Testimony of Gerry Cauley, President and Chief Executive Officer
North American Electric Reliability Corporation
Before the
Quadrennial Energy Review Task Force
Public Meeting on "Enhancing Resilience in Energy Infrastructure and Addressing Vulnerabilities"

April 11, 2014

Introduction

Good morning Mr. Secretary, members of the Task Force and fellow panelists. My name is Gerry Cauley and I am the President and CEO of the North American Electric Reliability Corporation (NERC). NERC was designated the Electric Reliability Organization (ERO) by the Federal Energy Regulatory Commission (FERC) in accordance with Section 215 of the Federal Power Act (FPA), enacted by the Energy Policy Act of 2005

The Security Challenge for the Grid

I appreciate the opportunity to speak to the topic of enhancing resiliency and addressing the vulnerabilities of our nation's energy infrastructure. The electric grid is one of the Nation's most critical infrastructures. The North American BPS is one of the largest, most complex, and most robust systems ever created. Several, if not all, of the other critical infrastructure sectors are dependent on electric power. As CEO of the organization charged with ensuring the reliability and security of the North American grid, I am deeply concerned about the changing risk landscape from conventional risks, such as extreme weather and equipment failures, to new and emerging risks in the security arena.

To explore the impacts of this changing risk landscape, NERC has worked with industry and government to better understand security risks and manage those risks. Based on all of the work NERC has been involved in to date, it is clear that the most effective approach against adversaries exploiting the newer risk landscape is through thoughtful application of resiliency principles. Resiliency requires proactive readiness for whatever may come our way and includes robustness; the ability to minimize consequences in real-time; the ability to restore essential services; and the ability to adapt and learn.

I am most concerned about coordinated physical and cyber attacks intended to disable elements of the power grid or deny electricity to specific targets, such as government or business centers, military installations, or other infrastructures. These threats differ from conventional risks in that they result from intentional actions by adversaries and are not simply random failures or acts of nature. NERC and industry take these threats very seriously. Long before the advent of mandatory standards, NERC and industry participants have worked to address physical and cyber threats to critical assets. These threats are not new, but have evolved and continue to demand more and more attention from industry, which faces numerous risks. Recognizing the costs for ratepayers associated with these efforts requires prioritization, along with risk management, to ensure that we are focusing resources on the greatest risks to the reliability of the BPS.

NERC has developed a strategic approach to ensure reliability of the BPS, focusing on five main elements: 1) developing mandatory and enforceable standards; 2) ensuring compliance and audit oversight; 3) enhancing the ES-ISAC capabilities; 4) engaging in public-private partnerships; and 5) conducting outreach, training, and education activities within and external to the BPS such as GridEx.

NERC's ongoing cybersecurity and physical security activities to ensure reliability of the bulk-power system (BPS). These activities include, but are not limited to:

- Developing a physical security standard (as directed by FERC on March 7, 2014), and conducting outreach to industry in conjunction with our federal partners;
- Planning and participating in a 13-city outreach effort in response to a physical security attack at a California substation;
- Receiving FERC approval on Critical Infrastructure Protection (CIP) Version 5 standards in November 2013, our most updated version of the mandatory cybersecurity standards;
- Issuing alerts related to cybersecurity and physical security concerns and continuing information sharing through the Electricity Sector Information Sharing and Analysis Center (ES-ISAC);
- Facilitating Grid Security Exercise (GridEx) II, for the Electricity Sub-sector in North America with more than 2000 participants;
- Participating in the Electricity Sub-sector Coordinating Council (ESCC), which provides a forum for communication between public and private sector partners in the Electricity Sub-sector; and
- Contributing to activities related to Executive Order (EO) 13636 and Presidential Policy Directive (PPD) 21, as well as supporting the White House-initiated, Department of Energy (DOE)-led Electricity Sub-sector Cybersecurity Capability Maturity Model (ES-C2M2), which will assist with development and measurement of cybersecurity capabilities within the sub-sector.

