**STATEMENT OF DR. CHRIS BECK**
**CHIEF SCIENTIST AND VICE PRESIDENT FOR POLICY**
**ELECTRIC INFRASTRUCTURE SECURITY COUNCIL**

**BEFORE THE HOUSE ENERGY AND COMMERCE COMMITTEE**
**SUBCOMMITTEE ON ENERGY**

**"THE ELECTRICITY SECTOR'S EFFORTS**
**TO RESPOND TO CYBERSECURITY THREATS"**

**FEBRUARY 1, 2017**

## Introduction

Chairman Upton, Ranking Member Rush, and Members of the Subcommittee, thank you for the opportunity to testify before you today on this important topic. My name is Chris Beck, Chief Scientist and Vice President for Policy at the Electric Infrastructure Security Council.

## EIS Council

The Electric Infrastructure Security Council, a 501(c)3 non-profit organization, is at its core a public interest organization. Our chief mission is to do our part to ensure societal continuity for Black Sky hazards – those threats that pose the risk of large-area (multiple states to continental in scope) and long-duration (one month or more) power outages, and the subsequent cascading failures of our other life supporting and sustaining critical infrastructures. We do this by hosting research and national and international collaboration focused on whole community resilience, restoration, response and recovery planning. Our programs and projects are intended to help facilitate utilities and other critical infrastructure sectors and their government partners develop

and implement cost-effective, consensus-based resilience and restoration measures by hosting frameworks for sustained coordination, planning, and best practice development. Our flagship program, the EIS Summit Series, hosts annual, international meetings of private sector, government, non-governmental, and academic organizations to further critical infrastructure resilience and whole community preparedness for Black Sky events.

**Black Sky Threats Overview**

"Black Sky" threats (or hazards) is increasingly becoming a term of art, referring to extreme natural or malicious threats that could cause extended and long duration power outages, covering many states and lasting more than a month. Six Black Sky threats have been identified as primary concerns. Three are naturally occurring: severe regional earthquakes (New Madrid fault), severe (worse-than-Sandy) terrestrial weather, and large geomagnetic disturbances caused by intense space weather. Three are malicious: coordinated physical attack on key electric grid nodes, high-altitude electromagnetic pulse attack (HEMP), and sophisticated cyberattack – the subject of today's hearing. As a further concern, malicious threats could be combined, or deployed at times of severe natural hazards, further increasing their impact.

While important differences exist between these threats, the commonality of their outcome will be power outages of unprecedented scope. For blackouts of this extent, cross-sector interdependencies would interfere substantially with the functionality of normal disaster planning. If we as a nation are to be adequately prepared for such hazards, to preserve the lives

of our citizens and sustain our society, new, well-coordinated approaches to restoration support and emergency planning will be essential.

**Black Sky Cyberattack on the Electric Grid**

The December 23, 2015 cyberattack on the Ukrainian electric power grid demonstrated that a blackout of electric power can be achieved through remote cyber means. 30 substations were taken offline, resulting in loss of electric power to approximately 225,000 customers, for up to six hours. The affected substations, though disconnected, were not permanently damaged, which allowed for reasonably rapid power restoration.

Once again, more recently, what is believed to be the 2nd cyberattack last year on Ukraine's Bulk Power System took place late Saturday night, December 18, 2016. Automation control systems at Ukraine's northern power substation were disrupted, causing a power outage through much of the northern part of Kiev.

Although these attacks were, thankfully, of limited scope and duration and therefore did not rise to the level of a Black Sky event, both may well have been essentially test cases intended, at least in part, to help perpetrators prepare far more extensive capabilities.

Stuxnet and Aurora demonstrated that catastrophic damage to physical equipment can be accomplished through cyberattack vectors. Both are examples of malware that can take control

of operational technology (OT) or industrial control systems (ICS), and cause disruption, misoperation, or destruction of the hardware that they control.

The successful coupling of such components – gaining control of multiple electric substations and/or generators at multiple locations throughout the country through remote access and then using that access to inflict permanent physical damage on them – could result in a Black Sky event. This would be the case if the damaged equipment were critical to grid operation and required a long period of time to repair or replace, such as large power transformers or generator turbines. It would also be the case if there is sufficient distributed disruption that the needed damage assessment and repair pushes restoration times beyond the point where cascading failures of other infrastructures begin interfering with the restoration.

