Remarks of Gerry Cauley, President and Chief Executive Officer, North American Electric Reliability Corporation

House Homeland Security Subcommittee on Cybersecurity Infrastructure Protection and Security Technologies The DHS Cybersecurity Mission: Promoting Innovation and Securing Critical Infrastructure

April 15, 2011

Introduction

Good morning Chairman Lungren, Members of the Subcommittee and fellow panelists. My name is Gerry Cauley and I am the President and CEO of the North American Electric Reliability Corporation (NERC). I am a graduate of the U.S. Military Academy, a former officer in the U.S. Army Corps of Engineers, and have more than 30 years experience in the bulk power system industry, including service as a lead investigator of the August 2003 Northeast blackout and coordinator of the NERC Y2K program. I appreciate the opportunity to testify today on the topic "The DHS and the Cybersecurity Mission: Promoting Innovation and Securing Critical Infrastructure.

NERC Background

NERC's mission is to ensure the reliability of the bulk power system of North America and promote reliability excellence. NERC was founded in 1968 to develop voluntary standards for the owners and operators of the bulk power system (BPS).[1] NERC is an independent corporation whose membership includes large and small electricity consumers, government representatives, municipalities, cooperatives, independent power producers, investor owned utilities, independent transmission system operators and federal power marketing agencies such as TVA and Bonneville Power Administration.

In 2007, 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. Upon approval by FERC, NERC's reliability standards became mandatory across the BPS. These mandatory reliability standards include Critical Infrastructure Protection (CIP) Standards 002 through 009, which address the security of cyber assets essential to the reliable operation of the electric grid. To date, these standards [and those promulgated by the Nuclear Regulatory Commission] are the only mandatory cybersecurity standards in place across the critical infrastructures of North America.

[1] The Bulk Power System (BPS) is defined as generation and transmission of electricity greater than 100kv, in contrast to the distribution of electricity to homes and businesses at lower voltages.

Subject to FERC oversight, NERC and its Regional Entity partners enforce these standards, which are developed with substantial input from industry and approved by FERC, to accomplish our mission to ensure the reliability of the electric grid. In its position between industry and government, NERC embodies the often-invoked goal of creating effective partnerships between the public sector and the private sector.

As a result of society's growing dependence on electricity, the electric grid is one of the Nation's most critical infrastructures. The bulk power system in North America is one of the largest, most complex, and most robust systems ever created by man. It provides electricity to more than 334 million people, is capable of generating more than 830 gigawatts of power and sending it over 211,000 miles of high voltage transmission lines, and represents more than $1 trillion in assets. The electricity being used in this room right now is generated and transmitted in real time over a complex series of lines and stations from possibly as far away as Ontario or Tennessee. As complex as it is, few machines are as robust as the BPS. Decades of experience with hurricanes, ice storms and other natural disasters, as well as mechanical breakdowns, vandalism and sabotage, have taught the electric industry how to build strong and reliable networks that generally withstand all but the worst natural and physical disasters while supporting affordable electric service. The knowledge that disturbances on the grid can impact operations thousands of miles away has influenced the electric industry culture of planning, operating and protecting the BPS.

The Cybersecurity Challenge for the Grid

Along with the rest of our economy, the electric industry has become increasingly dependent on digital technology to reduce costs, increase efficiency and maintain the reliability of the BPS. The networks and computer environments that make up this digital technology could be as vulnerable to malicious attacks and misuse as any other technology infrastructure. Much like the defense of this country, the defense of the BPS requires constant vigilance and expertise.

The assets that make up the BPS are varied and widespread. Consequently, the architecture within the systems varies from operator to operator. However, the computer systems that monitor and control BPS assets are based on relatively few elements of technology. Due to increasing efficiencies and globalization of vendors, the universe of suppliers for industrial control systems is limited. This trend is leading toward a fairly homogenous technological underpinning and, as older proprietary technology is replaced, the variation may decrease further.