Physical Security

In April of last year, a substation in California was the site of a physical attack. It is important to note the attack did not result in a power outage; in fact, no customers lost service. Nevertheless, the incident is a reminder of the vulnerabilities of our BPS and while rare, demonstrates that attacks are possible and have the potential to cause significant damage to assets and disrupt customer service. I would like to commend the owner of the substation for working tirelessly to not only recover from this attack, but to readily share lessons learned with government authorities and industry. Immediately after the event, the ES-ISAC issued an alert to inform industry of the event and provide advice on steps to mitigate and protect against such attacks. In addition, the ES-ISAC, DOE, FERC, the Department of Homeland Security (DHS), and the Federal Bureau of Investigation (FBI) developed an outreach effort to raise awareness of the event, inform industry of mitigation activities, and provide a forum for industry to meet with state, local, and federal authorities to discuss physical security concerns for their regions. This was an unprecedented public-private partnership effort to address physical security concerns and involved US and Canadian interests.

After September 11, 2001, industry developed and updated physical security guidelines to address the need for coordination and communication. These security guidelines address physical security response, best practices, and substation security. Specifically, they provide guidance on:

- Addressing potential risks;
- Identifying practices that can help mitigate the risks;
- Determining risk for an organization and practices appropriate to manage its risk;
- Identifying actions that industry should consider when responding to threat alerts received from the ES-ISAC and other organizations;
- Defining the scope of actions each organization may implement for its specific response plan; and

- Conducting assessment of and categorizing vulnerability and risk to critical facilities and functions.

In addition to these guidelines, NERC has a mandatory standard requiring reporting to NERC and law enforcement of physical damage or destruction of a facility or threats to damage or destroy a facility (EOP-004-2).

NERC is developing a physical security standard, which FERC ordered on March 7, 2014. NERC has 90 days to complete the standard and provide it to FERC for approval. This standard will address physical security threats and vulnerabilities for the most critical facilities and will focus on risk management activities and foundational physical security practices. The drafting team has already been formed and we fully intend to produce a standard in the timeline identified.

NERC measures to address cyber threats and vulnerabilities
Since 2007, NERC has updated its standards to reflect the changing cybersecurity landscape. On November 21, 2013, FERC issued an order approving CIP Version 5. CIP Version 5 requires that all cyber assets must now be categorized as Low, Medium, or High Impact assets. The revised standards also include 12 new requirements with new cybersecurity controls to address emerging cyber threats. In addition, CIP Version 5 removes technology-specific requirements by replacing them with a risk-based approach to implementing appropriate and changing technologies. That is, rather than specifying how to implement a requirement, the revised requirements specify the risk-based result that must be achieved, which enables industry to implement new and emerging technologies to address the risk. NERC is working with industry on the transition to this new standard, which is one of the most comprehensive, risk-based standards ever mandated.

Ensuring Compliance and Audit Oversight
Concurrent with developing mandatory reliability standards, NERC supports the ERO's Regional Entities to improve the consistency of compliance program results, improve risk-based approaches for auditing and spot checking, and promote a culture of security and compliance through education, transparency, and incentives. During this process, NERC seeks to capture compliance applications, positive observations, lessons learned, and recommendations. NERC's audit oversights enable NERC to evaluate the processes and criteria used by Regional Entities in their determination of registered entities' compliance with the NERC Reliability Standards, including the CIP Standards.

Compliance with the NERC CIP standards is an important element for properly securing the BPS. However, no single security asset, technique, procedure, or standard—even if strictly followed—will protect an entity from all potential cyber threats. The cybersecurity threat environment is constantly changing and our defenses must keep pace. Security best practices call for additional capabilities and technologies beyond those required by the CIP standards.

Enhancing the ES-ISAC’s Capabilities
Not all threats and vulnerabilities can be mitigated through a reliability standard. In such cases, NERC uses tools and technologies through the ES-ISAC, including Alerts and a secure web portal. The ES-ISAC gathers information from electric industry participants across North America about security-related events, disturbances, and off-normal occurrences within the Electricity Sub-sector and shares that information with key governmental entities. In turn, these governmental entities provide the ES-ISAC with information regarding risks, threats, and warnings that the ES-ISAC is then responsible for disseminating throughout the Electricity Sub-sector. The two functions that the ES-ISAC supports,

information sharing and analysis, are vitally important to all other critical infrastructures and key resource sectors that have active ISACs. Effective collaboration and communication is essential to addressing infrastructure protection and resilience within each sector, as well as the important interdependencies that exist among sectors.

