# FERC Technical Conference
# Supply Chain Risk Management

## March 2, 2016
## Charlotte, NC / WebEx

**Mike Hagee**
**SERC Security Program Manager - Physical**

# Background

- Notice of Proposed Rulemaking (NOPR) issued July 16, 2015
- FERC directed NERC "…to develop a new or modified Reliability Standard to provide security controls for supply chain management of industrial control system (ICS)…associated with bulk electric system operations."
- Perceived risk based on a 2014 ICS-CERT report on Havex and BlackEnergy malware
- Scope is for the entire product life cycle

# NOPR Parameters

- Only address obligations of the registered entities and not directly impose on suppliers, vendors or other entities that provide products or services
- Not dictate the abrogation or re-negotiation of current contracts with suppliers, vendors or others
- Allow flexibility in how an RE achieves that goal
- Possibly allow for exceptions (safety/operational gaps due to availability)
- Provide enough specificity so that compliance obligations are clear and enforceable

# FERC Technical Conference

- Date: January 28, 2016
- Location: FERC Headquarters, Washington, DC
- Purpose: To facilitate a structured dialogue on supply chain risk management issues
- Structure: Prepared remarks presented by invited panelists
- Attendance: In-person attendance or webcast

# FERC Staff Presentation

- Reviewed Supply Chain Security Efforts by other Federal Agencies:
  - Office of Management and Budget (OMB)
  - Department of Defense (DOD) Interim Rule
  - Department of Energy (DOE)
  - Others (Financial, NIST, NERC
- Summary: Highlighted programs could be used to inform or help guide development of a new or modified Reliability Standard

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

- 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 should be considered to mitigate supply chain risks

# Panel 1

| Panelists | Panelists |
|---|---|
| Utilties Telecom Council | NRECA |
| NIST | Southern Company |
| ISO New England | BitSight Tech |
| MISO | NERC |

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

- Identify types of assets that could be better protected
- Identify supply chain processes that could be better protected
- Identify controls or modifications that could be included in the Standard
- Identify existing mandatory or voluntary standards or guidelines that could form the basis for the standard

# Panel 2: Scope and Implementation of a New or Modified Reliability 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

# Panel 2

| Panelists | Panelists |
|---|---|
| Pepco Holdings | Cisco |
| United Illuminating | OSIsoft |
| WECC | American Electric Power |
| University of Houston | Ontario IESO |

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

- Generally describe how registered entities currently manage supply chain issues
- Identify standards or guidelines that are used to establish supply chain risk management practices
- Identify organizational roles involved in the development of supply chain risk management practices
- Describe approaches for identifying, evaluating, mitigating and monitoring supply chain risk

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

- Describe supply chain risk is addressed in contracting with vendors and suppliers
- Describe the capabilities of registered entities to inspect third party information security practices
- Describe the capabilities that registered entities have to negotiate additional security in their hardware, software and service contracts
- Describe how vendors and suppliers manage risk in their supply chain

# Panel 3

| Panelists | Panelists |
|---|---|
| Southern California Edison | NEMA (National Electrical Manufacturer's Association) |
| Idaho National Labs | Kansas City Power and Light |
| Schweitzer Engineering | Arkansas Electric Cooperative Corporation |
| Waterfall Security Solutions | PJM |

# Summary

- Most panelists agreed that imposing a Standard on registered entities is a costly and ineffective approach
- Many of the panelists noted that there were a wide variety of existing standards, guidelines and best practices on Supply Chain Risk Management that are publicly available and could be leveraged to address the issues
- It was duly noted that Supply Chain Risk Management is a cross-sector and international issue and not just the electric industry

# References

- FERC NOPR on Supply Chain Risk Management
- NIST SP 800-161 Supply Chain Risk Management Practices for Federal Information Systems and Organizations
- Cybersecurity Procurement Language for Energy Delivery Systems (Energy Sector Control Systems Working Group (ESCSWG)
- NEMA Supply Chain Best Practices

# Next Steps

- FERC Staff will aggregate comments and provide the Commission with recommendations or options on how to best address Supply Chain Risk Management issues
- No timetable for next course of action on Supply Chain Risk Management

# Questions?