



Critical Infrastructure Protection Issues Identified in Order No. 791

RM13-5-000

April 29, 2014

Agenda

10:00 – 10:15 p.m. Welcome and Opening Remarks by Commission Staff

Introduction

In Order No. 791, the Commission approved the Version 5 Critical Infrastructure Protection (CIP) Reliability Standards, CIP-002-5 through CIP-011-1 (CIP version 5 Standards), submitted by the North American Electric Reliability Corporation (NERC).¹ Order No. 791 directed Commission staff to convene a staff-led technical conference, within 180 days from the issuance date of the Final Rule, to examine several of the technical issues identified therein.² The purpose of this conference is to obtain further information as to: (1) the adequacy of the approved CIP version 5 Standards' protections for Bulk-Power System data being transmitted over data networks; (2) whether additional definitions and/or security controls are needed to protect Bulk-Power System (BPS) communications networks, including remote systems access; and (3) the functional differences between the respective methods utilized for identification, categorization, and specification of appropriate levels of protection for cyber assets using CIP version 5 Standards as compared with those employed within the National Institute of Standards and Technology (NIST) Security Risk Management Framework.

¹ *Version 5 Critical Infrastructure Protection Reliability Standards*, Order No. 791, 78 Fed. Reg. 72,755 (Dec. 3, 2013), 145 FERC ¶ 61,160 (2013), *order on reh'g*, Order No. 791-A, 146 FERC ¶ 61,188 (2014).

² *Id.* at PP 7, 150, and 225.

Panel 1**10:15 – 11:45 p.m. The Adequacy of the CIP version 5 Standards for Protection of BPS Communication Networks**

The Commission seeks information about the adequacy of the approved CIP version 5 Standards for protecting data being transmitted over BPS communication networks.

Panelists are encouraged to address:

- The vulnerabilities that BPS communication networks may be facing and how effectively they are being protected against these risks by the currently enforced CIP Reliability Standards.
- The adequacy of the approved CIP version 5 Standards security controls to protect BPS communication networks against current and projected vulnerabilities.
- The types of physical or logical controls that are currently being applied to protect BPS communication networks and the adequacy of these controls to address the protection of: (1) non-routable protocols, (2) serial communication links, (3) non-programmable components, (4) remote access processes and devices, and (5) data in motion.
- For each of the topics above, the panelists should address whether there are gaps in the current CIP version 5 Standards that could be addressed, and suggest recommendations for adjustment of the CIP version 5 Standards to address any gaps.

Panelists:

- Dan Skaar, President and CEO, Midwest Reliability Organization
- Kevin Perry, Director, CIP, Southwest Power Pool Regional Entity
- Richard Dewey, Senior Vice President & CIO, NYISO
- Steven Parker, President, EnergySec
- Mikhail Falkovich, Manager NERC/CIP Compliance, PSEG; Speaking on behalf of Electric Power Supply Association (EPSA)
- Tobias Whitney, Manager, CIP Compliance, North America Electric Reliability Corporation (NERC)

11:45 – 1:00 p.m. Lunch***Panel 2*****1:00 – 2:30 p.m. Need for Additional Definitions or Controls for CIP Reliability Standards**

The Commission seeks information on whether additional definitions and/or security controls are needed to protect BPS communications networks, including remote systems access. Panelists are encouraged to address:

- Whether the NERC Glossary of Terms needs either new definitions, or modifications of current definitions, to ensure adequate protection of BPS communication networks.
- 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.
- The types of physical or logical controls that may be needed to protect non-programmable components of data communications networks (e.g., cabling).
- The types of physical or logical controls that may be needed to address the cybersecurity needs of remote access processes and devices.
- 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.
- To what extent different types of encryption technology can be effectively employed on BPS communication networks without adversely affecting BPS operations.
- For each of the topics above, the panelists should address whether there are gaps in the current CIP version 5 Standards that could be addressed, and suggest recommendations for adjustment of the CIP version 5 Standards to address any gaps.

Panelists:

- Kevin Perry, Director, CIP, Southwest Power Pool Regional Entity
- Richard Kinas, Mgr. Standards Compliance, Orlando Utilities Commission
- James Boone, NERC Compliance Manager, Pepco Holdings Inc.
- Dr. Andrew Wright, N-Dimension Solutions
- Andrew Ginter, VP Industrial Security, Waterfall Security Solutions
- David Batz, Director, Cyber & Infrastructure Security, Edison Electric Institute

2:30 – 2:45 p. m. Break

Panel 3

2:45 – 4:15 p.m. NIST Frameworks Discussion

The Commission seeks information on functional differences between the respective methods used for identification, categorization, and specification of appropriate levels of protection for cyber assets using CIP version 5 Standards as compared with those employed within other cyber security frameworks, including the NIST Security Risk Management Framework (RMF) and the recently-released Framework for Improving Critical Infrastructure Cybersecurity (NIST Cyber Security Framework). Panelists are encouraged to address:

- The functional differences on how each framework approaches asset identification to address emerging threats, risks, and vulnerabilities. Panelists may suggest how the CIP version 5 Standards could be adjusted to address any concern or weakness, or explain whether or not the approaches identified in the NIST Security Risk

Management Framework and the NIST Cyber Security Framework are more appropriate for protecting BPS critical infrastructure.

- Whether it is prudent to use only facility ratings, (e.g., power, voltage, operating conditions), to identify and categorize BES cyber assets that are subject to CIP Standards in CIP-002-5. Panelists may suggest the inclusion of additional attributes, (e.g., data sensitivity) or recommend adjustments to the bright-line criteria for ensuring accurate identification and categorization of BES cyber assets. Panelists are encouraged to identify potential issues in Reliability Standard CIP-002-5 that could hinder the implementation of the CIP version 5 Standards (e.g. any issues relating to NERC Glossary of Terms definitions, CIP-002-5 criteria or impact levels).
- Comparisons between the CIP version 5 Standards security controls and the security controls of the two NIST Frameworks and the identification of specific security controls or control objectives that should be considered in future revisions of CIP standards.

Panelists:

- Patrick Miller, Managing Partner, The Anfield Group
- Brent Castagnetto, Manager, Cyber Security Audits & Investigations, WECC
- Gerald Mannarino, Director, Computer System Engineering, New York Power Authority
- Melanie Seader, Senior Cyber & Infrastructure Security Analyst, Edison Electric Institute
- Jason Christopher, Technical Lead, Cyber Security Capabilities & Risk Management, U.S. Department of Energy

4:15 – 4:30 p.m. Wrap-Up