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

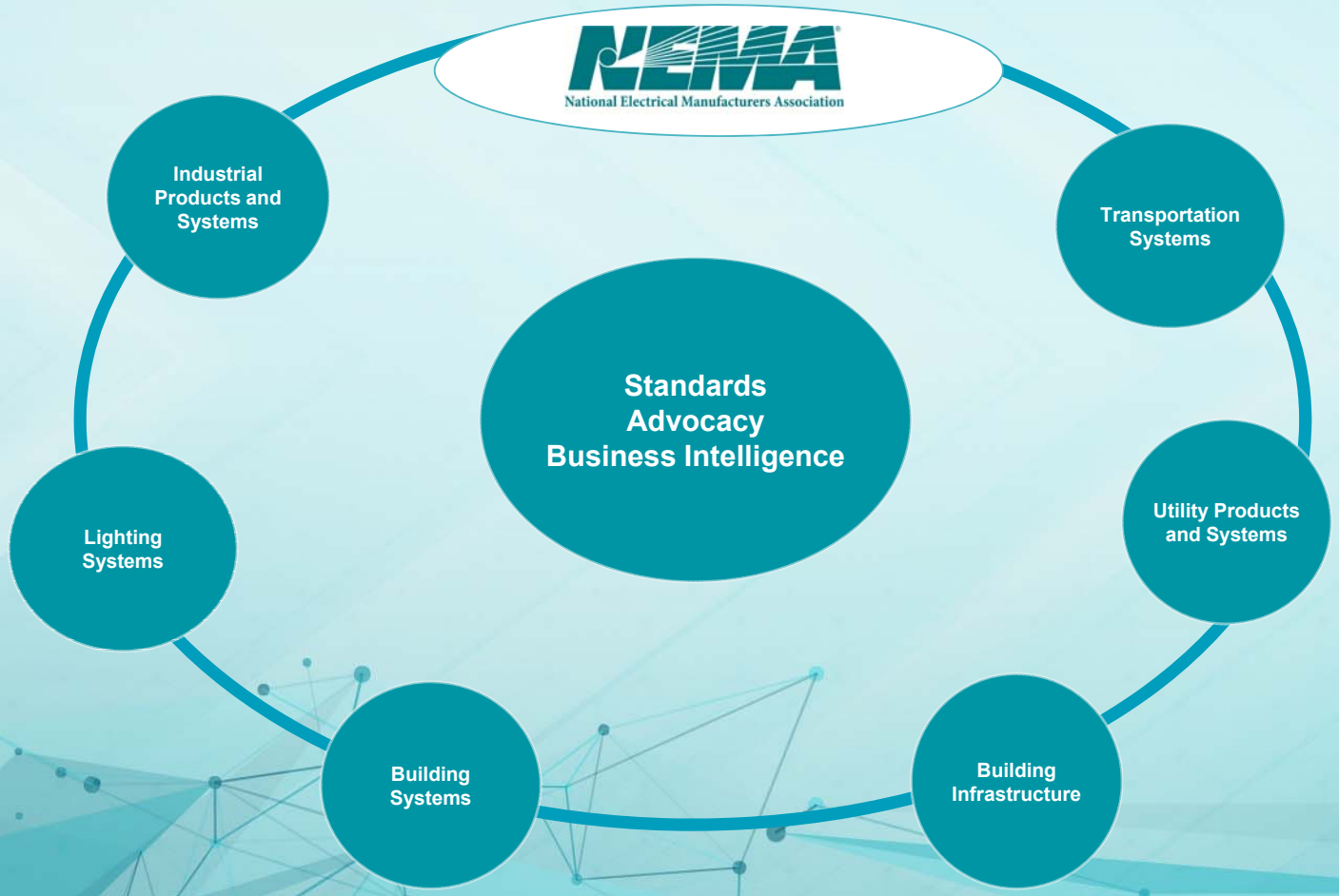
Help Member Companies….

- 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



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
  - Makes references to other documents for more information

Document Layout

- Introduction, Scope, Definitions
- Best Practices- Four Product Life Cycle Phases
  - Description of Product Life Cycle Phase
  - Identification of Threats and Analysis of Their Implications
  - Reference Documents
  - Manufacturers Recommendation

Manufacturing and Assembly

- Detect and eliminate anomalies in the embedded components
  - Evaluate component versions-malware analysis
  - Where technically feasible-code signing
  - 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.
  - Documented configuration management process
  - Consider 3rd party quality assurance audits
  - Company risk management system
  - Incident or event management plan
  - 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
  - Identity and access management
  - Encryption
  - Continuous protection

https://www.siemens.com/content/dam/webassetpool/mam/tag-siemens-com/smdb/corporate-core/topic-areas/digitalization/cybersecurity/shi-13378-cot-dok-narrative-online-2018-02-13-sbi-en.pdf

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
  - Cyber supply chain risk management
  - Cyber hygiene within their manufacturing facilities
- Standards and best practices should be industry-developed
  - Government collaboration-enhance security and drive innovation
- NEMA and its Members will continue to be a resource
  - 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