House Energy and Commerce Committee, Energy Subcommittee

Hearing: "The Electricity Sector's Efforts to Respond to Cybersecurity Threats"

Answers to Questions for the Record

Chris Beck, EIS Council

March 9, 2017

The Honorable Morgan Griffith

1. **Today, the electric industry works with the DOE, with DHS, with the FBI, and other agencies to share information on threats and intelligence. But there does not appear to be a coordinated way for industry to share or receive information across these agencies, leading to more individualized notices from agencies than may be desirable.**
   A. **How can the federal government ensure better coordination within its own agencies and with the electric industry regarding information on threats and intelligence sharing?**

The Electric Subsector Coordinating Council (ESCC) and the Electric Sector Information Sharing and Analysis Center (E-ISAC) are the two important information sharing bodies in the Electric Subsector and work under the auspices of the Department of Homeland Security (DHS), the agency with overall responsibility for critical infrastructure protection under the National Response Framework (NRF) and National Infrastructure Protection Plan (NIPP), and the Department of Energy (DOE), the electric sector-specific agency under the NIPP and the lead agency for Emergency Support Function 12 (ESF-12) under the NRF. Intelligence and threat information gathered by other Federal agencies (FBI and other Intelligence Community agencies) should flow through DHS/DOE to the ESCC and E-ISAC for effective information sharing and dissemination to electric sector utilities.

Some electricity utilities are participating in the Cyber Risk Information Sharing Program, which allows utilities to send network data for analysis against government sources.

   A. **How can we expand programs like this to provide a frictionless partnership between the public and private sectors that allows private industry to be more agile in its response and allows the government a level of assurance that the power grid is secure?**

The key quality of a sound public/private relationship is trust-building. Information sharing itself is not hard, and protecting the information is straightforward, though the possibility of the information being exfiltrated is always present. The biggest hurdles are the private sector feeling unsure that the government will properly protect sensitive information (from FOIA requests, for example) or use the information against them regarding regulatory compliance. The government has trouble providing information to the private sector because government-held information,

especially intelligence information, is often classified, and especially over-classified. A streamlined process for de-classifying information (or at least lowering the classification level) is needed to rapidly provide necessary information to the electric sector.

The Honorable Frank Pallone

Mr. Beck, your organization focuses on Black Sky hazards. From the perspective of a cyberattack, such an event should be viewed as the worst case scenario: large in scope and duration, likely combining physical and cyberattacks to the grid, and potentially spanning across multiple critical infrastructure sectors.

1. Are the current norms and practices for electricity sector workforce training and development sufficient to prepare workers to respond quickly and effectively to the threat of an imminent or ongoing Black Sky attack?

The current norms and practices are good for what they are designed for: small-scale attack, accident, or disaster. Most of the training and practices at the tactical level can be used for a larger-scale attack, but the strategy has to be different for Black Sky events, due to the greatly expanded scope. To cite one example, if a small scale incident caused the power of a city (or even most of a State – think Superstorm Sandy) to go out but did not affect the surrounding area, the response strategy is to evacuate people from the blackout area, and flow resources from the outside into the affected area to restore the power.

If, on the other hand, the entire Eastern Interconnection blacked out, evacuation is not feasible, and there are not enough "outside" resources to flow in to allow restoration. Current workforce training focuses on the correct tactical areas (malware detection and removal, tech platform rebuild, manual workarounds, etc.) but strategically this won't work for a Black Sky event because it won't be possible to flow enough trained technical support personnel in to help, and in a large-scale attack, utilities may be hesitant to flow those resources to others if they are afraid they may be the next target.

2. What more could be done to improve electricity sector workforce training and development to better prepare workers for such event? In particular, can you speak to any efforts that would better promote intra-sector mutual assistance and cooperation across critical infrastructure sectors, both of which you promoted in your testimony?