For many companies in the Electricity Sub-sector, the ES-ISAC portal is the first and often primary interface with the ES-ISAC. It allows the ISAC to reach thousands of industry members and hundreds of organizations across the sub-sector and is the mechanism for industry and government to contact ES-ISAC staff with questions, concerns, and security-related information in a secure manner.

NERC Alerts

NERC staff with appropriate security clearances often work with cleared personnel from Federal agencies to communicate unclassified sensitive information to the industry in the form of NERC Alerts. As defined in NERC's Rules of Procedure, the ES-ISAC developed the following three levels of Alerts for formal notice to industry regarding security issues:

- Industry Advisory. Purely informational, intended to alert registered entities to issues or potential problems. A response to NERC is not necessary.
- Recommendation to Industry. Recommends specific action be taken by registered entities. Requires a response from recipients as defined in the Alert.
- Essential Action. Identifies actions deemed to be "essential" to BPS reliability and requires NERC Board of Trustees approval prior to issuance. Like recommendations, essential actions require recipients to respond as defined in the Alert.

NERC determines the appropriate Alert notification based on the risk to the BPS. Generally, NERC distributes Alerts broadly to users, owners, and operators of the North American BPS using its Compliance Registry. Entities registered with NERC are required to provide and maintain updated compliance and cybersecurity contacts. NERC also distributes the Alerts beyond BPS users, owners, and operators to include other electricity industry participants who need the information. Alerts may also be targeted to groups of entities based on their NERC-registered functions (e.g., Balancing Authorities, Transmission Operators, Generation Owners, etc.).

Alerts are developed with the strong partnership of Federal technical organizations, including FERC, DOE National Laboratories, DHS, and BPS subject matter experts (SME), called the HYDRA team. NERC has issued 27 CIP-related Alerts since January 2010 (25 Industry Advisories and two Recommendations to Industry). Those Alerts covered items such as Sabotage events, Aurora, Stuxnet, Night Dragon, and the reporting of suspicious activity. Responses to Alerts and mitigation efforts are identified and tracked, with follow-up provided to individual owners and operators and key stakeholders. In addition, NERC released one Joint Product CIP Awareness Bulletin in collaboration with DOE, DHS, and the FBI titled, "Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPN)." The ES-ISAC also routinely shares actionable threat information through the portal to defend against cyber attacks; this information sharing is a daily activity.

The NERC Alert system is working well. It is understood by industry, handles sensitive information, and communicates this information in an expedited manner. The information needed to develop the Alert is managed in a confidential manner and does not require a NERC balloting process. Information sharing through the ES-ISAC is the greatest asset we have to combat emerging threats to cybersecurity and help ensure the reliability of the BPS. As a result, NERC continues to grow the ES-ISAC's capabilities by enhancing the ES-ISAC's private, secure portal to receive voluntary reports from industry members and working with various organizations (both industry and government) to obtain the data and mechanisms necessary to conduct these information sharing activities.

Engaging in Public-Private Partnerships

NERC works closely with Electricity Sub-sector members, other sectors, and our government partners on cybersecurity matters on a regular basis through both formal and informal structures. NERC works closely with the Electricity Sub-sector Coordinating Council (ESCC). As NERC's CEO, I am a member of the ESCC, which coordinates policy-related activities and initiatives to improve the reliability and resilience of the Electricity Sub-sector. The roles of the ESCC are to represent the Electricity Sub-sector, to build relationships with government and other critical infrastructure sectors, and to participate in joint initiatives as part of the "partnership framework" envisioned by the National Infrastructure Protection Plan and Energy Sector-Specific Plan. This past year, the ESCC underwent changes to broaden membership to 30 CEO-level representatives, formally recognizing the significant increased CEO interest and participation on cybersecurity issues. The ESCC's focus to address physical security and cybersecurity issues, working alongside our government partners, remains unchanged.

