2016
PUBLIC-PRIVATE
ANALYTIC EXCHANGE PROGRAM

2016 Public-Private Analytic Exchange Program

Identifying and Mitigating Supply Chain Risks in the Electricity Infrastructure's Production and Distribution Networks

Identifying and Mitigating Supply Chain Risks in the Electricity Infrastructure's Production and Distribution Networks

The Problem

America's electricity infrastructure is rapidly evolving as new technologies and business models are inserted into a grid that hasn't seen substantive changes since the early 20th century. Government investment in technologies is accelerating the rate of change as well as business models that improve reliability and promote economic development. However defining requirements and furthering research to secure the future supply chains for these technologies rarely takes place, despite known vulnerabilities of globalization and threats from potentially hostile adversaries. In short, without change, the attack surface of the evolving grid will broaden even as security risk mitigation falls behind.

The Answer

One answer is to synchronize policies to incentivize business and economic development in response to supply chain security shortfalls. Along with funding new business models and innovative technologies required by the new grid, investors – government and industry – need to incorporate requirements that address inherent supply chain risks. The electricity infrastructure must move away from a reactive paradigm towards a proactive model that acknowledges and mitigates inherent and potentially introduced supply chain risks.

The Dilemma

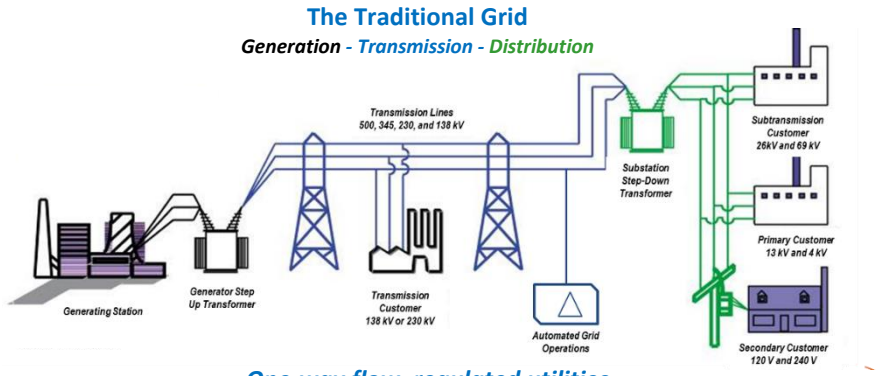
Two key impediments exist to implementing this approach.

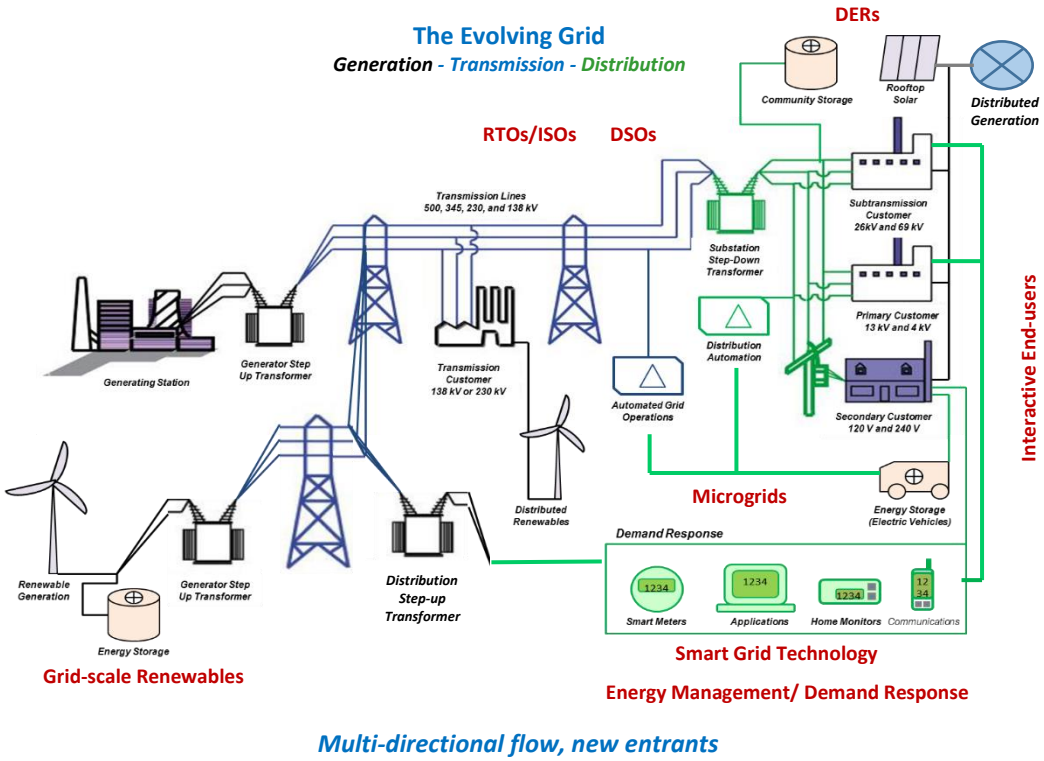
Not all parts of the electricity infrastructure are equally regulated. This creates a diffuse bureaucracy that provides inconsistent direction and regulation of the existing grid. This results in inconsistent requirements and oversight. On a practical level, this has also resulted in electricity infrastructure entities treating supply chain risks inconsistently.

Second, both industry and end consumers are influenced by cost and environmental interests. New technologies respond to both these goals, however, these improvements present a potential risk. As creation and consumption of electric power becomes more dependent on renewable resources, production and demand are increasingly balanced through real-time flow

of usage information. The attack surface may increase given the intermittent nature of renewable energy, generation of power at all stages of the system, and the use of the internet to track, communicate, and control usage.

