

# Securing Battery Energy Storage Systems from Cyberthreats

## BEST PRACTICES AND TRENDS

### WEBINAR PRESENTATION

PETER FOX-PENNER, THE BRATTLE GROUP

PHIL TONKIN, DRAGOS

HARRY KREJSA, CARNEGIE MELLON INSTITUTE  
FOR STRATEGY & TECHNOLOGY (MODERATOR)

DECEMBER 9, 2025



# Presenters

---



Peter Fox-Penner

**THE BRATTLE GROUP**

PFoxP@brattle.com



Phil Tonkin

**DRAGOS**

PTonkin@dragos.com



Harry Krejsa

**CARNEGIE MELLON**



harrykrejsa@cmu.edu

**Securing Battery Energy Storage Systems from Cyberthreats**

**BEST PRACTICES AND TRENDS**

**PREPARED BY**  
Peter Fox-Penner, The Brattle Group  
Phil Tonkin, Dragos  
Justin Pascale, Dragos  
Noah Rauschkolb, The Brattle Group  
Purvaansh Lohiya, The Brattle Group

December 2025



Sponsored by Fluence. [Link.](#)

# Agenda

---

- Introduction - Harry Krejsa
- Presentation of report findings - Brattle and Dragos
- Audience Q&A
- Closing remarks – Harry Krejsa

