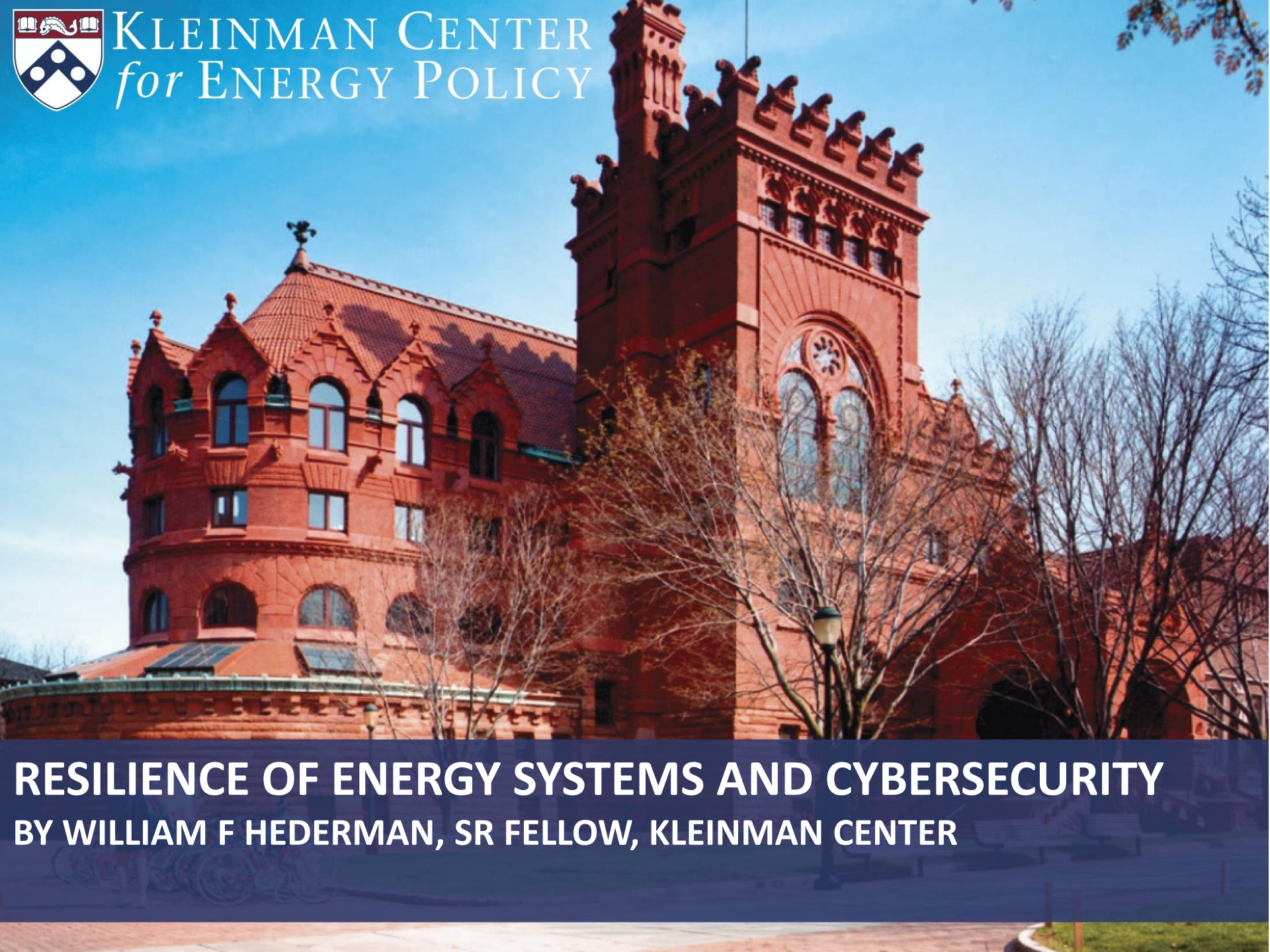

RESILIENCE OF ENERGY SYSTEMS AND CYBERSECURITY

BY WILLIAM F HEDERMAN, SR FELLOW, KLEINMAN CENTER

Presentation to

USEA Technology Briefing: What does "Resilience" of the Electric Power Sector mean today?

- hederman@alum.mit.edu (best contact)
- Washington, DC
- October 31, 2018

Purpose

- Explore two significant and simultaneous issues related to resilience:
  - Increased threat of cyber attacks on the grid and related assets.
  - Increased opportunities and challenges posed by the advancement of Distributed Energy Resources (DER).

Current Situation

- North American Electric Grid has become a major asset of national security.
  - Roles and Responsibilities for cybersecurity in the power secure are not well-defined.
- Cyber situation
  - Adversaries (nation-state and criminal) are pursuing increasingly powerful and persistent attacks.
  - Significant defensive efforts have, to date, averted major disruptions.
- DER situation
  - Increasing penetration of distribution systems by DER devices and support controls and related software.
  - Provides potential enhancement to system resilience.
  - Distribution oversight remains largely outside of federal regulatory scrutiny.
  - State-level oversight, interest and capability vary significantly among states.

