UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Technical Conference on Critical Infrastructure Protection Issues Identified in Order No. 791

Prepared Statement of David Batz
April 29, 2014

Good afternoon members of the Commission Staff. I am David Batz, Director, Cyber & Infrastructure Security at Edison Electric Institute, and am here today representing Edison Electric Institute and its member companies.

We appreciate the Commission holding this conference.

EEI is the association of the nation's shareholder-owned electric utilities and its affiliates world-wide. Its members own or operate approximately 70% of the electric industry assets in this country. In addition, its members include Generator Owners and Operators, Transmission Owners and Operators, Load-Serving Entities, and other entities that are subject to mandatory Reliability Standards developed and enforced by NERC.

The Commission requested input on a number of technical issues including:

1. Whether the NERC Glossary of Terms needs either new definitions, or modifications of current definitions, to ensure adequate protection of BPS communication networks.
2. The types of physical or logical controls that may be needed to protect BPS communication network components communicating via non-routable protocols, or through serial communication links.

3. The types of physical or logical controls that may be needed to protect non-programmable components of data communications networks (e.g., cabling).
4. The types of physical or logical controls that may be needed to address the cybersecurity needs of remote access processes and devices.
5. How the confidentiality, integrity, and availability of data in motion (i.e., being transmitted) over BPS communication networks can be ensured physically and/or electronically.
6. To what extent different types of encryption technology can be effectively employed on BPS communication networks without adversely affecting BPS operations.
7. For each of the topics above, the whether there are gaps in the current CIP version 5 Standards that could be addressed, and suggested recommendations for adjustment of the CIP version 5 Standards to address any gaps.

EEI Member Companies are strongly aware of the importance of reliability to our customers and therefore the importance of the issues we are covering today. Protecting the nation's electric grid and ensuring a reliable supply of power is the electric power industry's top priority. The electric power industry takes cybersecurity threats very seriously. Cybersecurity incidents may disrupt the flow of power or reduce the reliability of the electric system. Key to the success of this effort is the ability to provide measures capable of protecting the evolving intelligent network against interruption, exploitation, compromise or outright attack of cyber assets, whether the

attack vector is physical, cyber or both. Our members are committed to providing reliable and resilient infrastructure for the communities that we serve. We believe that reliability consists not only of protection and prevention, but also recovery and response. We believe that entities need to have the ability to be flexible in responding to evolving and newly emerging threats.

Recognizing that there are a broad range of interdependencies, and potential consequences associated with the loss of different facilities or components, EEI supports a risk-based, prioritized approach that identifies assets truly critical to the reliable operation of the electric grid. This ensures the most important elements of our system receive the highest level of attention, as well as the resources necessary to secure them. Without engaging on the specifics of potential vulnerabilities associated with the equipment that is the subject of this technical conference, it is important to consider that Bulk Power System owners and operators have to evaluate and prioritize relative risk on a constant basis, and that the range of threats and vulnerabilities have widely varying potential impacts on the system. Protections provided for a specific asset should be commensurate with the associated cyber or physical risk. Further, the controls established for a specific equipment need to be assessed as part of each entity's defense in depth of all of its BES cyber-systems, not in isolation.
In response to the cyber and physical threats, electric companies employ various strategies to protect these systems, but security risks still exist to some degree.

With respect to the issue of changes to the NERC Glossary of Terms, EEI believes that it is appropriate for the structure of the mandatory CIP standards to arrive at a steady state. Looking at the progression through the rear view mirror, EEI

appreciates that initial versions of CIP standards aimed at requirements for those assets that had more obvious systemic importance. While the electric industry had over the years developed an established framework for traditional operations and planning issues upon which to base Reliability Standards under Section 215, initial CIP Standards reflected industry's first impression for structuring enforceable requirements from the perspective of critical infrastructure protection. Looking at the combined effects of accumulated experience up to now with performance under the Standards, the Commission's directives under Order No. 706, and the exhaustive considerations of the drafting project, EEI strongly believes that v.5 provides a durable framework that will not require significant change or expansion for several years.

As a general matter, EEI strongly believes that the v.5 NERC Standards ensures a durable and long-lived framework that allows companies to decide most appropriate technologies, applications, and controls, based on risk assessments of their assets and facilities. Instead of micro-managing specific technologies, practices, or processes, EEI asks that the Commission allow the regulated entities through the approved V.5 Standards to exercise flexibility and adaptability to meet changing threats and vulnerabilities, new IT technology, and the cost effectiveness of meeting their performance requirements under the Standards. Rather than applying enormous resources to the constant review and revision of the Standards, EEI believes that limited resources are best applied to planning and management of their CIP and cybersecurity work. In addition, the Commission should allow the electric industry to examine through experience whether v.5 contains any reliability gaps or overlaps, or inefficiencies that merit formal review in the standards development process.

Technical discussions of new and emerging issues can and should take place in a far more productive and efficient venue than the NERC standards development process. In addition, EEI believes that considerable process exhaustion has taken its toll on stakeholders in the v.5 Standards development. Considering the highly dynamic nature of CIP and cybersecurity issues, and evolving technology, EEI urges the Commission to allow time for companies, NERC, and the Commission itself, to gather experience with v.5, and continue discussions on the technical issues in the appropriate industry venues.

In the near term, as the industry embarks on v.5 Standards compliance activities, and NERC and the Regions develop associated audit and compliance review materials, EEI suggests that guidance documents addressing related specific technical matters incorporate particular appropriate terms and definitions, such as those published in NISTIR 7298 (Rev 2).