# Opening Remarks: Harry Krejsa



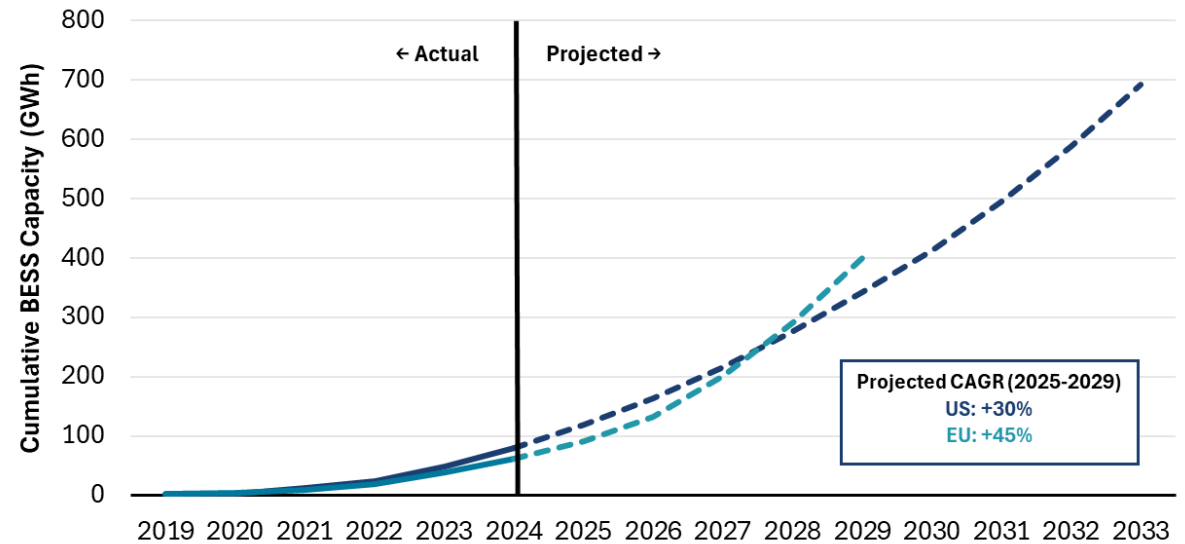
# Report Presentation - Introduction



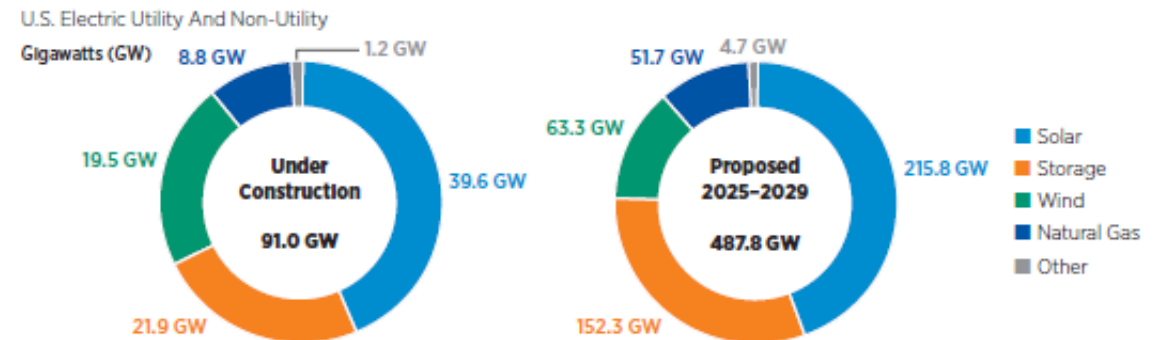
# Importance and Growth of BESS

- Battery Energy Storage Systems (BESS) provide **capacity, flexibility, and fast response** to support the functioning of the US electric power system
- Batteries **improve grid reliability and stability** and **improve the utilization of low-cost clean generation**
- Global utility scale **BESS deployment is growing rapidly** across the US, EU, and Asia
- Utility scale BESS capacity is **projected to grow 8X in EU by 2030 and more than 3x in US by 2033**
  - Storage is expected to comprise about one-third of US capacity additions 2025-2029

### Historic/Projected Growth Of Battery Energy Storage Capacity



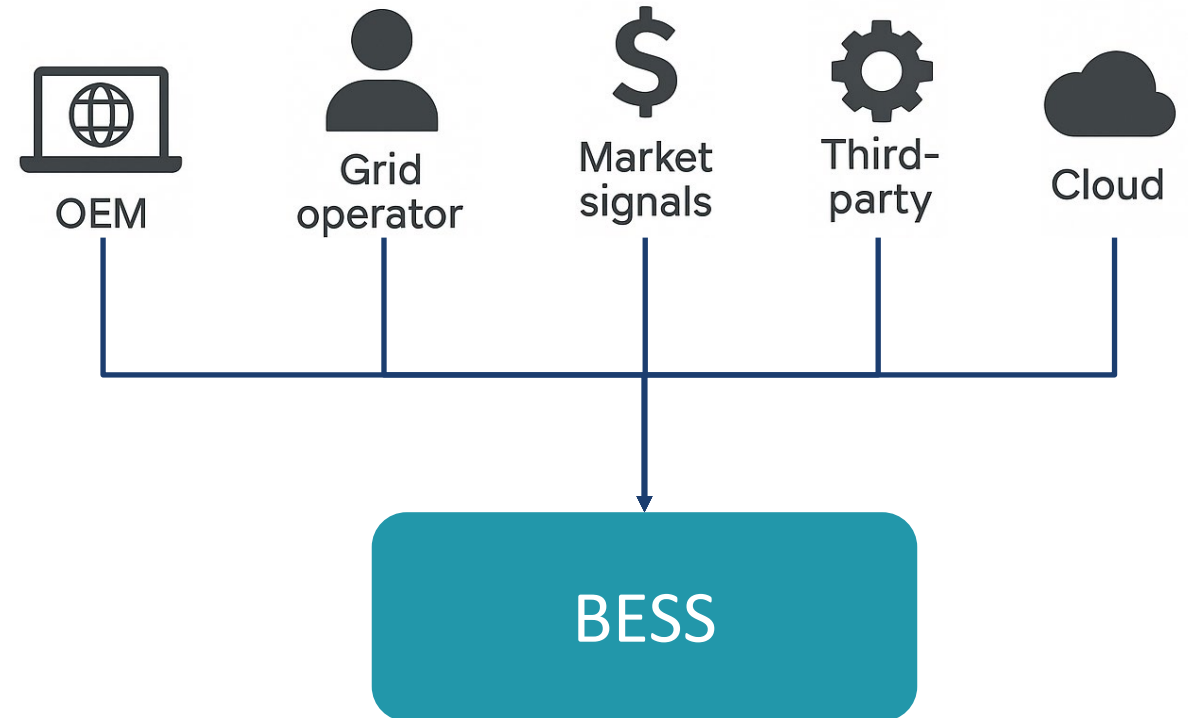
### STAGE OF ANNOUNCED CAPACITY ADDITIONS 2025-2029