A broader partnership activity NERC was heavily engaged in this past year was helping to implement EO-13636 and PPD-21. NERC and industry SMEs participated in the working groups to help shape the final products. The various EO and PPD working group activities all focused on enhancing public-private partnerships, developing tools and best practices for sectors to use, and ultimately, reducing risk to critical infrastructure sectors. For all of these efforts, NERC worked closely with industry representatives and government partners to build new and improve upon existing cybersecurity-focused capabilities, processes, and products.

NERC also continues to provide leadership to significant DHS-affiliated public-private partnerships. These groups are:

- Cross-Sector Cyber Security Working Group, which was established to coordinate cross-sector initiatives that promote public and private efforts to help ensure secure, safe, and reliable critical infrastructure services; and
- Industrial Control Systems Joint Working Group, which is a cross-sector industrial control systems working group that focuses on the areas of education, cross-sector strategic roadmap development, and coordinated efforts to develop better vendor focus on security needs for industrial control systems.

Within the sub-sector, NERC's Critical Infrastructure Protection Committee (CIPC) focuses on both physical security and cybersecurity issues impacting the BPS. The committee consists of both NERC-appointed regional representatives and technical SMEs. CIPC coordinates NERC's security initiatives and serves as an expert advisory panel to the NERC Board of Trustees, standing committees in the areas of physical security and cybersecurity, and the ES-ISAC. CIPC also coordinates with government individuals and entities to hold joint briefings and participate in other activities to address security policy matters. NERC also collaborates with the Industrial Control Systems Cyber Emergency Response Team to share threat, vulnerability, and security incident information.

Conducting Outreach, Training, and Education Activities

In addition to collaborating with industry and government partners, NERC regularly conducts outreach to and training for our partners. We do so through assessments, exercises, webinars, and guidelines.

GridEx II

In 2011, NERC facilitated the first-ever GridEx for the Electricity Sub-sector in North America. NERC now holds a biennial distributed play exercise and executive tabletop discussion to:

- Exercise the current readiness of the electricity industry to respond to a security incident, incorporating lessons learned;
- Review existing command, control, and communication plans and tools for NERC and its stakeholders;
- Identify potential improvements in cybersecurity and physical security plans, programs, and responder skills; and
- Explore senior leadership policy decisions and triggers in response to a coordinated cyber and physical event of national significance with long-term grid reliability issues.

NERC held GridEx II on November 13-14, 2013, where over 230 organizations participated in the Distributed Play session. Additionally, a group of senior industry and government executives participated in a tabletop session based on the Distributed Play scenario but greatly expanded in scope. The exercise built upon the objectives and findings from the 2011 GridEx recommendations and simulated a coordinated cyber and physical security attack to offer participants a worst-case scenario to review their existing command control and communication plans and to identify potential areas for improvement. The exercise was the most comprehensive effort to date that addressed both cyber and physical security. NERC released reports in March 2014 detailing lessons learned and recommendations. These reports are posted on NERC's website.

Cyber Risk Preparedness Assessments (CRPA)

The ES-ISAC developed the CRPA program to assess, through exercises, an entity's current cybersecurity capabilities and the adequacy of existing reliability mechanisms. By conducting these assessments, the ES-ISAC targets areas for improvement and identifies best practices that it can then share with industry. Since 2010, over a dozen entities have participated in the CRPA program and have responded positively to the impact the CRPAs have on strengthening their operations, and ultimately helping to protect the BPS.

The CRPA program continued to mature in 2013 with the addition of the ES-C2M2 key practice areas informing and complementing the CRPA program. The program used the ES-C2M2 to shape the analysis of the exercise and focus the post-exercise discussion and report around the response capabilities as defined through the ES-C2M2. As part of the ES-ISAC's strategy to support adoption of the CRPA methodology more broadly across the industry, the ES-ISAC hosted a workshop in 2013 to provide training and templates for industry to use in support of their own exercise programs. The CRPA also supported the GridEx II exercise, providing documentation and training to exercise participants on using the ES-C2M2 in assessing their organization's response capabilities.