The key components of the training are mostly adequate, with the one exception being training mutual assistance on utility-specific operational technology (OT) systems, which is currently challenging due to proprietary business and security concerns. ESCC's Cyber Mutual Assistance Program is certainly making progress in this area, but it is very challenging. Within the electricity subsector, pre-event, cross-utility training for direct OT system support is one option. While individual utilities' OT systems vary, there does exist a commonality of hardware and software system architectures that will allow rapid cross-training for mutual assistance. That said, in a large-scale cyberattack on the electric grid, system personnel within the sector will likely be needed to restore their own systems.

Additional trained personnel from outside of the electric subsector could provide a needed 'surge capacity' from other sectors. The approach being developed by EIS Council is the Certified Power Recovery (CPR) Engineering Team concept, wherein technical personnel from outside the electric power sector – but with requisite computer and electrical engineering backgrounds – can be trained and certified (pre-event) to supplement cybersecurity and power system engineering talent within the sector during large-scale emergency response activities. Another important source of external support is the use of State National Guard forces to help respond to utility requests for assistance.

It is certainly concerning that there are apparently not enough qualified applicants to fill the need for cybersecurity jobs in our country. I think this is a critical aspect of the issue that our Committee should evaluate as we continue our oversight of the security of our electric grid.

This is indeed a concern, needing long-term leadership and incentives – from both government and the private sector – to develop and maintain a robust, trained workforce to address this growing challenge.

The Honorable John Sarbanes

1. **What technical or funding support are you receiving from federal agencies on grid cyber security in terms of research and development and standard setting guidance? How could this support be enhance or improved?**

EIS Council is funded almost exclusively through philanthropic grants and does not currently receive any federal funding. That said, EIS Council considers the current standard-setting process for cybersecurity within the electricity subsector (NERC CIP) to be sufficient as a standard. Electric utilities should use and view the standard as a baseline for their protection activities, but must go beyond the standard in the ever-evolving challenge of cyber adversaries – which the standards simply cannot evolve fast enough to stay abreast of.

The Honorable Jerry McNerney

1. **The second installment of the QER noted that the traditional definition of reliability may be insufficient to ensure system integrity and available electric power in the face of physical attacks and cyber threats, among other things. And that the security of the systems, particularly cybersecurity, is a growing concern. Would you agree with this assessment?**

Yes. The challenge is that the standard metrics for reliability used by regulators – especially at the state level – do not effectively address the impact of physical and cyber- attacks, and cost recovery for resilience investments is a hard case to make. Cyberattacks, as discussed at the hearing, are the most rapidly evolving threat: malware continues to become more sophisticated (though so do the defenses against it); proliferation of malware is very easy and rapid; and the "attack surface" grows as more computer-based systems interface with the grid.

2. **Is there a uniform definition used in the energy and electricity sector – or at the federal level – of what cyber "secure" or "resilient" means?**

Mostly 'Yes' for cyber "secure" definition. The NERC Critical Infrastructure Protection (CIP) Cyber standards outline clear compliance guidelines for cybersecurity practices. This approach is necessary and understandable, and it does serve as a baseline for cybersecurity practices across the Bulk Power System. Compliance with the NERC CIP standards is an important component that highlights accepted practices for increasing the cybersecurity of Bulk Power System utilities. Additionally, the NERC CIP should probably be voluntarily followed by the distribution utilities (even though they are not part of the BPS and therefore not under FERC/NERC jurisdiction) because: 1) they present an attack surface to the BPS, and 2) a sudden loss of load would have significant impact on the BPS.

Mostly 'No' for "resilient" definition. While 'resilient' is typically understood to mean "the ability to withstand an assault/injury and rapidly recover", this has not yet been quantified more precisely. The electric power industry, other infrastructure sectors, government (Federal, and State), and interested academic and non-governmental organizations (including EIS Council) are all working to develop and gain consensus for reasonable resilience metrics.

3. **How costly is it to fund research R&D for cyber from a utilities perspective? When updating your networks and physical infrastructure, are you able to put in new, more cyber secure equipment in select areas or does it need to be done across the board? Do you feel that cyber security and resilient investments are adequately reflected in rate-making cases?**

Cybersecurity R&D is not very costly for government or utilities. Certainly the proliferation of cyberattack methods is very cheap, and while those on the defensive are always at a disadvantage, there are cost-effective methods available for protection and resilience, including critical system isolation, clean, rapidly-installable backup systems, and manual workarounds as necessary.