Under Construction status also includes Site Prep and Testing; Proposed status also includes Feasibility, Application Pending, and Permitted. Data includes new plants and expansions of existing plants, including nuclear updates. Includes projects with an expected online date up to 2029. Source: Velocity Suite (Hitachi Energy), April 2025

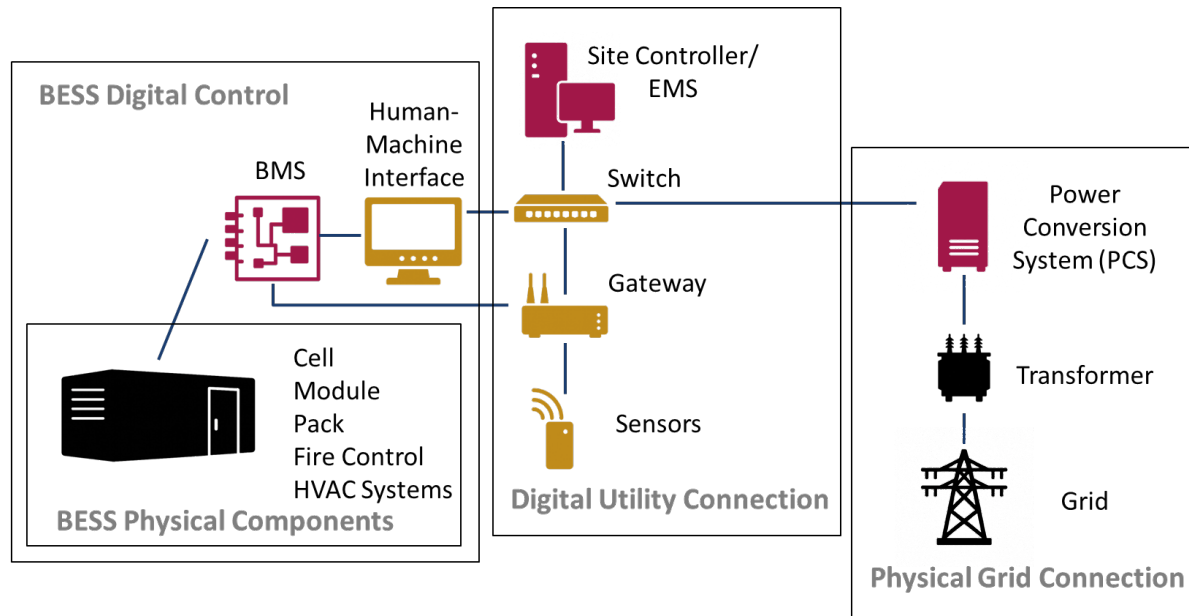
# Why BESS Cybersecurity?

- BESS is becoming a **critical full-scale resource in modern power systems**, not a peripheral asset
- Highly digitized, remotely managed systems create **many potential intrusion pathways**
- Standardized designs and common components **increase the impact of a single intrusion strategy**
- Cyber incidents can cause **major revenue losses, capital damage, and extended outages**
- Large scale BESS failures can trigger **regional grid instability and national security risks**