**Black Sky Cyberattack on Multiple Infrastructure Sectors**

While cyberattacks on the Bulk Power System could be particularly devastating, there is no reason to believe that a determined adversary would limit an attack to this subsector. While the continued and rapid evolution of cyber threats are making protection continually more difficult, the electric subsector is far better protected than many other infrastructure sectors. Simultaneous attacks on the oil and natural gas subsector, on water systems, communications, government, emergency response, or other infrastructures could both create new categories of severe disruption and seriously complicate power restoration operations.

## Special Challenges for Cyberattack Response

In the aftermath of a natural disaster, response activities typically commence once the immediate danger has passed. In a cyberattack scenario, it is possible, or even likely, that the attacker could launch subsequent attacks to disrupt response and recovery efforts and/or cause further damage, using the same attack vector if it is not properly removed from the affected computer systems.

A closely related challenge is the tension between response/recovery and attribution. Identifying and removing malware from an affected system or installing updates or patches will be necessary for recovery to normal operation. Such actions, however, can also overwrite critical data needed for understanding the malware and for attacker attribution.

## Evolving Threats and Vulnerabilities

Of all the Black Sky threats, the cyber threat is constantly evolving and therefore very difficult to mitigate or stay ahead of. While the most sophisticated cyberattack vectors may require nation-state level activity, any determined adversary can acquire destructive malware through online criminal marketplaces. Such malware is constantly evolving and can be further modified for novel destructive purposes, and adversaries will continue to seek and develop them to attack U.S. infrastructure assets, among other targets.

At the same time as the threat is evolving, the “attack surface” continues to grow with the ever-growing trend to computerize, automate and allow remote access and control. One such example

is the strong push to update distribution networks through the installation of smart meters, which have the potential to be remotely accessed by adversaries. This could provide a new cyberattack path to the distribution utility. Additionally, if the meters were to be disconnected and destroyed, it could not only affect the homes or businesses whose power would be cut off, but if done on a large enough scale, could cause grid instability due to sudden, unexpected load loss, and require much time and effort to restore.

Another key challenge that is emerging due to the evolving technological and economic landscape is the issue of third-party service providers who have connectivity and access to utility networks. This allows the possibility for an adversary to infiltrate a utility not through a direct attack on the utility's system itself, but through a trusted but less secure third-party connection. In addition, in our evolving global supply chain, malicious actors have opportunities to insert malware into critical hardware or software at several points along a product's production lifecycle. Furthermore, third party vendors may have access to or hold sensitive utility data. If compromised, this data can provide an adversary with a roadmap – designs, blueprints, operational data – for attacking the utility.

**Enhanced Planning for Electric Subsector Response and Recovery**

The cybersecurity challenges are daunting, but electric power utilities are taking important steps to addressing this ever-evolving challenge. The largest and most sophisticated utilities are achieving cybersecurity enhancements nearly on par with the banking sector, which has the longest history of understanding and addressing security threats, including cyber threats.

To effectively respond to cyber incidents, it is critical to ensure that utilities and responsible government agencies have robust plans and procedures for critical response activities, communication, and partnership. Such plans and procedures must be vigorously exercised and constantly updated and improved, to keep pace with the threat. The GridEx series, hosted by NERC, is a good example – a biennial exercise of increasing difficulty and complexity, intended to push the system past the "breaking point", then gather lessons learned to improve planning for better protection and faster restoration of the system in future.

The leading power utilities have taken positive action along the cyberattack threat timeline or "kill chain". Primary control centers' physical and IT infrastructures have been hardened to resist attack, and their networks are constantly monitored and scrubbed of malware. Robust backup control centers that can operate the utility system if the primary has been successfully attacked are in place. Secure, clean copies of IT and OT software are held and ready for rapid installation to respond and recover from successful attacks. "Spare tire" operational modes – initiated by the North American Transmission Forum – that do not offer the full functionality of regular operations but that allow limited, critical operations to continue during response and recovery activities are being developed and implemented. Utilities must also maintain the ability to use mechanical controls, through regular training. There is certainly a large spread between the capabilities of the most sophisticated and forward-leaning companies and others that are not as well capitalized or fully appreciate the threat, but these represent the current best practices.

While robust plans and procedures to enhance the resilience of individual utilities is a critical component, a sophisticated, Black Sky level cyberattack would affect several hundreds or even thousands of locations nearly simultaneously, and without warning. In the interconnected grid, the successful disruption of utilities that were unable to defend against the initial attack will likely shut down, and these can cause the cascading blackout of even those utilities that were prepared for attack. To effectively respond to such a crisis, enhanced partnerships between utilities themselves, utilities and government agencies, and across infrastructure sectors will be important.

