BEFORE THE
UNITED STATES HOUSE OF REPRESENTATIVES

COMMITTEE ON ENERGY AND COMMERCE,
SUBCOMMITTEE ON ENERGY AND THE ENVIRONMENT

TESTIMONY OF THE HONORABLE GARRY BROWN
CHAIRMAN, NEW YORK STATE PUBLIC SERVICE COMMISSION

ON BEHALF OF THE
NATIONAL ASSOCIATION OF REGULATORY UTILITY COMMISSIONERS

ON

"Protecting the Electric Grid: H.R. 2165, the Bulk Power Systems Protection Act of 2009, and H.R. 2195"

October 27, 2009

National Association of
Regulatory Utility Commissioners
1101 Vermont Ave, N.W., Suite 200
Washington, D.C. 20005
Telephone (202) 898-2200, Facsimile (202) 898-2213
Internet Home Page http://www.naruc.org

Good morning Chairman Markey, and Members of the Subcommittee:

My name is Garry Brown, and I am Chairman of the New York State Public Service Commission (NY PSC). I also serve as Chair of the Electricity Committee of the National Association of Regulatory Utility Commissioners (NARUC), on whose behalf I am testifying here today. I am honored to have the opportunity to appear before you this morning and offer a State perspective on "Cyber Security."

NARUC is a quasi-governmental, non-profit organization founded in 1889. Our membership includes the public utility commissions serving all States and territories. NARUC's mission is to serve the public interest by improving the quality and effectiveness of public utility regulation. Our members regulate the retail rates and services of electric, gas, water, and telephone utilities. We are obligated under the laws of our respective States to assure the establishment and maintenance of such utility services as may be required by the public convenience and necessity and to assure that such services are provided under rates and subject to terms and conditions of service that are just, reasonable and non-discriminatory.

I want to thank you for holding this timely hearing. State regulators take the reliability and security of the bulk-power system very seriously. Through strong federal, State, public, and private partnerships, we have consistently maintained and improved reliability and security of the grid. As times and technologies have changed, new risks

and vulnerabilities have emerged. The transition to a smarter, digital, more efficient grid — while full of promise — carries with it unforeseen concerns and unintended consequences. As Congress considers legislation in this area, it should build on existing federal-State coordination and result in a framework where vulnerabilities to the system are identified, prioritized, and resolved in a timely fashion. Such legislation must distinguish between imminent threats, which require immediate action, and vulnerabilities, which can be resolved more deliberately.

State commissions are old hands at overseeing and ensuring the highest levels of reliability from our nation's utility service providers. Reliable service is the top priority of commissions, even more than affordability and environmental friendliness: if the lights go off, it doesn't matter how cheap or green the electricity is. Our nation's utilities (municipal, cooperative, and investor-owned) have done this country proud in responding to the greatest calamities and catastrophes, quickly and capably restoring power after hurricanes, earthquakes, wildfires, and as my State can attest, acts of terrorism. Commissions understand that preparedness should not focus on response, but should also assure that resilience is built into our infrastructure as a core principle.

As with most sectors of the economy, information systems are rapidly merging with utility systems, potentially heightening the risks of service disruption. Cyber security is an emerging area of risk for our utilities and State Commissions as well, and although it is unique in some respects, this is not the first time our utility systems have faced new reliability threats. Through a strong public-private partnership, we have

overcome past risks, and it is my belief that overall, this merging of information systems into the electric and other utility sectors improves their resilience, reliability and efficiency.

By way of background, State commissions are economic regulators. We have not traditionally had a national security role, either at the State or national level, as this is the province of Emergency Management Agencies, State Policy, and Departments of Homeland Security. However, now the lines defining and separating roles in critical infrastructure protection between the federal government, state agencies, and the private sector owners of critical infrastructure are necessarily overlapping. Cooperation and acceptance of responsibility is a must. With modern threats becoming apparent to us in the last several years, we understand that our traditional responsibility to ensure reliable service must include the need to ensure security. Breaches of security, obviously, can have extremely serious reliability consequences. From my vantage point, State commissions can identify certain key areas of concern about cyber security. The first concern focuses on business process systems — email, office computing, databases, etc. — that are not unique to utilities. In fact, commissions in recent years have improved their own security, along with everyone else, as attacks on these systems become more sophisticated and we become more dependent on them for our operations.

