

**DOE/FERC Technical Conference (Security Investments for Energy Infrastructure)
March 28, 2019T.J. Galloway Remarks**

Introduction

Chairman, Commissioners, and senior FERC staff. Thank you for inviting me to participate in today's panel on the important topics of **cyber and physical security, best practices, and industry and government engagement**.

My name is Tom Galloway, and I am president and CEO of the North American Transmission Forum.

The Forum is a voluntary, non-profit membership consisting of about 90 transmission companies located in the United States and Canada. Together, Forum members account for about 85% of the U.S. and Canadian high voltage circuit miles and peak load.

The Forum's mission is to promote **excellence** in the operation of the electric transmission system. We do this by sharing timely and detailed information, including best practices, as well as fostering continuous improvement.

Resiliency (All Hazards, Including Cyber and Physical Security)

In 2013, Forum members made the deliberate decision to add *resiliency* to our mission statement. We view reliability and resiliency as closely related but different concepts.

Reliability relates to the transmission system's ability to perform within a defined set of parameters for a designed set of contingencies, whereas resiliency is the ability to withstand and recover rapidly from severe system events. We use an "all hazards" approach to resiliency, which includes cyber and physical security. We have divided activities into three principal phases: prepare for, operate through, and recover from each of the hazards.

Since 2013, the Forum and EPRI have jointly run one or more annual resiliency summits on key topics, including severe weather impacts and storm hardening; resilient system design; security, EMP, and GMD threats; cross-sector dependencies and coordination; and restoration practices, training, and drills.

Our next summit is scheduled for April 3-4 and will include attendance by FERC staff and remarks by Director of the Office of Energy Infrastructure Security Joe McClelland.

NATF Cyber and Physical Security Activities

Beyond conducting summits, we have been active enhancing member cyber and physical security in other ways, including:

- Developing and maintaining security "Principles of Excellence," which go beyond mandatory compliance
- Conducting about a dozen detailed peer reviews annually, including review of the host member's security performance using the Principles of Excellence as the criteria
- Assisting members (via small, focused, highly qualified teams) on a variety of security topics

- Developing a range of best practice and reference documents, such as CIP-014 guidance for determination of critical assets to help member's prioritize physical security activities
- Conducting webinars on key resiliency and security topics, such as key spare parts, incident command structure, substation physical security, and planning for resilience

Key Projects

In addition to routine, programmatic activities, the Forum has undertaken several key projects related to resiliency and security.

Supplemental Operating Strategies (SOS) – At the request of the Electric Subsector Coordinating Council (or ESCC), Forum members identified key capabilities and associated strategies to allow manual operation of the grid given a large-scale loss of situational awareness tools. Subsequent project phases will further analyze capabilities given a coincident loss of certain physical assets.

Grid Security Emergencies (GSE) – Upon Presidential declaration of an GSE, the Secretary of Energy is authorized to direct grid operators to take certain actions to protect and preserve grid reliability and resiliency. The Forum has been working with the Department of Energy, Electricity Information Sharing and Analysis Center (E-ISAC), and others to develop a framework such that those orders can be optimized, in general and specifically for various relevant scenarios.

Supply Chain Cyber Security – The Forum is developing frameworks and criteria for member use to help ensure cyber security of key equipment, including energy management systems and protective relaying.

Top Threats to Energy Infrastructure

The top four threats from my perspective are:

1. Rapid growth in the use of digital technology throughout the electric system during a timeframe of increasing cyber threats.
2. Advanced persistent cyber threats, especially by nation-states, including threats related to supply chain.
3. Delays sharing details about those threats from government to industry, due to factors such as limitations in clearances.
4. Cross-sector dependencies (communications and fuel) and associated coordination challenges.

I've included responses to some of the specific questions posed for this conference as an attachment to my written remarks.

I look forward to your questions.

Attachment 1

Threats to Energy Infrastructure:

1. What cyber and physical security threats are most concerning for the energy industry? What critical factors should industry consider when evaluating the risk these threats present and prioritizing risk-mitigating security initiatives to address these threats?

From my perspective, advanced persistent cyber threats by nation-states is the most concerning for the energy industry. The entire electric system (generation, transmission, distribution, and load) is evolving rapidly to include more interconnected digital devices. This increased use of digital technology increases the system's "cyber cross-section" and provides adversaries non-traditional avenues of attack.

An added element of the cyber threat involves supply chain. New standards have been implemented to address this issue but the scope and complexity is cause for concern.

2. Does industry have adequate resources to evaluate sophisticated threats such as whether adversaries have established access to their networks, whether insider threats exist, or whether supply chain equipment or subcomponents are compromised?