Electric utilities have a long history of providing mutual assistance, as we witnessed during Superstorm Sandy and many other natural disasters. The same concept can be applied for mutual support in response to a cyber incident, though challenges unique to cyber need to be taken into account. The mutual assistance provided during Sandy was primarily focused on repairing, replacing, and reconnecting downed power poles and lines, a standard practice across the country. In contrast, while every utility has IT and OT systems, OT systems in particular vary greatly from utility to utility, and so are much less “standard” than poles and power lines and the tools needed to repair them. On a positive note, an inherent security benefit of this non-uniformity of OT systems makes it less likely that any one piece of malware could successfully infect and attack all OT systems. The challenge from the mutual assistance perspective for recovery is that a utility that intends to help another may not be able to, or could possibly even cause further harm if they were to take well-intended but improper action on an OT system.

That said, there are options for cyber mutual assistance, a concept and practice introduced and being driven by the Electricity Subsector Coordinating Council. Moving along the spectrum from least to most difficult, assisting utilities who can provide IT expertise to a compromised utility can assist with cleaning, repairing, and restoring the afflicted utility's IT system, thus freeing up the affected utility's staff to focus on OT issues. They could also help with recovery and attribution by reviewing network logs to find malware signatures or other anomalies. If attacks are ongoing, they may be able to support active perimeter defense activities. Finally, if either a common OT system is identified between utilities, or, more likely, pre-event cross-utility training on each other's OT architecture is done, a supporting utility could directly assist in OT restoration.

IT and OT professionals, however, are typically a limited resource. In a large enough attack, availability of such expertise will likely be too limited to address the need. In addition, especially given the problem of sustained or follow-on cyberattack, CEOs may be reluctant to flow critical personnel to assist others when they might be the next target. To bolster the intra-electric sector mutual support, external support is also necessary.

Government support for utilities is available at the Federal and State levels. Federal resources include the DHS Industrial Control Systems Computer Emergency Response Team (ICS-CERT) teams to provide focused operational capabilities including system analysis and advice on mitigating ICS compromises, and the Electricity Information Sharing and Analysis Center (E-ISAC) to provide information on emerging and evolving threats, and their mitigations. Within

the Department of Defense, USCYBRERCOM is analyzing its ability to provide support to utilities under Defense Support to Civil Authorities missions. In addition, they recognize that because CONUS military installations rely on civilian electric power grids, adversaries can attack and weaken U.S. military power by going after the supporting electric infrastructure. Finally, the Department of Energy is the Federal coordinator and primary agency for Emergency Support Function 12 (ESF 12), the primary mission of which is to facilitate the restoration of damaged energy systems. In addition to authorities under ESF 12, key provisions of the Fixing America's Surface Transportation (FAST) Act of 2016, provide the Secretary of Energy with broad authority to issue emergency orders for electric grid protection and restoration if the President declares a "grid security emergency", which includes the occurrence or imminent danger of a cyberattack.

At the State Level, a growing number of National Guard units are developing expertise and programs to assist electric utilities in combatting cyberattacks. State fusion centers are also providing information on cyber threats, and a growing number of states recognize that electric power and other utilities must be involved in emergency planning and disaster response operations.

However, for a large scale attack these options, taken together, might be overwhelmed by the scale of the attack. Another possibility that may be helpful would be expanding the concept of Mutual Assistance, to develop a mechanism to assist corporations in bringing in IT and OT professionals from other private sectors resources. This could include arranging for participation

by corporations in many fields, including information technology, aerospace, water/wastewater utilities, telecommunications, manufacturing, and others. Many aerospace companies, for example, have established cybersecurity business divisions within their companies.

To make use of these potential resources for a major disaster, new best practice approaches could be developed for implementation by those power companies that wish to provide certification and periodic training of supplemental, volunteer engineering and technical teams for preplanned support to internal corporate IT and OT professionals. EIS Council is facilitating a process to explore this opportunity, working with interested power industry and external, private sector providers, as part of a Certified Power Recovery (CPR) Engineering Team Initiative.

