Supply Chain Data Request

Howard Gugel, Vice President of Engineering and Standards
Informational Webinar
September 23, 2019
Cyber Security Supply Chain Standard

• Background
  - FERC issued Order No. 829 on July 21, 2016
  - NERC Board Approved the Standard in August 2017
  - Standard filed in September 2017
• High and medium impact Bulk Electric System (BES) Cyber Systems
• No requirements for low impact BES Cyber Systems
• NERC committed to addressing risks appropriately
  ▪ Identify best practices
  ▪ Develop guidance resources
  ▪ Support common understanding of compliance obligations
• Support effective and efficient implementation (e.g. CIP V5 transition)

• **Supply chain risk study**

• Communicate supply chain risks to industry

• Forum and association white papers

• Plan to evaluate effectiveness of supply chain standards
Recommendations from Study

• Include in Supply Chain Standards
  ▪ Electronic access controls for medium and high impact BES Cyber Systems
  ▪ Physical access controls for medium and high impact BES Cyber Systems

• Do not include in Supply Chain Standards
  ▪ Electronic access monitoring and logging
  ▪ Physical access monitoring and logging
  ▪ Protected Cyber Assets

• Collect more data on low impact BES Cyber Systems

• Develop guidelines with Critical Infrastructure Protection Committee (CIPC) Supply Chain Working Group
  ▪ Application to lows
  ▪ Evaluation of Protected Cyber Assets (PCAs)
• Developed with Supply Chain Working Group
• Options discussed
  ▪ Collect detailed information on all BES Cyber Assets
  ▪ Collect information based on location
• Draft posted for 20 day comment period
• 35 respondents
• 5 questions
• Many changes made for clarity
• Timing remained the same
• Approved by Board in August
• Issued on August 19
• Responses due October 3
• Applicable to entities in CIP-002-5.1a
• Focused on low impact BES
Summary of Request

- Contact information
- Number of assets containing BES Cyber Systems
  - High/medium impact with External Routable Connectivity (ERC)
  - Medium impact without ERC
  - Low impact
  - Low impact with external connectivity (see CIP-003-7, Attachment 1)
- How you plan to address low impact BES Cyber Systems in supply chain
- Location risk-based survey on low impact BES Cyber Systems
- Question on cost
Next Steps

- Analyze survey responses
- Present summarized results to industry
- Recommend actions, if any, to NERC Board in November
Questions and Answers