



**Critical Infrastructure Protection Supply Chain Risk Management  
RM15-14-000  
January 28, 2016**

**Agenda**

***Welcome and Opening Remarks by Commission Staff***  
**9:30 – 9:45 a.m.**

***Introduction***

In a July 16, 2015 Notice of Proposed Rulemaking (NOPR) in the above-captioned docket, the Commission proposed to direct the North American Electric Reliability Corporation (NERC) to develop new or modified Critical Infrastructure Protection (CIP) Reliability Standards to provide security controls relating to supply chain risk management for industrial control system hardware, software, and services. The Commission sought and received comments on this proposal, including: (1) the NOPR proposal to direct that NERC develop a Reliability Standard to address supply chain risk management; (2) the anticipated features of, and requirements that should be included in, such a standard; and (3) a reasonable timeframe for development of a standard. The purpose of this conference is to clarify issues, share information, and determine the proper response to address security control and supply chain risk management concerns.

***Staff Presentation: Supply Chain Efforts by Certain Other Federal Agencies***  
**9:45 a.m. - 10:05 a.m.**

***Break***

**10:05 p.m. - 10:15 p.m.**

***Panel 1: Need for a New or Modified Reliability Standard***

**10:15 a.m. – 11:45 a.m.**

The Commission staff seeks information about the need for a new or modified Reliability Standard to manage supply chain risks for industrial control system hardware, software,

and computing and networking services associated with bulk electric system operations. Panelists are encouraged to address:

- Identify challenges faced in managing supply chain risk.
- Describe how the current CIP Standards provide supply chain risk management controls.
- Describe how the current CIP Standards incentivize or inhibit the introduction of more secure technology.
- Identify possible other approaches that the Commission can take to mitigate supply chain risks.

**Panelists:**

1. Nadya Bartol, Vice President, Industry Affairs and Cybersecurity Strategist, UTC
2. Jon Boyens, Project Manager, Information Communication Technology (ICT) Supply Chain Risk Management, National Institute of Standards & Technology (NIST)
3. John Galloway, Director, Cyber Security, ISO New England
4. John Goode, Chief Information Officer/Senior Vice President, Midcontinent Independent System Operator (MISO)
5. Barry Lawson, Associate Director, Power Delivery & Reliability, National Rural Electric Cooperative Association (NRECA)
6. Helen Nalley, Compliance Director, Southern Company
7. Jacob Olcott, Vice President of Business Development, Bitsight Tech
8. Marcus Sachs, Senior Vice President and Chief Security Officer, North American Electric Reliability Corporation (NERC)

***Lunch***

**11:45 a.m. - 1:00 p.m.**

***Panel 2: Scope and Implementation of a New or Modified Standard***

**1:00 p.m. - 2:30 p.m.**

The Commission staff seeks information about the scope and implementation of a new or modified Standard to manage supply chain risks for industrial control system hardware, software, and computing and networking services associated with bulk electric system operations. Panelists are encouraged to address:

- Identify types of assets that could be better protected with a new or modified Standard.
- Identify supply chain processes that could be better protected by a Standard.
- Identify controls or modifications that could be included in the Standard.
- Identify existing mandatory or voluntary standards or security guidelines that could form the basis of the Standard.
- Address how the verification of supply chain risk mitigation could be measured, benchmarked and/or audited.
- Present and justify a reasonable timeframe for development and implementation of a Standard.
- Discuss whether a Standard could be a catalyst for technical innovation and market competition.

**Panelists:**

1. Michael Kuberski, Manager, Grid Protection and Automation, Pepco Holdings Inc. (PHI)
2. Jonathan Appelbaum, Director, NERC Compliance, The United Illuminating Company
3. Nick Weber, CIP Compliance Auditor, Western Electricity Coordinating Council (WECC)
4. Art Conklin, Ph.D., Associate Professor and Director of the Center for Information Security Research and Education, University of Houston
5. Edna Conway, Chief Security Officer, Value Chain Security, Cisco
6. Bryan Owen, Principal Cyber Security Manager, OSIsoft
7. Alberto Ruocco, Vice President and Chief Technology Officer, American Electric Power (AEP)
8. Doug Thomas, Vice President and Chief Information Officer, Ontario Independent Electricity System Operation (IESO)

***Break***

**2:30 p.m. - 2:45 p.m.**

***Panel 3: Current Supply Chain Risk Management Practices and Collaborative Efforts***

**2:45 p.m. – 4:15 p.m.**

The Commission staff seeks information about existing supply chain risk management efforts for information and communications technology and industrial control system hardware, software, and services in other critical infrastructure sectors and the government. Panelists are encouraged to address:

- Generally describe how registered entities and other organizations currently manage supply chain issues.
- Identify standards or guidelines that are used to establish supply chain risk management practices. Specifically, discuss experience under those standards or guidelines.
- Identify organizational roles involved in the development and implementation of supply chain risk management practices.
- Generally describe approaches for identifying, evaluating, mitigating, and monitoring supply chain risk.
- Generally discuss how supply chain risk is addressed in the contracting process with vendors and suppliers.
- Generally describe the capabilities that registered entities currently have to inspect third party information security practices.
- Generally describe the capabilities that registered entities currently have to negotiate for additional security in their hardware, software, and service contracts. Describe how this may vary based on the potential vendor or supplier and the type of service to be provided.
- Generally describe how vendors and suppliers are managing risk in their supply chain.

**Panelists:**

1. Douglas Bauder, Vice President, Operational Services, and Chief Procurement Officer, Southern California Edison
2. Andrew Bochman, Senior Cyber & Energy Security Strategist, INL/DOE
3. Dave Whitehead, Vice President of Research and Development, Schweitzer Engineering
4. Andrew Ginter, Vice President, Industrial Security, Waterfall Security Solutions
5. Steve Griffith, Industry Director, National Electrical Manufacturers Association (NEMA)
6. Maria Jenks, Vice President, Supply Chain, Kansas City Power & Light (KCP&L)
7. Robert McClanahan, Vice President/Chief Information Officer, Arkansas Electric Cooperative Corporation (AECC)
8. Thomas O'Brien, Chief Information Officer, PJM Interconnection, LLC

**4:15 p.m. - 4:30 p.m. Closing Remarks**