The industry, through coordination with governmental partners, is gaining the expertise and resources to evaluate these threats. Two examples include the CRISP program which can help detect malware on industry systems and the capability for forensic testing of devices at national labs and other locations.

3. How are interdependencies among energy infrastructure sectors considered in risk management analyses?

Awareness of the challenges with cross-system dependencies has grown significantly in the last few years. In particular, the need for robust communications – within the electric sector and with other sectors – has been highlighted. Several important initiatives are underway to improve communications resiliency – such as the via the ESCC R&D committee.

In addition, the changing generation fuel mix – including a large and increasing fraction fueled by natural gas – has been highlighted in many venues and is being closely evaluated. System Planning is evolving to consider fuel supply as the most limiting contingency.

4. What are some of the challenges (e.g. staffing or technology), that industry faces, in order to keep current with the threats?

At a macro level, increased digitization of the grid (transmission, generation, distribution, and load) in an environment of increasing cyber threats. To a lesser extent, use of traditional analog and digital technology can offer some challenges to workforce skills.

5. What other current or emerging threats should be addressed? For example, what are some of the types of physical and cyber security threats that Unmanned Aircraft Systems (i.e., drones) can present? What experience has industry had with commercially-available products used to address these issues?

Industry UAS use has increased significantly and with good effect – primarily in damage assessment and for right of way inspections rearding vegetation encroachment. This increased use poses potential threats regarding both cyber and physical security. Foreign sourced or compromised UASs could be used to assess sensitive industry assets and facilities during routine flights. In addition, UASs could be used to impact system assets – by flying into or dropping materials onto important assets.

Mitigation: Strategies and Best Practices:

6. What are some of the best practices that industry uses to ensure effective action against cyber and physical security threats? Are adequate tools available for industry to assess where to apply best practices (e.g., risk management analyses) for cyber and physical security threats? Do these analyses differ between cyber and physical security threats?

The industry has placed significant focus on risk assessment and internal controls (RAIC). These techniques apply to a range of reliability and resiliency risks including cyber and physical security. One specific Forum Practice Group is focused on developing RAIC best practices.

7. How does industry validate the effectiveness of, and maintain its mitigation techniques/measures (e.g., red teaming, manufacturers recommendations) for, both physical and cyber protection? What are the processes to confirm the results are addressed? Are these lessons shared with others in the industry?

Many NATF members have evolved their routine emergency plan drills and exercises to be more sophisticated – including assumption of malicious cyber and physical acts. For example, one NATF member just completed their 5th annual “Resilient Grid” exercise. This exercise included multiple adjacent utilities, representation for local, state, and federal government; and assumed a large-scale impact both territorially and in terms on key assets. The lessons learned from this exercise were shared in multiple confidential venues within the NATF.

Similarly, multiple “best practices” have been developed on how to harden key facilities from a range of attacks (physical, cyber, and EMP). A specific NATF workshop was held in 2018 to share these best practices and practical lessons learned from those members that had implemented related upgrades.

8. What resources are available to assist industry in evaluating risk to energy infrastructure and implementing mitigation measures, especially for small to medium size owners and operators?

Robust sharing of lessons learned in a variety of settings – inside and outside of NATF.

9. What training opportunities are available to owners and operators to understand the various risks to their energy infrastructure and the measures taken to mitigate against physical and cyber threats? What training is necessary and not available?

One training opportunity involves an overview of all the detection, prevention, and mitigation activities that are already underway.

10. How does industry mitigate key vulnerabilities to address disruptions from a cyber or physical attack or an extreme natural event (e.g. geomagnetic disturbance)? How should spare equipment, sharing programs, contractor and mutual assistance programs, and other processes be considered in addressing disruptions? What role should the federal government play in helping industry prevent and respond to disruptions? What preparations should be made by industry to assure adequate response and recovery efforts?

Significant focus has been applied to improve governance for large scale events. Such as through the development and testing of EEI's National Response Event (NRE) in the wake of hurricane Sandy. This structure helps ensure effective nation-wide mutual aid for extremely large-scale events. Similar frameworks are being used to help share specialized skills (e.g. Cyber Mutual Aid). A more recent initiative is the developing of framework for allow for execution of directives following declaration of a Grid Security Emergency (GSE).

Similarly, significant work and progress has been made on the topic of key spare parts. These include EEI's STEP and Spare Connect programs, Grid Assurance, and RESTORE. NATF has also done several evaluations of key spare parts and is hosted a related webinar later this year. In addition, several NATF members have innovated on equipment designs that allow for a greater degree of inter-changeability and faster replacement / deployment. Federal government support may be most helpful in reducing barriers to transport of large power transformers following an event with significant system damage.