# Major Components of a Battery Energy System

**Components of a Modern Battery Energy Storage System (DC Block Structure)**

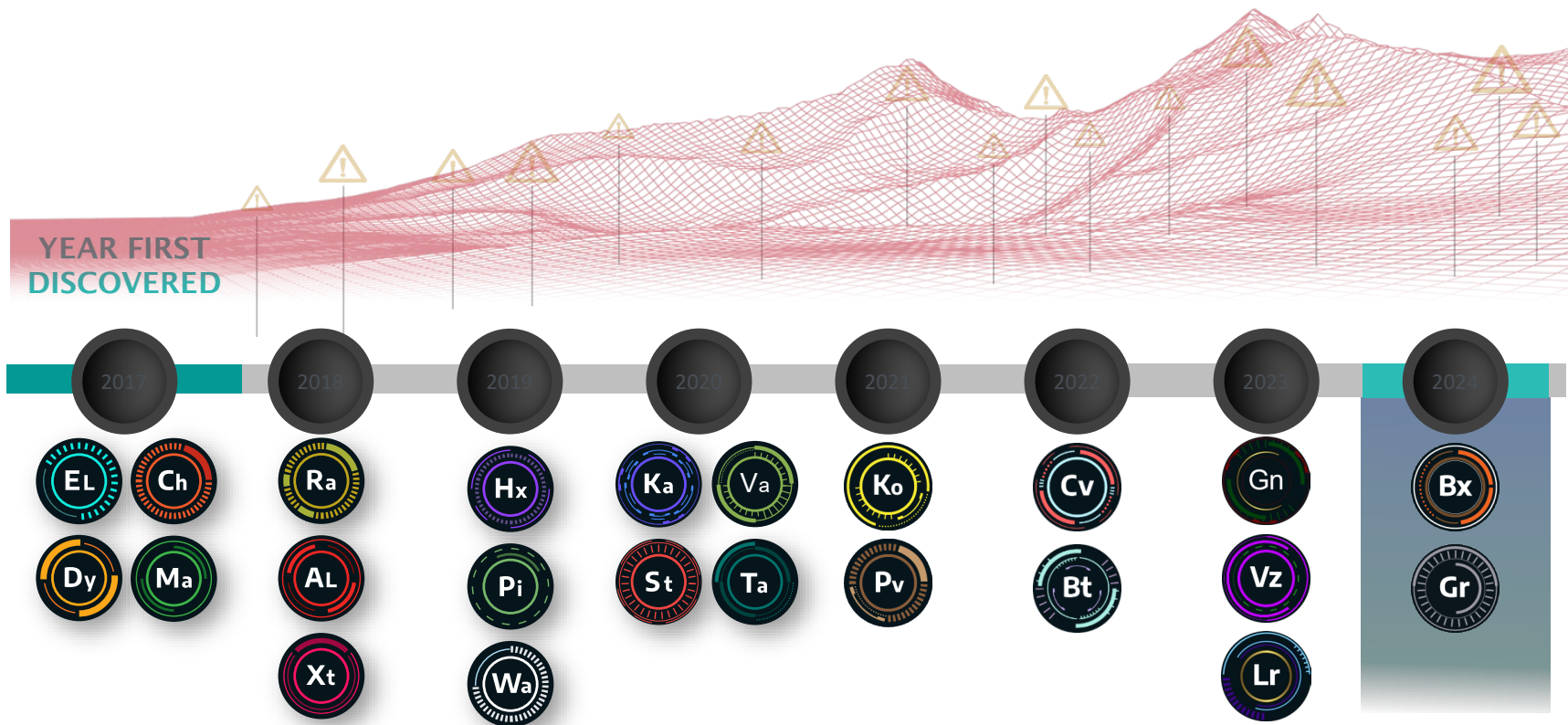


- **Core elements:** Battery cells and packs, power conversion systems, and transformers
- **Control stack:** BMS, EMS, human machine interfaces, and digital utility connections
- **Supporting systems:** HVAC, fire suppression, and physical security infrastructure
- Cyber risk is concentrated in “smart” components with embedded software and connectivity
- **PCS, BMS, EMS, inverters, networking gear, and remote access interfaces (colored red and yellow in chart at left) are the most vulnerable to intrusion.**