A second vulnerability is more specific to regulated utilities: control systems. Supervisory Control and Data Acquisition (SCADA) systems are already inextricably part of utility operations, and have served to improve the efficiency and reliability of our

system operations in every system throughout the country. In recent years, vulnerabilities to these SCADA systems have been repeatedly highlighted, perhaps most notably through the "Aurora" incident.

Finally, commissions have begun to probe the cyber-preparedness of our utility companies in the realm of smart grid. With tens of billions of dollars in investment on the line, commissions want to know that the investments aren't going to introduce new and unmanaged risks. In concept, the smart grid has the potential to provide many improvements in situational awareness, prevention, management, and restoration. In spite of introducing new vulnerabilities, smart grid fundamentally makes the electric system more secure. Still, this technology brings with it new vulnerabilities and points-of-access to create intentional disruption, which should be taken extremely seriously. "Guns-gates-and-guards" analogs of password protection and "security through obscurity" must be augmented with a framework of maximum system resilience and next-generation safeguards that allow the network to be impregnable, even if devices connected to it are compromised.

In each of these areas, steps are being taken to manage the risk. The regulated companies that we oversee have, through the North American Electric Reliability Corporation, developed standards for cyber security that we believe are a good step in the right direction for SCADA and business process systems. NERC, for example, has adopted a cyber-security standard for the bulk electric system. The question of how far that standard extends (i.e., to what extent it would reach down into the distribution

system) is not yet clear. NERC's cyber security ("CIP") standards are extensive and thorough. Over the past two years, electric utilities across the country have requested significant additional staffing and dollars for CIP standard compliance activities in their transmission rate case filings at FERC. The CIP standards already in place are adequate for both physical and cyber security. However, extending the applicability of those standards to lower voltage facilities raises the question of how much more we are willing to pay for a marginal increase in cyber security. The issue of how much more money should be put into this effort when it is virtually impossible to stop some cyber attacks (e.g., hackers getting into the Pentagon's computer system) needs to be addressed.

Smart grid poses an additional, and particularly thorny, policy issue as well. Through NARUC's collaborative with FERC on smart grid and through other activities, State commissions have also begun to identify key areas to assure that smart grid investments boast the highest, most sophisticated levels of security. Recent federal funding support for smart-grid investments has incentivized the deployment of hardware in advance of the development of standards for cyber security, among other issues. Commissions may be confronted with expenditures on cyber security for which no specific standard has yet been reached. This draws commissions into specific areas of review in order to determine the prudence of expenditures — a review that would be unnecessary if the expenditure would be made in compliance with recognized standards.

Commissions therefore have had to become more expert in their understanding of prudent smart grid and cyber security investments. Because we are not security

regulators, our interest in the area is driven only by our obligation to assure the reliability of service for our ratepayers and the prudence of the costs (including cyber-security spending) that goes into their rates.

Let me give you three examples of activity that commissions have engaged in to ensure that companies are focused on this issue.

Since 2005, the Pennsylvania Public Utility Commission has required all jurisdictional utilities to have a written cyber security plan to complement their emergency response, business continuity and physical security protocols, each of which are tested on an ongoing basis. Earlier this year, the Pennsylvania PUC issued an order on cyber security in reaction to media reports of grid infiltration by international hackers. Pennsylvania also issued a secretarial letter to its utilities encouraging them to be active in the NIST Standards development process by reviewing and commenting on the NIST Framework and the Cyber Security Coordination Task Group documents and to participate in various related working groups.

While Pennsylvania has not done specific audits, investigations or reviews of cyber-security plans on their own, it has incorporated cyber-security review in its management audits process. Pennsylvania performs management and efficiency audits at least once every five years on all electric, gas, and water utilities with over $10 million of plant in service.

Another State taking action is Missouri. Missouri requires all of its utilities to have in place reliability plans, and in May 2009 queried its utilities about steps taken or planned regarding cyber security as it relates to company operations. The Missouri Commission required the utilities to furnish Staff with a verified statement stating if the company is in compliance with NERC Order No. 706 or what actions and how long the company will take to become compliant. The Commission also asked what other organizations, groups, industry groups or other organizations these companies participate with, such as local FBI or State agencies, regarding security issues.

In my own State of New York we are sharing the responsibility for critical infrastructure protection at the Department of Public Service. Since 2003, when it was created, our Office of Utility Security has carried out a regular program of oversight of both physical and cyber security practices and procedures at the regulated utility companies in the energy, telecommunications and water sectors. Staff of this office is devoted full time to this security audit responsibility. Generally, we utilize the existing NERC CIP standards as benchmarks to form our own judgments about the quality of cyber security measures in place at the regulated utilities. Staff is adhering to a schedule that calls for visiting each regulated electric utility company four times a year to audit compliance with some portion of the CIP standards, with the goal of measuring compliance with all of the standards at each company over the course of a year.