When updating networks, and physical infrastructure, it is certainly possible to target select areas for protection, to ensure minimal, base-level functionality of the system. Across the board protection, if available/affordable is better, which is captured in the defense-in-depth concept.

Currently such investments present a challenge in rate-making cases. Standard reliability metrics and cyber- or physical security standards do not readily transfer to rate-case making, because prevention of an unspecified outage area and duration due to enhanced security measures are speculative, compared to typical actuarial-informed risk analysis of more commonly addressed reliability concerns.

4. **Are customers appropriately knowledgeable on cybersecurity? How do we address that shortcoming?**

No, customers are not appropriately knowledgeable on cybersecurity. This is still a societal blind spot. Public education on cybersecurity is one avenue. But much more importantly, cybersecurity requirements must become a standard practice within the electric sector – as well as government

– when purchasing equipment from vendors. A canonical example is that computer systems, especially purchased in bulk, often have standardized usernames and passwords that must be changed at the discretion of the utility or user. Often this is overlooked. While the initial overhead of device-specific authentication may seem onerous, real security benefits will flow when individual devices are configured for security. Cybersecurity requires a conscious effort to identify risks at all levels of the Grid.

5. **Electricity is one of our most critical infrastructures. And our ability to respond to natural disasters or attacks requires access to electricity. Your testimony touched on power grid restoration and the need for cross-sector planning. First, do you believe there's adequate cross-sector planning as of now? Does the electricity sector have sufficient capability to communicate and respond to emergency situations?**

As of now, No – but improving (for both questions). In the modern economy, multi-level infrastructure interdependencies have become the norm. In this environment, cross-sector planning is essential to allow rational, effective resilience and disaster response. Too often, though, these cross-sector dependencies are not fully recognized, and there exists the assumption that the other supporting infrastructures/businesses will be operational to support response/recovery/restoration activities, without the requisite recognition of the interdependencies. This could – in some cases – be a mutual 'bootstrap' scenario. For example, a gas-fired electric generator needs just-in-time fuel delivery from a pipeline, which relies on electricity to pump the natural gas to the generator. In other cases it might be a question of restoration priorities. A blacked-out electric utility will typically focus on restoration of the most customers served, often referred to as 'meters', in as short a time as possible. One of those 'meters' could be the local water and/or wastewater utility, which in an emergency is much more important to restore than domicile-level electricity.

Communications represent yet another interdependency. Some electric utilities do have their own communications networks and infrastructure. Most rely to a large degree on the well-known commercial provider telecommunications companies, which in turn rely on electricity. Even for those with their own networks and who can therefore communicate internally to speed restoration, challenges would arise when trying to communicate with government and other infrastructure sectors (who do have a legitimate need to know the power restoration status) when trying to coordinate effective response and restoration actions.

6. **There have been an increasing number of new technologies placed onto the grid in the past decade. Protection throughout the supply chain is an area that deserves our attention, and that standards and best practices should be implemented but not overly prescriptive.**

Agree. The supply chain challenges are daunting, but must be addressed. As was mentioned by Gerry Cauley at the hearing, NERC is now looking at supply-chain security guidance for BPS utilities. Certification requirements from product vendors is one key to addressing this complicated problem. A second is to adopt procurement practices that specify systems with only minimal, stripped down, 'white list' programs, functions, and connectivity. For example, critical

systems should not be procured with any extraneous software applications, require two-factor authentication for any access, and require physical access security protocols.

7. **Are there concerns about potential cyber threats from systems that are already in place but we haven't seen an incident from yet?**

Certainly. There is a widely-used saying in cybersecurity circles: "If you're connected, you're infected." Chief security officers recognize that their systems are under near-constant attack, and that their systems are likely already breached – at least at some level. Continuous monitoring, patching, cleaning, and malware quarantine and removal should be standard operations. In addition, 'clean', disconnected backup systems that can be rapidly installed to replace compromised systems, and the ability to isolate critical components from the larger network, are needed to rapidly respond to currently undetected compromises.