# **Report Section II: Threat Landscape and Impacts**



# Tracking OT Threats



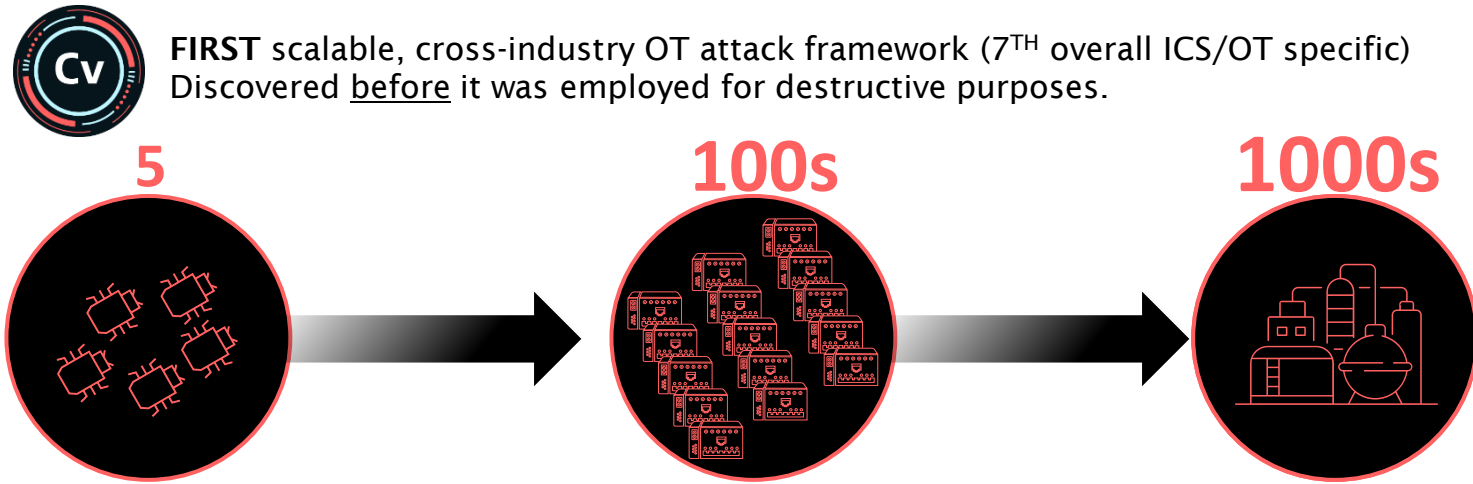
# Homogenous Technology

Operational Technology has moved from heterogenous systems to using shared technologies and patterns between industries, as addition to sharing between IT and OT

Advantages for efficiency can be advantages to the adversary



# Tracking OT Threats



**FIRST** scalable, cross-industry OT attack framework (7<sup>TH</sup> overall ICS/OT specific)  
Discovered before it was employed for destructive purposes.

CAPABLE OF DISRUPTIVE & DESTRUCTIVE ICS CYBER ATTACKS

## Magnitude of Potential Harm

**BESS cyber incidents can result in plant outages and even cause regional blackouts with major economic, social, and national security impacts**

- Forced outages for a 100 MW, 4-hour BESS can cause about **\$400,000–\$1.2 million in monthly revenue loss per asset**
  - Permanent damage to a BESS can create **capital losses an order of magnitude larger** than outage-related revenue losses
- Societal costs are much larger: In ERCOT, a 16-hour outage can impose more than **\$13,000 per-MWh in value of lost load on customers**
  - A scenario with 100,000 customers losing 3,000 MWh can cost **~\$43 million in economic losses in a single day**
- **Long lead times** for key components, including transformers (up to 36 months), can **greatly extend restoration time**



# **Report Section III: Emerging Regulatory Trends**



# Emerging Regulatory Trends in the US

## Growing Focus on Foreign Entities of Concern and Supply Chains

- Successive Biden and Trump administrations have adopted an increasingly **cautious posture toward Chinese and other adversarial suppliers** (Russia, Iran, North Korea)
- A series of executive orders and agency rules **increasingly target “foreign adversaries”** and connected technologies in critical infrastructure, including BESS systems
- Recent legislation and proposals (including the IRA, OBBBA and the Decoupling from Foreign Adversarial Battery Dependence Act) **limit tax benefits and federal support for projects using components from specified countries**
- **New requests for executive action** from Congressional committees and members:
  - In October, five committee chairs led by Rep. Moolenaar urged the Dept. of Commerce to **expand national-security restrictions on many technologies, including BESS, and named two Chinese suppliers to investigate**
  - In November, Rep. Pfluger wrote a letter warning that **Chinese-made solar and battery inverters threaten US security and should be blocked from energy infrastructure**
- **Further federal actions** that restrict BESS components, control systems, and related technologies from Chinese entities seem likely over time