For example, the bulk power system could be as vulnerable to digital threats as IT systems, but with far more critical implications. As proprietary industrial control systems continue to integrate Commercial Off-The-Shelf (COTS) systems, these platforms could inherit the embedded vulnerabilities of those systems. As illustrated by the Stuxnet malware, industrial control system software can be changed and a loss of process control can occur without intrusions even being detected. The Stuxnet intrusion methods may serve as a blueprint for future attackers who wish to access controllers, safety systems, and protection devices to insert malicious code that could result in changes to set points and switches, as well as the alteration or

suppression of measurements. NERC, through the Electricity Sector-Information Sharing and Analysis Center (ES-ISAC), issued an alert on Stuxnet, as it has done with other vulnerabilities, to inform the industry and recommend preventative action.

Establishment and continued refinement of NERC's enterprise risk-based programs, policies and processes to prepare for, react to, and recover from cybersecurity vulnerabilities need to continue to be a high priority for the industry. The bulk power system has not yet experienced wide-spread debilitating cyber-attacks due in large part to the traditional physical separation between the industrial control system environment and business and administrative networks. However, the increased sharing of Internet and computer networking by control systems and business and administrative networks means that digital infrastructures that were formerly physically separated are now becoming susceptible to common threats.

The Role of NERC and Critical Infrastructure Protection Reliability Standards

The NERC CIP standards require electric sector entities to develop a risk-based security policy based upon their specific assets, architecture and exposure. This policy, if properly implemented, will provide insight into the entity's systems and provide the opportunity to mitigate potential threats and vulnerabilities before they are exploited. Compliance with the NERC CIP standards is a first step in properly securing the BPS. However, there is no single security asset, security technique, security procedure or security standard that, even if strictly followed or complied with, will protect an entity from all potential threats. The cybersecurity threat environment is constantly changing and our defenses must keep pace. Security best practices call for additional processes, procedures and technologies beyond those required by the CIP standards. Simple implementation of enforceable standards, while valuable and a necessary first step should not be seen as the security end-state.

It is important to emphasize the difficulty of addressing grid security through a traditional regulatory model that relies principally on mandatory standards, regulations, and directives. The defensive security barriers mandated by CIP standards can be effective in frustrating ordinary hackers by increasing the costs and resources necessary to harm to the grid. They may not, however, stop the determined efforts of the intelligent, adaptable adversaries supported by nation states or more sophisticated terrorist organizations.

NERC is moving forward with a number of actions to complement our mandatory CIP standards and provide enhanced resilience for the grid. As chair of the Electricity Sub- Sector Coordinating Council (ESCC), I work with industry CEOs and our partners within the government, including the Department of Energy, Department of Defense and Department of Homeland Security, to discuss and identify critical infrastructure protection concepts, processes and resources, as well as to facilitate information sharing about cyber vulnerabilities and threats. This type of public/private partnership is key to coordination and communication efforts on cybersecurity topics and initiatives. NERC is also developing a North American cybersecurity exercise to prepare for and test a national response plan for the electric sector.

The most effective approach for combating sophisticated adversaries is to apply resiliency principles, as outlined in a set of nine recommendations the National Infrastructure

Advisory Council delivered to the White House in October 2010. I served on that Council, along with a number of nuclear and electric industry CEOs. Resiliency requires more proactive readiness for whatever may come our way. Resiliency includes providing an underlying robust system; the ability to respond in real-time to minimize consequences; the ability to restore essential services; and the ability to adapt and learn. The industry is already resilient in many aspects, based on system redundancy and the ability to respond to emergencies. To further enhance resiliency, examples of the NIAC team's recommendations include: 1) a national response plan that clarifies the roles and responsibilities between industry and government; 2) improved information sharing by government regarding actionable threats and vulnerabilities; 3) cost recovery for security investments driven by national policy or interests; and 4) a national strategy on spare equipment with long lead times, such as transformers. At NERC, we are working with stakeholders to develop programs that build upon the resiliency inherent in the grid to better secure critical assets and ensure the continued reliability of the BPS.

Information Exchange is Critical

NERC and the electric industry can only deal with the risks they are aware of. It is impractical, inefficient and impossible to defend against all possible threats or vulnerabilities. Entities must prioritize their resources to ensure that they are protected against those risks that pose the greatest harm to their assets, their business and their customers. The electric industry is in the best position to understand the impact that a particular event or incident could have on the BPS, but they do not have the same access to actionable intelligence and analysis that the government does. This lack of information leads the industry to be, at best, a step behind when it comes to protecting against potential threats and unknown vulnerabilities. Too often the industry has heard from government agencies that the threats are real, but are given little or no additional information. This leads to frustration among the private sector leaders who are unable to respond effectively due to ill-defined and nebulous threat information.

