted to obtain information about current operating conditions that could be valuable in crafting and carrying out a successful attack against the Bulk Power System. These attacks are simplified by the fact that the data is often transmitted in clear text and without end-point authentication or integrity verification, making the data manipulation easy to accomplish.

The Current (Version 3) Standards

Today, the CIP Version 3 standards require only that the communication network systems serving as Electronic Security Perimeter Access Points and any communication network devices and infrastructure residing within the Electronic Security Perimeter be protected under the CIP standards. These protections consist of a combination of basic logical and physical controls, including the requirement that these devices be subjected to physical and electronic access controls and managed per a variety of administrative and technical controls. The standard explicitly excludes any communications infrastructure outside of the Electronic Security Perimeter, including communications between Electronic Security Perimeters.
The FERC-approved definition of Cyber Asset as applied in the CIP Version 3 standards includes “data” which was understood to mean both data in motion and data at rest. To protect data in motion, the registered entity was expected to physically protect the cabling over which the data were transmitted within the Electronic Security Perimeter. The standard does not require encryption or other controls to protect the data communicated outside of the ESP. It quickly became apparent that physically protecting the data in motion was problematic given the pre-existing characteristics of the Critical Asset and the design of the communication networks. FERC approved an interpretation of CIP-006-2, Requirement R1.1, on July 15, 2010, allowing for alternative physical or logical protection controls in lieu of a six-wall boundary. Essentially, this interpretation recognized and addressed the problems with protecting data in motion when the data and its transmission media could not be contained within a six wall boundary. On March 21, 2013, FERC remanded an interpretation of the same requirement that sought to exclude data cabling, and thus data in motion, from the CIP standards when the Electronic Security Perimeter was not entirely contained within a single Physical Security Perimeter. While the application of CIP-006-3, Requirement R1.1, as interpreted, serves to protect the data within the ESP, it still does not protect data in motion between ESPs or between the ESP and any field Cyber Assets not subject to the CIP standards.

Currently Applied Controls

At audit, I have seen a variety of protections for data within a control center Electronic Security Perimeter. Those controls include the physical protection of the network communication devices and data cabling within the control center facility and the control of electronic access at the ESP network perimeter. While not required by the CIP standards, I have also seen, albeit not consistently, the use of encrypted VPN tunnels between the primary and backup control center ESPs. However, I have also seen where the registered entity has implemented or continued the use of a non-routable protocol between the control center and a field asset for the express purpose of keeping the field asset out of scope of the CIP standards. The use of a routable protocol to communicate beyond the confines of an Electronic Security Perimeter is a determinant for identifying Critical Cyber Assets and registered entities are legitimately leveraging that determinant to minimize the number of Critical Cyber Assets they have in the program. Unfortunately, I have also seen registered entities attempt to argue that the use of Multiprotocol Label Switching, or MPLS, for their wide area networking is not communication using a routable protocol because data is directed from one network node to the next based on short path labels rather than long network addresses, avoiding complex lookups in a routing table. Similarly, I have seen entities argue that a routable protocol was not in use because the data was going, in part, through a Layer 2 switch, or that a relay was not communicating outside the ESP with a routable protocol because it was serially connected to an RTU that was, in turn, communicating with a routable protocol. In those instances, the registered entity was advised of non-compliance with the CIP standards.

The CIP Version 5 Standards

The CIP Version 5 standards, as currently approved, have made some substantive changes to address the security gaps present in today’s CIP standards. There remain significant gaps that can, in many cases, be readily addressed without excessive expenditure of resources. And, the CIP Version 5 standards took a step backwards with respect to communication networks and data. As FERC noted in Order 791, the definition of Cyber Asset was modified to remove communication networks from the definition and to limit data to that residing within the device, also known as data at rest. I see two gaps with respect to communication networks. First of all, routable data communicated between Electronic
Security Perimeters should be encrypted. This presumes an ESP or electronic access control of some sort at assets containing Low impact BES Cyber Systems. For data communication between ESPs, the encryption can be readily established by defining an encrypted VPN tunnel in the firewall or router at each end of the communication path. If an ESP has been extended across multiple, geographically dispersed assets where end-to-end physical control of the communication network cannot be maintained, high-speed encryptors are commercially available that will encrypt the data as it travels between the physical locations. The data encryptors are not viewed as ESP Access Points and there is no expectation of attempting to impose electronic access control beyond the connection negotiation between the two devices. Registered entities should also consider encrypting non-routable data traffic between the control center and the field asset; in other words the RTUs and relays in the generation plants and transmission substations. There are in-line, or “bump in the wire” solutions available to address this need. Encryption should be avoided, however, if the data latency introduced by the encryption process could cause the intended operation to fail. An example of data latency risk is found in protective relaying schemes where millisecond timing is needed to protect the equipment from damage. Ideally, the data in motion should also be cryptographically hashed in order to detect modification, and date/time stamped to detect a replay attack. Hashing and date/time stamping are not widely used today and are not something that can be easily introduced, but they are far superior to protecting the integrity of the data than can be accomplished with encryption alone.

Secondly, some sort of protections should be extended to the communication network infrastructure outside the ESP where the registered entity has administrative management control over the hardware. NERC Reliability Standard COM-001-1.1 requires each Reliability Coordinator, Transmission Operator, and Balancing Authority to provide adequate and reliable telecommunications facilities for the exchange of Interconnection and operating information. The standard requires the telecommunications facilities to be redundant and diversely routed where applicable. The purpose is to provide for high availability of the critical communication networks, both local and wide area. The CIP Version 5 standards should require the registered entity to protect the Cyber Assets used to provision these networks to the extent the registered entity has administrative control over the assets. No one expects the registered entity to impose the CIP standards on a commercial carrier, such as AT&T, but the registered entity can certainly apply some aspect of the CIP Version 5 standards to the equipment it manages. I suggest that modifications be made to the CIP Version 5 standards to address both of these gaps that at a minimum restrict physical and electronic access.

Summary

In summary, while the CIP Version 5 standards have made substantive changes that will close a number of security gaps present in the Version 3 standards, two significant communication network gaps remain that should be addressed. The integrity of the data relied upon for Bulk Power System reliability needs to be protected during communication by encryption at a minimum and, where possible, through the application of cryptographic hashing and date/time stamping. The critical communication network Cyber Assets outside of the Electronic Security Perimeter but under the management control of the registered entity need to be protected through the application of an appropriate set of security controls.

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