Security Briefings and Guidelines

Another example of NERC's outreach and training efforts included a classified briefing campaign in 2013. The ES-ISAC, DHS, DOE, and FBI collaborated to host a series of briefings focused on tactics and tools of emerging cyber threat actors. Similar to the 2014 physical security outreach campaign, this campaign included a multi-city tour across the United States and was developed following a NERC Alert that detailed how attackers use common tools to infiltrate critical infrastructure networks and gain access to control system networks. The briefings were designed to raise awareness within the control systems community to better protect the BPS.

In addition, NERC's CIPC holds security briefings and workshops throughout the year to educate industry about items such as physical security assessments and penetration testing. CIPC also developed physical security guidelines for the Electricity Sub-sector to assist entities in responding to a physical security situation. The guidelines also include a reference document that any entity can adapt to its specific physical security policies and procedures.

Finally, NERC hosts its annual Grid Security Conference (GridSecCon), which brings together cybersecurity and physical security experts from industry and government to share emerging security trends, policy advancements, and lessons learned related to the Electricity Sub-sector. GridSecCon 2013 included discussions focused on industry being transformational, strategic, and tactical in its approach to securing systems. Specifically, participants were asked to consider different information sharing techniques; determine if their organizations are resilient through self-assessments; test response activities through exercises; work to ensure that security is built into operations; and enhance the workforce by recruiting, training, and retaining individuals who can address these and other issues. Additionally, almost 200 stakeholders attended credentialed training sessions in cyber and physical security.

Ongoing Reliability Assessments

NERC's mission to ensure the reliability of the BPS goes beyond issues related to security of the grid. As directed by Section 215(g) of the FPA, NERC, as the ERO, conducts periodic assessments of the reliability and adequacy of the North American BPS. NERC produces summer and winter assessments as well as an annual the Long Term Reliability Assessment which assesses the adequacy of the bulk electric system in the United States and Canada over a ten-year period.

NERC conducts special assessments which have covered reliability topics such as the integration of variable generation, the impact of environmental regulations on reliability, gas-electric interdependency and most recently a joint report with the California ISO which identified the need for further study on essential reliability services.

The November 2013 joint report with the California ISO, *Maintaining Bulk Power System Reliability while Integrating Variable Energy Resources – CAISO Approach,* concluded that, when the portion of the resource mix provided by renewable and distributed resources reaches 20% to 30% of the total supply, the reliability of BPS can be diminished. This results from reduced availability of essential reliability services to support bulk system reliability. Larger dispatchable generating units have always inherently provided essential reliability services for the BPS. As these units are retired, and non-dispatchable renewable and distributed generation connect to the grid without replacing the essential reliability services, the availability of essential reliability services is diminished. These services include demand and resource balancing and voltage and frequency support.

As large quantities of variable energy resources—predominately wind and solar PV—are integrated into the BPS, a greater proportion of the system's total resource mix will have limited inertial rotating mass capability and operational flexibility. These new resources with much different operating characteristics will displace electric generation, as well as the essential reliability services, provided by large rotating machines and the operating characteristics those machines provided. Therefore, it is necessary that in addition to the energy and capacity needs of a given system, essential reliability services must be assessed and given due consideration in both BPS planning and policy implementation. NERC continues to assess these challenges and is developing pro-active measures to address any potential issues through a suite of tools available to NERC, including but not limited to Reliability Standards.

Conclusion

As outlined today, NERC has many tools available, including standards and guidelines to provide foundational security efforts. These, along with the ES-ISAC and all of its capabilities to help address imminent and strategic physical and cyber threats to the power grid, provide a coordinated comprehensive effort to address cybersecurity and physical security. We work with government, industry, and other stakeholders to share what we know, educate our partners, and learn what we can to secure our systems and stay ahead of the threats.