We have the benefit in New York of a close and effective partnership with our umbrella State cyber security office. The NYS Office of Cyber Security and Critical

Information Coordination (CSCIC) directs efforts to maintain good cyber security practices within State government agencies. CSCIC also provides cyber threat and vulnerability information externally to several infrastructure sectors, establishing an excellent record for being a prompt and reliable source of such information. We at the Department of Public Service work closely and constantly with both CSCIC and our State Office of Homeland Security on infrastructure protection preparedness. We share information regularly and often through the Governor's Homeland Security Executive Council, and less formal daily interactions. We collaborate to provide joint briefings and notifications to utility company information systems managers regarding cyber threats and countermeasures, and just discovered vulnerabilities.

FEDERAL LEGISLATION

I would now like to briefly address legislation that is currently being considered in the 111th Congress. As I have previously stated in this testimony, NARUC believes that as Congress considers legislation in this area, it should build upon existing federal-State coordination and result in an environment where vulnerabilities to the system are identified, prioritized, and resolved in a timely fashion. Congress needs to distinguish between imminent threats, which require immediate action, and vulnerabilities, which can be resolved more deliberately.

Importantly, any legislation in this area should focus on the ability for federal agencies with information identifying priority vulnerabilities and imminent threats to

communicate with the various electricity providers, State and federal law enforcement entities, and State regulatory authorities. In nearly all situations, the electric power industry can protect the reliability and security of the bulk power system without government intelligence information. However, in the limited circumstances when the industry does need government intelligence information on a particular threat or vulnerability, it is critical that such information is timely and actionable. After receiving this information, the electric power industry can then direct its expert operators and cyber security staff to make the needed adjustments to systems and networks to ensure the reliability and security of the bulk power system.

In short, if the federal government is aware of a vulnerability or threat but does not effectively communicate that information to the utilities, how can they be expected to address these concerns? Additionally, State regulators must be given adequate information so that they are not in a position where they must sign a "blank check" for the mitigation of any federally identified vulnerability, which will then be passed onto ratepayers, along with potential new greenhouse gas mitigation costs.

We believe that neither H.R 2165, introduced by Representative Barrow, and H.R. 2195, introduced by Representative Thompson, or S. 1462 from Senator Bingaman, offer the needed guidance to ensure that the federal entities provide timely and actionable information to the energy providers or State government agencies. Perhaps provisions could be added to establish a process for federal intelligence agencies to provide the requisite security clearance to an employee with responsibility for cyber security. I am

told that there are employees at energy providers and some State agencies that have "secret" level clearance; however in some instances this level would not be adequate.

Second, the scope of legislation should be limited to cyber security on the bulk power system and in emergency situations. If the federal government has actionable intelligence about an imminent threat to the bulk power system, State commissions are ready, willing and able to provide any assistance or issue any complementary orders that may be necessary with regard to similar emergency situations on the distribution systems. In these limited circumstances, when time does not allow for classified industry briefings and development of mitigation measures for a threat or vulnerability, FERC in the United States and the appropriate corresponding authorities in Canada should be the government agencies that direct the electric power industry on the needed emergency actions. These actions should only remain in effect until the threat subsides or upon FERC approval of related NERC reliability standards.

In the United States, Section 215 of the Federal Power Act (Energy Policy Act of 2005) invested FERC with a significant role in bulk power system reliability, and it would be duplicative and inefficient to recreate that responsibility at another agency. It is our opinion that H.R. 2165 is preferable to the other bills in this regard.

Additionally, we recognize that it may be necessary for federal government authorities to intervene, should it have actionable intelligence about an imminent cyber threat that would harm our national security, with regard to distribution assets. In these

instances and in very limited locations federal actions could require certain actions to be taken by the electric power industry. However, we must insist that State commissions or other appropriate State agencies be fully included from beginning to end of the emergency situation. We would suggest that language be included in H.R. 2165 to address and limit the circumstances where this could occur.

In total, NARUC believes that H.R. 2165 takes the best approach to the issues that confront cyber security on our nation's electric system and we thank Representative Barrow, Chairman Waxman, and you Chairman Markey for introducing this legislation.