# Emerging Trends in the US

---

## Evolving Federal, State, and Industry Roles

- As noted in last slide, US policy is **shifting from trade tools to more direct cyber and supply chain controls for critical infrastructure**
- NERC CIP standards and FERC directives are **expanding to address inverter-based and storage resources**
  - In September, FERC approved NERC CIP-015-1, requiring **internal network security monitoring** for high- and medium-impact assets connected to the BES<sup>1</sup>
  - FERC also proposed to approve an expansion of CIP-003-11 (Security Management Controls) to apply to **all assets connected to the bulk electric system (BES)** (rather than just high- and medium-impact assets), thereby enhancing security and privacy controls for all parts of the system<sup>2</sup>
- **States are emerging as active cybersecurity regulators**, creating cyber integration centers, grid security councils, and “cyber commands”
- State laws such as Texas’s Lone Star Infrastructure Protection Act and Georgia’s SB 346 **restrict FEOC-linked entities from critical infrastructure and state contracts**
- Industry and voluntary standards are becoming more prevalent, but **experts see a need for prescriptive, “secure by design” requirements** and financial incentives to drive higher levels of protection

1. <https://www.federalregister.gov/documents/2025/07/02/2025-12309/critical-infrastructure-protection-reliability-standard-cip-015-1-cyber-security-internal-network>.

2. <https://www.federalregister.gov/documents/2025/09/23/2025-18396/critical-infrastructure-protection-reliability-standard-cip-003-11-cyber-security-security>.

# Emerging Trends in Europe

---

## Fragmentation, Foreign Dependence, and Tech Sovereignty

- National implementation of EU rules is uneven, creating a **patchwork of cybersecurity practices** across an interconnected grid
- **Some member states maintain close ties with Chinese vendors**, while **others restrict or ban Chinese technology** in energy infrastructure. This divergence creates **inconsistent protection, higher compliance costs, and systemic exposure** across the European power network
- **EU industrial policy seeks to pair decarbonization targets with “tech sovereignty,”** but dependence on Chinese components in BESS and grid edge technologies remains high
- Compared to the more prescriptive regimes (for example Australia’s AESCF), the EU approach still relies heavily on operator-driven risk management rather than detailed technical controls

# Emerging Trends in Europe

---

## Despite fragmentation, significant movement in EU Cyber Directives and Regulation

### Updating occurring on all three major enactments:

- Network and Information Security Directive (NIS-2)
- Cyber Resilience Act (CRA)
- Cyber Security Act (CSA)
- **NIS2 is expanding cybersecurity obligations to more sectors and smaller BESS installations**
  - **Asset owners must demonstrate that their controls are “defendable” under attack**, with responsibility placed squarely on operators
  - 15 out of 27 EU Member States have incorporated the NIS2 directive into their national law
- The CRA will require all products with digital elements, including BESS components, **to meet EU cybersecurity standards and lifecycle support by 2027**
- In advance of 2027 implementation, EU has launched **coordinated risk assessments** for additional critical sectors, including solar PV and wind, and may expand to include BESS
- Ongoing updates to the EU Cybersecurity Act aim to **strengthen the mandate and tools of the EU cybersecurity agency - proposal due in January 2026**

# **Report Section IV: Recommendations for Action**



# Mitigating the Threats



- 01** Establish **firm contractual requirements for patching, vulnerability disclosure, and long-term support**

---

- 02** Build **defensible architectures** with segmentation, strong perimeters, and safe shutdown modes

---

- 03** Maintain **continuous network monitoring** to detect abnormal behavior

---

- 04** Enforce **secure remote access** with role-based controls, MFA, logging, and dedicated workstations

---

- 05** Require **verified HBOMs and SBOMs** for critical components and **enforce secure development practices**

---

- 06** **Integrate cybersecurity during design and procurement** to avoid costly retrofits

# **Report Section V: Conclusions**



# Conclusion

---

**Proactive, lifecycle cybersecurity is essential to protect revenue, assets, and grid stability**

- Global Battery Energy Storage System (BESS) deployment is accelerating and expanding the importance of **secure, resilient storage assets**
- Cyber threats to BESS are increasing due to **standardization, remote access pathways, and foreign sourced components**
- US and EU policymakers are moving toward **stricter supply chain and cybersecurity requirements**
- **BESS developers, owners, and operators, as well as other electric system stakeholders, should consider the measures discussed in our report**



**Secure  
Technology**



**Secure  
Supply Chain**



**Secure Regulations  
& Governance**

**Q & A**

