NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Technical Conference on Critical Infrastructure Protection Supply Chain Risk Management

Remarks of Marcus Sachs, Senior Vice President and the Chief Security Officer
North American Electric Reliability Corporation
January 28, 2016

Chairman Bay, Commissioners, staff, and fellow panelists. My name is Marc Sachs and I am a Senior Vice President and the Chief Security Officer at the North American Electric Reliability Corporation (NERC). I greatly appreciate the opportunity to participate in today's technical conference related to supply chain risk management.

As discussed in NERC's comments on the Revised Critical Infrastructure Protection Standards Notice of Proposed Rulemaking (NOPR), NERC appreciates the Commission's attention to this issue. It is vital to the reliability and security of the bulk power system (BPS) that electricity subsector participants continue focusing on mitigating security risks associated with the global supply chain. As the Commission discusses in the NOPR, complex supply chains for information and communications technology and industrial control systems present risks to BPS security, providing various opportunities for adversaries to initiate cyberattacks. As I will discuss, several requirements in the CIP Reliability Standard already help to mitigate certain supply chain risks. Nevertheless, for reasons I will articulate, additional mandatory Reliability Standards may not be the most efficient and effective way to further mitigate these risks. Should the Commission decide to direct NERC to develop additional Reliability Standards, I will offer some items for the Commission to consider.

Supply chain risk management is not an issue that the electric industry faces alone. It cuts across all industry sectors, and presents challenges for states and federal governments as well. Over the past two decades I have served in various positions that required a deep understanding of how the global supply system works, and the emerging cyber threats that result from globalization. Prior to joining NERC in May 2015, I was in the telecommunications sector and worked closely with the federal government on many security issues, including supply chain risk management. Specifically, I served as vice president of National Security Policy for more than seven years at Verizon Communications, Inc., where I led national and homeland security public policy efforts. In 2008, I was one of the first private sector experts to identify how the supply chain could be used as an attack vector, and gave several classified and unclassified briefings on this subject over the next few years. Prior to Verizon, I was the deputy director of the Computer Science Laboratory at SRI International, which supported DHS' Cybersecurity Research and Development Center. Among other projects, I was involved in research being used today to support security techniques used by major US-based electronics companies to fabricate consumer and critical

infrastructure electronic components in foreign factories. In 2002, I was appointed by the President to serve on the staff of the National Security Council as the director for Communication Infrastructure Protection in the White House Office of Cyberspace Security, and on the staff of the President's Critical Infrastructure Protection Board, where I coordinated efforts to protect and secure the nation's telecommunication and Internet infrastructures. Even at that early timeframe we were already concerned about globalization and its impact on critical infrastructure protection.

Based on my prior experience, I am well aware of the challenges associated with supply chain risk management and its importance to critical infrastructure sectors. Supply chain management is a complex global issue that is not susceptible to an easy, one-size-fits-all approach. Supply chains for information and communications technology and industrial control systems are long and multidimensional, involving numerous parties in a multitude of countries across the globe. Multiple entities across the globe may participate in the development, design, manufacturing, and delivery of a single product purchased by a registered entity. For example, nearly 100% of all electronic components sold in the United States – ranging from consumer smart phones and laptops to sensors and control systems are manufactured outside of the country. Software is mostly written abroad as well, and even contracted technical support services are rapidly being outsourced to foreign companies and entities. Nearly all of this movement to Asia, South and Central America, Africa, and the Middle East is due to lower labor costs in those regions, reliable global high-speed communications networks, relatively low shipping costs, and low or non-existent import duties into the US.

We cannot go back to domestic-only production of electronic goods and services. Our nation's economy as well as the economies of other countries depends on a globalized supply system. We must recognize that other countries are experiencing the same vulnerabilities and concerns that we face, and many are looking to us for guidance.

As supply chain management risks are constantly evolving, the development and sharing of industry best practices, lessons learned, and developing the technical means to mitigate those risks, including identifying counterfeit or non-genuine parts and components, is the way ahead. NERC understands that the electric industry is already engaging in this activity. For instance, industry participants worked with the Department of Energy to draft the DOE guidelines – *Cybersecurity Procurement Language for Energy Delivery Systems* – referenced in the NOPR. Further, as NERC noted in its NOPR comments, the Edison Electric Institute developed a set of key principles and recommendations for entities to consider for managing supply chain cybersecurity risks.