Overall, cybersecurity protection enhancements really require continuing evolution of both private and public sector leadership, addressing this threat diligently, and continuously. Security has not traditionally been a high priority item within many infrastructure sectors, including electric power. That has certainly changed dramatically in recent years, but continuation of the trend to address cyber security throughout the nation's large and diverse energy sector, at the highest levels of decision making, is necessary to ensure that cyberattacks can be addressed. To cite one important example, the Electricity Subsector Coordinating Council (ESCC) is a public-private partnership between leadership in the Federal government and CEOs of electric power utilities. The ESCC is focused on protecting our grids from national-level security events, which includes cyberattacks. When the CEO of a company takes security and resilience seriously, the company develops a culture of security and resilience. Inclusion of security, and specifically cybersecurity principles in internal planning for company expansion, equipment replacement,

and employee training are all essential to promote the most cyber secure electric power sector we can.

**Enhanced Planning for Cross-Sector Restoration Support**

While there are many challenges associated with the evolving needs for cyber protection, the electric subsector, in particular, is already a leader in addressing these issues. However, another and perhaps even greater challenge must be addressed, if we wish to be prepared for the multi-sector coordination challenges that would be presented to power restoration teams if a cyber-attack – in spite of protection measures – proved successful.

Once a power outage exceeds a critical threshold – perhaps several days, for example, emergency generators in many interdependent infrastructure sectors will run out of fuel. Today there are not yet adequate plans to provide for extensive resupply of such fuel – or of burned-out generators – in an environment with severely disrupted communications, transportation, and limited and failing lifeline infrastructures. As a result, the processes power companies typically have in place to deal with severe emergencies will face unique challenges, including "black start" procedures designed for restarting grid segments without outside power.

Power grid restoration following a successful cyber-attack will only be possible if extremely broad multi-sector preplanning is in place to provide for cross-sector support to that restoration process, to coordinate the support that these other infrastructure partners will themselves need in

this environment, and to save and sustain lives during an extended restoration process. EIS Council's EPRO SECTOR initiative is hosting a coordinated planning process to address this need. This initiative is hosting planning by leaders of a wide array of interdependent sectors, as they utilize this framework to help define, detail and implement cross-sector coordination processes that will be needed in Black Sky scenarios. Best practice information is also gathered and shared through EIS Council's EPRO Handbooks and Black Sky Playbooks. Handbook I focuses on the Electricity Subsector and Whole Community Preparedness. Handbook II is a two-volume resource that focuses on the Fuels and Water/Wastewater Sectors. Handbook III, currently in development, will put a special focus on cross-sector cooperation for restoration activities. The Black Sky Playbooks are specific to each sector, but also include cross-sector planning through the identification of "external requirements" – assistance needed from other sectors and government agencies to prepare for and respond to Black Sky hazards.

By its nature, this process must provide for ongoing, operational, coordinated planning by a wide array of public and private sector corporations and agencies. Many streams of parallel meetings are now going on throughout the year, designed to host cross-sector planning by many sectors, to include energy, water, food and pharmaceutical production and distribution, health care, communication, transportation and both state and federal agencies.

This process is truly vital, if societal continuity is to be ensured to address, not simply a possible successful cyber-attack, but for any Black Sky hazard. Our purpose and role in hosting this uniquely broad EPRO SECTOR process is simply as hosts and facilitators. However, I would

like to publicly express our thanks to the remarkable, high level participation of senior leaders from many sectors already involved in this complex and expanding process.

## Conclusion

A sophisticated, distributed cyberattack on IT and OT systems within the electric power sector is one of the six Black Sky threats that could cause widespread and long-term power outages within the United States or anywhere in the world. Of the Black Sky threats, it is the fastest evolving and the most difficult to stay fully abreast of.

Effective protection and response for a cyberattack will require diligent effort by the entire electric sector, and by their partner sectors. Protecting and restoring utility OT systems is challenging, because each utility has its own architecture design, which can include unique protocols and legacy equipment that may be years old.

If, in addition, we wish to ensure national and societal continuity in the aftermath of a successful cyber-attack, unprecedented, broad and well-coordinated planning is required, not just for electric utilities, but by a wide array of other infrastructure sectors, and governments at all levels.

In summary, proper prior communication, coordination, information sharing and cross-training is enhancing the security of our Nation's electric grid, and by extension, our Nation as a whole, and

the power industry is a leader in this domain. Those efforts, however, must be continually expanded and strengthened, as the cyber threat continues to evolve. To address the full ramifications of this hazard, broadly coordinated public and private sector planning is needed that goes far beyond the electric subsector.