Although there are a number of physical or logical controls that can be employed to protect BPS communication network components communicating via non-routable protocols, or through serial communication links, there is no “silver bullet” to address all potential communication related cybersecurity problems.

Entities may employ physical security mechanisms to aid in the protection of remote nodes in addition to the practice of physical security often used to protect central collection communication servers. Recognizing that physical security cannot be guaranteed; particularly for remote, unattended facilities, entities may incorporate other controls as part of an overall risk management strategy. These may include integrity checks, and out-of-bound detection for communication links as well as working with

system vendors to understand how their products respond to invalid or unauthorized messages being inserted into a communications channel. Some entities may choose to incorporate cryptographic modules for certain serial communications. However it is important to remember that encrypted serial communications does not solve or address all potential attack vectors. In addition, there are important availability and performance issues that should be contemplated before cryptographic modules are deployed. As specified in the PNNL AGA-12, Part 2 Performance Test Results[1]

> A principal concern observed during performance testing activities is the impact of repeated decommissioning of SCM-1 devices upon SCADA communication. To avoid the problem, the device had to be taken out of service with all data communication cables removed prior to making a configuration change. This repeated decommissioning was unpredictable and may be a barrier to implementation. During laboratory performance testing, the reliability of vendor equipment was observed. While not directly related to performance, reliable operations of vendor equipment will directly impact the willingness of asset owners to adopt any technology. The security objectives for control systems are personnel safety, reliable operations, data integrity, and lastly confidentiality. The AGA- 12 devices provide data confidentiality and integrity, but SCM-1 devices adversely impacted reliability. An installed security appliance that is inoperable provides no added value to the field device. No SCADA data, no control functions, and no remote engineering access are supported. A decommissioned device is equivalent to a failed modem. Security solutions cannot adversely impact reliable operations or personnel safety.

Although there are a number of physical or logical controls that can be employed to protect non-programmable components of data communications networks (e.g., cabling), there is no single solution or technology to address all potential communication related cybersecurity problems. Each entity should consider the facts and

[1] M.D. Hadley, K.A. Houston, T.W. Edgar, "AGA-12, Part 2 Performance Test Results," *Pacific Northwest National Laboratory,* August 2007, Page 50, Accessed 4/21/2012

circumstances associated with the communication paths that are used for BPS related communications.

These measures can include:[2]

- Restricting logical access to the network and network activity
- Restricting physical access to the network and devices
- Protecting individual components from exploitation
- Maintaining functionality during adverse conditions
- Restoring system after an incident

The particular measures selected by an entity to manage risk associated with communications networks are dependent upon a risk assessment and an understanding of BPS process to be secured as well as features or limitations of the network media, equipment and interfaces, as well as health and safety considerations.

In addition, it is important to note that the use of encryption can significantly complicate the implementation of other security controls such as intrusion detection systems and anomaly detection systems.

Regarding types of physical or logical controls that may be needed to address the cybersecurity needs of remote access processes and devices, v.5 brings a strong set of new requirements and controls for remote access.

[2] NIST SP 800-82, Page 10

The next two issues, securing data in motion and questions about encryption will be addressed together. As stated earlier, the particular measures selected by an entity to manage risk associated with communications networks are dependent upon a risk assessment and an understanding of the data to be secured as well as features or limitations of the network media, equipment and interfaces, as well as health and safety considerations. Encryption does not solve all security problems, and if improperly implemented can lead to a lack of availability and reliability.

The Department of Homeland Security offers guidance concerning this issue in their Catalog of Controls:

> 2.8.9.2 Supplemental Guidance[3]
>
> The use of a third-party communication service provider instead of organization-owned infrastructure may warrant the use of encryption. The use of cryptographic mechanisms within a control system could introduce communications latency because of the additional time and computing resources required to encrypt, decrypt, and authenticate each message. Any latency induced from the use of cryptographic mechanisms must not degrade the operational performance of the control system.
>
> 2.8.20.2 Supplemental Guidance
>
> Message authentication provides protection from malformed traffic from misconfigured devices and malicious entities. The intent is to establish confidence at each end of a communications session with respect to the validity of the data and the identity of the sender. This is to address man-in-the middle attacks, which can include session hijacking,

[3] Department of Homeland Security Catalog of Control System Security – Recommendations for Standards Developers, April 2011, Page 68

> insertion of fake information, or instruction sets in the middle of a session.
>
> In situations where the ICS cannot protect the authenticity of communications sessions, the organization employs compensating controls (e.g., auditing measures, isolation/segmented architecture, additional physical isolation). Enhanced auditing measures or encryption mechanisms designed to enhance session authenticity must not impact ICS operations by consuming too many available resources or by slowing down communications to an unacceptable level as to constitute a self-inflicted denial-of-service attack.[4]

Cybersecurity risk, as with all risks, cannot be completely eliminated, but instead must be managed through informed decision making processes.[5] EEI member companies are committed to maintaining the safe and reliable operation of the BPS and managing cybersecurity risk.

Mandatory and enforceable Standards represent an important tool that can be used to support the reliability of the BPS. However, Standards alone are not sufficient to address a dynamic environment of emerging risks, unpredictable threat actors, and rapid changes in technology. The industry is also engaged in public-private partnerships, information sharing between government and industry, and the exchange of best practices both within the electricity sub-sector and with other critical sectors and disciplines.

[4] Department of Homeland Security Catalog of Control System Security – Recommendations for Standards Developers, April 2011, Page 72

[5] U.S. Department of Energy, "Electricity Subsector Cybersecurity – Risk Management Process," May 2012, Page 2