NERC is committed to using its many reliability tools – guidelines, training exercises, alerts, situational awareness, and, where necessary, mandatory Reliability Standards – to support industry's efforts to mitigate supply chain risks. As detailed in NERC's NOPR comments (at pages 15-17), NERC's CIP Reliability Standards already include requirements that help mitigate supply

chain risks. Among others, the CIP cybersecurity Reliability Standards include the following requirements, many of which include controls that correspond to controls in NIST SP 800-161:

- CIP-004-6, Requirement R1 requires responsible entities to implement cybersecurity awareness programs, which may include the reinforcement of cybersecurity practices to mitigate supply chain risks.
- CIP-004-6, Requirement R3 requires entities to implement a personnel risk assessment to attain and retain authorized electronic access and authorized unescorted physical access to BES Cyber Systems. The personnel risk assessment applies to any outside vendors or contractors seeking to attain and retain such access.
- CIP-004-6, Requirements R4 and R5 require entities to implement access (physical and electronic) management and access revocation programs. These programs must include outside vendors and contractors.
- CIP-005-5 and CIP-006-6 require entities to implement protections to control electronic and physical access to BES Cyber Systems, including access by outside vendors and contractors.
- CIP-007-6, Requirement R2 requires entities to implement a patch management process for tracking, evaluating, and installing cybersecurity patches. Applying patches on a timely basis may help mitigate risks associated with cybersecurity vulnerabilities created during the design and manufacturing stages of the supply chain.
- CIP-007-6, Requirement R3 requires entities to implement processes to deploy, detect, prevent, and mitigate the threat of malicious code. These processes may help entities detect and address malicious code inserted into a product prior to acquisition by the entity.
- CIP-007-6, Requirement R5 requires entities to implement processes for system access control. These processes would apply to any outside vendors or contractors granted access to protected devices.
- CIP-008-5 requires entities to implement a Cyber Security Incident response plans. These plans may help identify if a BES Cyber Security Incident relates to a supply chain issue and reduce the impact of any incident caused by a supply chain issue.
- CIP-009-6 requires entities to implement plans to recover the reliability functions performed by BES Cyber Systems in the event of a cybersecurity incident. These recovery plans will help reduce the impact of any incident caused by a supply chain issue.
- CIP-010-2, Requirement R3 requires entities to perform vulnerability assessments at least once every 15 calendar months. The vulnerability assessments may help identify any vulnerabilities resulting from supply chain issues.
- CIP-010-2, Requirement R3, Part 3.3 requires that entities perform, for all high impact BES Cyber Systems and their associated Electronic Access Control and Monitoring Systems

and Protected Cyber Assets, an active vulnerability assessment prior to adding a new applicable Cyber Asset to a production environment. This assessment will help mitigate supply chain risks to the most critical assets prior to commissioning.

- CIP-010-2, Requirement R4 requires entities to implement a plan to address risks associated with transient devices. These plans must include protections for transient devices managed by vendors and contractors.
- CIP-011-2, Requirement R2 requires entities to implement processes for protecting critical information (i.e., BES Cyber System Information) prior to the reuse or disposal of Cyber Assets.

Given the limitations of Section 215 of the Federal Power Act (FPA), however, additional mandatory NERC Reliability Standards may not be the most efficient and effective way of mitigating supply chain risks. As the Commission recognizes, a Reliability Standard under Section 215 of the FPA has limited applicability. It cannot "directly impose obligations on suppliers, vendors or other entities that provide products or services to registered entities." Many of the actions of suppliers, vendors and other third parties are beyond the control of registered entities and, in turn, the reach of NERC's Reliability Standards. To mitigate supply chain security risks, electric sector participates must work closely with other industry sectors, government partners, and the suppliers of goods and services, and continue to develop, share, and refine existing guidance documents and practices for addressing supply chain management.

Should the Commission direct NERC to develop additional mandatory Reliability Standards to address supply chain risk management, it should:

(1) provide sufficient time for standard development activities to enable NERC to thoroughly consider these issues and engage in educational and outreach efforts, including additional technical conferences and the formation of a task force, as discussed in NERC's NOPR comments, to provide a better understanding of the nature of supply chain risks and the extent to and manner in which a mandatory Reliability Standard can effectively protect against those risks; and

(2) clarify that any such Reliability Standard build on existing protections in the CIP Reliability Standards and the practices of registered entities, and focus primarily on those procedural controls that registered entities can reasonably be expected to implement during the procurement of products and services associated with BES operations to manage supply chain risks.

As discussed in NERC NOPR comments, a supply chain management Reliability Standard could include procedural controls surrounding the need to (1) transact with organizations that meet certain criteria (i.e., only transact with "trusted" suppliers), (2) include cybersecurity procurement language in contracts with suppliers, vendors and contractors for products and services, and (3) review and validate the security practices of suppliers, vendors and contractors,

to the extent possible. A potential approach could be to require registered entities to obtain a certification from a supplier that an independent third party reviewed and endorsed the supplier's supply chain management practices.

Further, the Commission should also stress that the supply chain management Reliability Standard must be flexible to account for: (i) the differences in the needs and characteristics of registered entities; (ii) the diversity of BES system environments, technologies, and risks; and (iii) issues related to the limited applicability of mandatory NERC Reliability Standards.

Thank you for the opportunity to present on these issues today. I look forward to answering any questions.