Electrical Manufacturers’ Role in Cyber Supply Chain Risk Management

NIST Cybersecurity Risk Management Conference
Agenda

• Introduction and Overview of NEMA
• NEMA’s Supply Chain Best Practices
• NEMA’s Cyber Hygiene Document
• Summary & Key Takeaways
Who is NEMA?
Mission

Help Member Companies….

- Expand market opportunities
- Mitigate barriers and costs
- Enhance business performance

By…

- Developing Standards and promoting code adoption and use
- Advocating for Members and their products
- Providing exclusive industry data, customized research and economic forecasts
- Educating Members on evolving technologies, industry trends and legislative/regulatory conditions
The NEMA Ecosystem

Standards Advocacy Business Intelligence

- Industrial Products and Systems
- Transportation Systems
- Utility Products and Systems
- Lighting Systems
- Building Systems
- Building Infrastructure
NEMA’s Supply Chain Best Practices
Purpose

• Identify a set of industry best practices and guidelines for manufacturers to implement during product development

• Minimize possibility that bugs, malware, viruses, other exploits that can be used to negatively impact product operation

• Not intended to be all-inclusive
  o Makes references to other documents for more information
Document Layout

• Introduction, Scope, Definitions

• Best Practices- Four Product Life Cycle Phases
  o Description of Product Life Cycle Phase
  o Identification of Threats and Analysis of Their Implications
  o Reference Documents
  o Manufacturers Recommendation
Manufacturing and Assembly

• Detect and eliminate anomalies in the embedded components
  o Evaluate component versions-malware analysis
  o Where technically feasible-code signing
  o Documented design and purchasing process
Tamper Proofing

- Configuration of manufactured device can’t be altered from the production line to the operating environment
  - Tamper resistant coatings or seals
  - O/S with minimal kernel features and reduced application sets
  - Disabling unsecure communications (i.e. FTP, TFTP, and Telnet)
  - Secure-by-default protocols
Security Development Life Cycle

• Manufactured device complies with security requirements of the operating environment.
  o Documented configuration management process
  o Consider 3rd party quality assurance audits
  o Company risk management system
  o Incident or event management plan
  o Tight communication channels- both upstream and downstream
Revocation and Decommissioning

- Processes to prevent obsolete/discontinued devices from being used to penetrate active networks
  - Purging/sanitization techniques
  - Physical destruction/disposition
  - Consider penetration testing
Alignment with Portions of Siemens Charter of Trust

• Responsibility throughout the digital supply chain
  o Identity and access management
  o Encryption
  o Continuous protection

NEMA’s Cyber Hygiene Document
NEMA’s Cyber Hygiene Best Practices Document

- Identify a set of industry best practices and guidelines to increase cybersecurity sophistication
- For electrical equipment and medical imaging manufacturers in their manufacturing facility and engineering processes
  - Not intended to specify product features
- Not intended to be all-inclusive
  - Makes references to other documents for more information
Fundamental Principles

- Segmenting Networks
- Understanding Data Types & Flows
- Hardening Devices
- Monitoring Devices and Systems
- User Management
- Hardening Devices
- Updating Devices
- Providing a Recovery Plan or Escalation Process
Summary and Key Takeaways
Summary and Key Takeaways

• NEMA Members understand their important role
  o Cyber supply chain risk management
  o Cyber hygiene within their manufacturing facilities

• Standards and best practices should be industry-developed
  o Government collaboration-enhance security and drive innovation

• NEMA and its Members will continue to be a resource
  o Future work project addressing cyber hygiene from the end-user/application perspective
Document Links:
https://www.nema.org/Standards/Pages/Supply-Chain-Best-Practices.aspx
https://www.nema.org/Standards/Pages/Cyber-Hygiene-Best-Practices.aspx

Questions?
Steve Griffith
Industry Director, PMP
NEMA Transportation Systems Division
Steve.Griffith@nema.org