NERC and DHS

Improving the amount and quality of actionable intelligence available to industry is a priority for NERC and is reflected in a number of joint projects underway with DHS and DOD.

NERC is working with DHS' National Cybersecurity and Communications Integration Center to develop a Memorandum of Understanding for bi-directional sharing of critical infrastructure protection information between the government and the electricity sector in North America. The MOU will result in cybersecurity data flow, analytical collaboration, and incident management activities across the spectrum of cybersecurity coordination to include detection, prevention, mitigation and response/recovery.

NERC and DHS cooperative activities will align differing, but related missions, business interests, strengths, and capabilities to identify and develop mitigations for emerging cybersecurity risks, which will enhance the protection of critical infrastructure and government networks and systems that are vital to national security and the Nation's economy. Under this MOU, NERC, as the ES-ISAC, will act as a clearing house, disseminating actionable intelligence, including classified contextual information to appropriately cleared staff within the

BPS community. NERC also will provide anonymous situational awareness to DHS analysts to supplement the information DHS received from the intelligence community. We see this effort as crucial to improving the level of threat awareness within the industry and improving information between government and industry.

As noted before, NERC also uses the ES-ISAC to send Alerts and Notifications to registered BPS entities. These Alerts and Notifications are developed with the strong partnership of federal technical partners, including DHS and the Department of Energy National Laboratories, and BPS subject matter experts, called the HYDRA team by NERC.

NERC also provides leadership to two significant DHS-affiliated public-private partnerships. These are the Partnership for Critical Infrastructure Security (PCIS) and the Industrial Control Systems Joint Working Group (ICSJWG). The PCIS is the senior most policy coordination group between public and private sector organizations. On the government side, PCIS is comprised of the National Infrastructure Protection Plan (NIPP) Federal Senior Leadership Council (FSLC) and the State, Local, and Tribal Government Coordinating Council (SLTGCC), as well as the chairs of all of the other Government Sector Coordinating councils. On the private side, PCIS is comprised of the chairs of all of the private sector coordinating councils. The ICSJWG is a cross-sector industrial control systems working group that focuses on the areas of education, cross-sector strategic roadmap development, coordinated efforts on developing better vendor focus on security needs and cybersecurity policy issues.

NERC, DOE and DOD

NERC is engaged with other agencies besides DHS, including DOD and DOE National Laboratories, to further the level of awareness and expertise focused on cybersecurity, especially as it pertains to the BPS. We are working with Pacific Northwest National Laboratory on developing certification guidelines for Smart Grid Cyber Operators and the Electric Sector Network Monitoring initiative. Similarly, we are working with the Idaho National Laboratory to promote the Cyber Security Evaluation Tool for use within the electric sector. NERC also is partnering with the Industrial Control Systems Cyber Emergency Response Team to share threat, vulnerability and security incident information.

Additionally, NERC is working with DOE and the National Institute of Standards and Technology to develop comprehensive cybersecurity risk management process guidelines for the entire electric grid, including the BPS and distribution systems. We believe this to be particularly important with the increasing availability of smart grid technologies. While the majority of technology associated with the smart grid is found within the distribution system, vulnerabilities realized within the distribution system could potentially impact the BPS. Everyone engaged in smart grid implementation should ensure that appropriate security applications and technologies are built into the system to prevent the creation of additional threats and vulnerabilities.

Conclusion

As our Nation becomes more dependent upon electricity and as the BPS becomes more dependent on information systems, we must secure those systems that enable our way of life. As discussed today, NERC is committed to working with DHS and other government agencies on several efforts to promote innovation and secure our critical infrastructure. As Congress considers policy decisions in this arena, NERC would suggest that the ESCC and the ES-ISAC be considered as key elements in the cybersecurity mission. NERC continues to work with government and industry to utilize its expertise and promote thoughtful innovation as we address the question of how to ensure security in our open society. The cybersecurity challenges facing us are not intractable - they are the result of our own great innovation and can be overcome through our own great ingenuity.