

Good morning. My name is Steven Parker, and I am President of Energy Sector Security Consortium, commonly known as EnergySec. I would like to thank the Commission for the opportunity to participate in this important panel discussion addressing the security of communications in the Bulk Power System. In my opening statement I will discuss this issue as it relates to the NERC CIP standards.

Though not entirely ignored, communications are only tangentially addressed in the CIP standards. The standards themselves are centered on the protection of those cyber assets deemed to have importance in the operation of the bulk power system, but largely ignore the function of communication itself. First, let me point out some notable exceptions.

The requirement for Electronic Security Perimeters (which I will refer to as ESPs) results in some restrictions on communications to and from protected cyber assets. Likewise, the requirement to limit ports and services both through such perimeters, as well as on cyber assets themselves, provides another communication related control. Communication devices themselves, such as switches and routers, are often in scope for the CIP standards. And finally, there are requirements related to remote interactive access.

Despite these examples, significant gaps exist in version 5 of the standards with respect to communications. I will briefly touch on three of these areas, and hope to expand on these during the balance of the panel discussion.

First, with respect to ESPs and required port restrictions, the standards allow any and all communication deemed necessary for operations by an entity, even if such communications utilize insecure protocols. There are no requirements related to the security of the communications themselves.

Second, non-routable communications are entirely out of scope. In version 5, all requirements related to ESPs involve only routable communications. As written, the standard and its associated formal definitions can be reasonably be construed to allow any form of non-routable communication to and/or from any in-scope cyber asset and any other asset with no protections whatsoever. This is a significant gap.

And third, communications occurring outside of an ESP are also out of scope. This is significant since most wide area communications occur outside the context of an ESP. For example, the Inter-Control Center Communications Protocol (ICCP), is used to exchange operational data between control centers. Although the servers involved in the process are nearly universally considered to be in-scope for protection, the wide area communications through which the data is exchanged, is universally out of scope.

I don't believe these gaps to be intentional, rather, they are a natural byproduct of requirements which center on cyber assets alone. Although the focus on cyber assets was a proper first step in early versions of the CIP standards, I believe the time has come to address communications as a function.

To be clear, I am not suggesting that specific, prescriptive controls are missing from the standards and should be developed. Rather, I assert that the standards lack defined security objectives for communication functions, and that such objectives should be defined and addressed in future versions of the CIP standards.

Let me explain this further by mentioning two distinct but related topics. First, in the guidance section of CIP-005-5, the drafting team explained that specific requirements for serial communications were excluded, since no universally applicable requirements could be identified. Second, in paragraph 108 of Order 791, the Commission stated that NERC might address the lack of specific requirements for low-impact assets by, “developing objective criteria against which the controls adopted by responsible entities can be compared and measured in order to evaluate their adequacy”

We see two concepts here. First, prescriptive controls can be difficult to construct. Second, an alternative to prescriptive controls might be to articulate objectives and associated criteria for evaluating whether those objectives have been met. Such an approach allows entities the flexibility to be innovative in meeting security objectives.

Communications is an area where such an approach would be appropriate, if not necessary. Communication technologies used in the Bulk Power System are numerous and diverse. There is no set of prescriptive controls that would be both appropriate and sufficient for all such communications. However, it is likely that a set of security objectives for the protection of such communications could be developed, and indeed it should be.

To summarize, there are significant gaps related to communications in version 5 of the CIP standards. These gaps should be addressed in future versions, but require a different approach than that currently used. I look forward to exploring this further in the remainder of this panel discussion.

Thank you.