The security challenge posed by transformation of the electricity infrastructure's grid – a 20th century unidirectional system with relatively linear generation, transmission, and distribution that is evolving into a 21st century multidirectional system with non-linear generation and complex distribution – is exemplified in the following graphics.





The AEP team interviewed representatives from electricity infrastructure industry and academia, as well as government officials at the federal and state levels, national laboratories, and government and non-government regulators to better understand the tensions inherent between rapidly evolving the grid and securing supply chain risks. The team identified the following Key Findings as areas of concern for the supply chain of the future electric infrastructure.

Supply Chain Risk Key Findings

- The supply chain for the electricity infrastructure is **increasingly attractive as a threat vector** due to global outsourcing and resulting lack of visibility into the sources of component parts and services. Vulnerabilities may be inherent – pre-existing, some known and others unknown – or introduced by hostile actors.
- Sophisticated threat actors may employ **blended attacks** involving some combination of insider access, cyber intrusion, and technical access.
- Sophisticated threat actor objectives range from **theft** of intellectual property and sensitive information, through **misappropriation** of system controls, to – worst case – **sabotage** of system operations.

Evolving Grid Key Findings

- The ongoing evolution of the electricity infrastructure grid from a localized, luxury convenience of the early 20th century into a service embedded in the fabric of modern life requires that the **supply chain for the electric grid be considered a critical element** of overall risk management.
- Adoption of **new technologies** and business models is **driving changes throughout** the grid – generation, transmission, distribution, and consumption.
- In particular, internet-enabled technology provides the greatest benefit to all players within the grid, but may introduce additional vulnerabilities into the system. Thus, this **technology is expanding the potential attack surface**.

Roles and Responsibilities Key Findings

- USG does not speak with one voice. Supply chain risk management is **hampered by unsynchronized research, policy, and financial incentives**.
- **Regulation is broad, diffuse and not comprehensive**. For example, FERC mandates do not cover the entire grid (i.e. not applicable to TVA, cooperatives, or nuclear power plants).
- Research initiatives do not address supply chain risk management as a design or technical constraint.
- **Financial incentives** to modernize the grid are **not linked to security outcomes**.

Based on what the team discovered, the following recommendations are provided, grouped by which entity the team believed was best positioned to enact these changes.

Recommendations for Government

- Continue to use existing organizations and authorities, but **prioritize SCRM at all levels** – Federal, Regulatory, State, and Industry.
- **Emphasize incentives for SCRM compliance** – "more carrots, less stick".
- Recommend **study of supply chain risks from self-regulated or unregulated elements** of the electricity infrastructure (such as cooperatives, behind the meter technologies, etc.).
- **Future legislation** concerning the electricity infrastructure should **incorporate supply chain** considerations.

Recommendations for Industry

- **Implement the Cyber Security Capability Maturity Model** across the Electricity Infrastructure.
- Electricity infrastructure members must **incorporate specific supply chain requirements in contract language** and monitor compliance.

Recommendations for Public-Private Partnership

- **Improve information sharing** and industry best practices.
- **Synchronize business and economic development** and financial incentives **with supply chain risk requirements**.

For further insight and engagement, contact the 2016 AEP Electricity Infrastructure Supply Chain Risk Team Champion:

Office of the Director of National Intelligence
National Counterintelligence and Security Center
Supply Chain Directorate
301-243-0120

Acknowledgement

We would like to acknowledge and extend our appreciation to the government agencies, companies, academic institutions, and individuals that supported development of this paper.

This paper could not have been developed without the support of the Office of the Director of National Intelligence and the Department of Homeland Security. We thank these sponsors for the opportunity to have participated in the 2016 Public-Private Analytic Exchange Program.

Individuals and Organizations Consulted

- Dr. Stephen Flynn, Kostas Research Institute for Homeland Security, Northeastern University
- Dr. Ranaan Miller, Executive Director MIT Energy Initiative, Utilities of the Future Study, Massachusetts Institute of Technology
- Prof. William Hogan, Raymond Plank Professor of Global Energy Policy, John F. Kennedy School of Government, Harvard University
- Ms. Judith Judson, Commissioner, Massachusetts Department of Energy Resources
- Mr. Bridger McGaw, AthenaHealth Inc.
- Representatives from ISO-New England
- Representatives from National Grid New England PLC
- Representatives from Eversource Energy Inc.
- Representatives from EnerNOC Inc.
- Representatives from Veolia North American Technologies Inc.
- Representatives from Schweitzer Engineering Laboratories Inc.
- Representatives from the American Petroleum Institute
- Mr. David Howard, Office of Electricity Delivery and Energy Reliability, U.S. Department of Energy
- Representatives from Pacific Northwest National Laboratory, U.S. Department of Energy
- Representatives from Idaho National Laboratory, U.S. Department of Energy
- Representatives from the National Institute of Standards and Technology, U.S. Department of Commerce

Team Members

- Office of the Director of National Intelligence, National Counterintelligence and Security Center, Supply Chain Directorate
- Tanya Bodell, Executive Director, Energyzt Advisors, LLC
- Dr. Michael Cohen, Principal Critical Infrastructure Security Engineer, MITRE Corp.
- Wesley Lammers, IT and Risk Management Analyst, Xcel Energy Inc.
- Christopher Ruemke, Economist, Commodity Futures Trading Commission
- Orlando Stevenson, Cybersecurity Analyst, North American Electric Reliability Corp.

All judgments and assessments are solely based on unclassified sources and are the product of joint public and USG efforts.