Roadmap to highly secure and integrated grid: Strategic Goals

- Strengthen cybersecurity to a level that reduces foreseeable threats and consequent damage to acceptable levels.
- Specify key tradeoffs with the most quantitative detail possible.
- Encourage each set of stakeholders to prepare for gathering to discuss relevant issues and to make necessary compromises.
- Get these conversations to begin (perhaps at USEA).

Proposed Destination: A 21st Century Grid

Priorities:

- Reliability
- Security
- Safety
- Resilience
- Environmental acceptability
- Affordability

Important Partners on this road

- Utilities (public/private, electric/gas/telecom/water)
- Vendors
- Product developers (hardware and software)
- Customers (I/C/R)
- Regulators (federal/state, economic/environmental/reliability/other)
- Public accountancy auditors
- Other governmental entities
- NGOs and other citizens

Potential New Key Participants

- INPO or INPO-like organization
- UL or UL-like organization
- CCRO or CCRO-like organization
- Cyber monitoring unit(s), like MMUs, with responsibility for a State of Grid Cybersecurity Report (annual, classified and unclassified)
- One or more Stakeholders Forums

Succeeding through Collaboration

- Practice, practice, practice
- Outreach (e.g., FBI, local law enforcement)
- Apply the utility tradition of mutual assistance
- Vendor inclusion wherever possible (they consider themselves left out today).
- Discussions of classified material requires security clearances (and clearances require significant lead times). Classified materials also require special handing.

Illustrative Dilemmas to Discuss Early

Cost	v.	Security
Openness/ Information availability	v.	Security
Improve resilience	v.	Endanger reliability (DER?)
Collaboration	v.	Leadership
Herding	v.	Boldness
Standards	v.	Innovation/ Diversity
Diversity	v.	Scale economies
Flexibility	v.	Uniformity
Specific directives	v.	Technology neutral decisions
Manual controls	v.	Automated controls
Duplication	v.	Innovation
Harmonization	v.	Control
Protection through classification	v.	Broad sharing of information
Big Data	v.	Privacy

Related important Topics for early consideration

- How can PUCs best fulfill their key roles?
- Who is currently responsible for what aspects of cybersecurity?
- Are current roles and responsibilities appropriate?

Best (and other) Practices

- Illustrative spectrum of security engagement:
  - None
  - Token/Minimal
  - Compliant*
  - Typical/Standard*
  - Best (current)
  - Advanced/Leading
  - Ideal

* Asterisk indicates a minimal level of competency, probably approximate to one of these levels of practice, would be required for participation beyond the observer levels in roadmap development.

Key Dimensions of Risk Management

- Threat analysis/assessment
- Vulnerability assessment
- Probabilities of attack/attack success
- Calculations of effects/ damage potential
- Plans for continuity of business and services

Risk Management Process

- Identify: relevant assets, systems, networks.
- Assess: threats, vulnerabilities, probabilities, effects.
- Specify: risk preferences, security requirements.
- Select: security controls/measures.
- Implement/execute: selected measures.
- Assess: effectiveness of implemented measures.
- Authorize: standards from successful measures.
- Revise: unsuccessful measures
- Continue: monitoring, assessment, reporting

State PUCs

- Have significant responsibilities for IOU investments in cybersecurity.
- Vary greatly in stance with regard to cyber threats and DER.
- Many are not adequately prepared to oversee, direct, develop, or enforce cybersecurity rules.
- USDOE and other federal agencies sometimes seek to enhance PUC capabilities with funding.
- Maturity classification could assist PUCs.

Illustrative Options to Address Cyber Threats to Reliability

- Integrate grid physics into decision algorithms. Allow no damaging actions/instructions.
- Upgrade authentication of instructions received.
- Educate workforce regarding importance of cyber hygiene. Include 3rd party verification of effectiveness of education.
- Update communications/connections with NERC, FERC, PUC.

Options to Address Cyber Threats to Resilience

- Develop and practice table-top and broader exercises to prepare for responding to attacks.
- Update mutual assurance agreements to cover contingencies possible created by cyber attacks (including pre-attack information sharing).

Distributed Energy Resources (DER)

- Include the following: distributed generation (dispatchable and non-dispatchable), demand side resources, and associated support equipment and software.
- Two-way real time communications is often essential for operations to remain reliable while incorporating DER.
- The many AMI resources rushed to the grid through the ARRA introduced significant security challenges.
- Include supply chain issues.

Identification of Appropriate Practices for Cybersecurity

- NIST, core associations, leading CPA auditors [WH COI alert]
- Explore application of a formalized maturity assessment program regarding cybersecurity practices – for utilities and all in grid supply chains.
- Industry can work with PUCs to determine two or three maturity levels that PUCs could use (e.g., minimum acceptable, recommended, best practice, maximum reimbursed).

Next Steps

- Proceed to develop the advanced technology solutions.
- Proceed to collaborative meetings on a voluntary, mutual assistance basis.
- We are in a “Hidden War” and action is necessary now.