SPECIFIC SUBCOMMITTEE QUESTIONS

Mr. Chairman, in your invitation you requested that in my testimony I provide answers to seven questions you posed. I have alluded to some of them previously, and will attempt to provide general responses here:

1. What measures, if any, are state public utilities commissions taking to protect the electric grid against cyber security, EMP, or other vulnerabilities to and threats from malicious acts?

As regulators of investor-owned utilities, and, in some instances, municipal and co-op utilities, State commissions broadly become involved in their capacity to oversee reliable service and to ensure prudent expenditures by the electric utility companies.

Ensuring reliable service means holding utilities to high levels of performance in the face of all hazards. Commissions require utilities to comply with reliability standards and to possess emergency preparedness plans that minimize or eliminate the possibility of events with varying probabilities and consequences (ranging from hurricanes to insider acts). Moreover, commissions approve the prudence of expenditures on all activities, including critical infrastructure protection, via the rate case process.

Some commission staffs retain experts on security and critical infrastructure protection. The Public Utilities Commission of Ohio, the New Jersey Board of Public Utilities and the Michigan Public Service Commission are examples of commissions that have been integrated into their Governors' Homeland Security advisory infrastructure. Also, Colorado, New York and Texas have specific staffs detailed to this issue. Even when staff are not been designated with a security focus, NARUC's Committee on Critical Infrastructure has members from most States participating and staying abreast of national trends, issues, and best practices. This committee regularly educates and engages members in tabletop exercises, workshops, and dialogues on topics ranging from hurricanes to copper theft. Cyber security has been a core discussion topic for the past three years.

Specific to cyber security, commissions vary in their approaches. Some, such as New York, Texas, and Oregon, have or are acquiring specific expertise in cyber security. Others more indirectly rely on CIP standards compliance or reliability standards adherence to ensure that this area is addressed.

2. What gaps or limitations, if any, are there in the existing process and standards under section 215 of the Federal Power Act for ensuring that the electric grid is adequately protected against cyber security, EMP, or other vulnerabilities to and threats from malicious acts?

Through strong federal, State, public, and private partnerships, we have consistently maintained and improved reliability and security of the grid. As times and technologies have changed, new risks and vulnerabilities have emerged. The transition to a smarter, digital, more efficient grid — while full of promise — carries with it unforeseen concerns and unintended consequences. As Congress considers legislation in this area, it should build upon the existing federal-State coordination and result in an environment where vulnerabilities to the system are identified, prioritized, and resolved in a timely fashion. Congress needs to distinguish between imminent threats, which require immediate action, and vulnerabilities, which can be resolved more deliberately.

3. What new federal authority, if any, is needed to protect the grid against such vulnerabilities and/or threats – whether in the form of emergency response authority or standard-setting authority? If new authority is needed, what federal agency or agencies, or other entity (such as the North American Electric Reliability Corporation) should be tasked with such authority and how should it be structured?

NERC has adopted a cyber-security standard for the bulk electric system. NERC's cyber security ("CIP") standards are extensive and thorough. Over the past two years, electric utilities across the country have requested significant additional staffing and dollars for CIP standard compliance activities in their transmission rate case filings at FERC. The CIP standards already in place are adequate for both physical and cyber security. The question of how far that standard extends (i.e., to what extent it would reach down into the distribution system) is not yet clear and needs to be better defined. Extending the applicability of those standards to lower voltage facilities raises the question of how much more we are willing to pay for a marginal increase in cyber security. The issue of how much more money should be put into this effort when it appears virtually impossible to stop some cyber-attacks (e.g., hackers getting into the Pentagon's computer system) needs to be addressed.

4. If new federal authority is needed in this area, should it extend only to cyber security vulnerabilities and/or threats, or should it also address physical vulnerabilities and/or threats, or some subset thereof, such as vulnerabilities and/or threats specifically related to EMP or large transformers?

Cyber security may pose a new paradigm for some because of the ability of a cyber attack to be geographically remote from the affected area. As such where near-term threats are identified it may be relevant to introduce emergency authority by federal authorities.

For large transformers, programs are already being put into place, such as the Spare Transformer Exchange Program (STEP), the costs of which have already been approved by commissions in every participating footprint. No further federal authority is warranted in this area.

With regards to EMP, it is appropriate for the federal government to weigh the probability and consequence of this vulnerability, as without such analysis there is no basis for Federal authority. In the interim, EMP should be weighed among other vulnerabilities, and decisions made in circumstances that consider the cost-effectiveness of mitigation of this vulnerability against cost effectiveness for addressing a range of hazards. It is not an appropriate area for new federal authority unless a real threat (i.e., a new significant probability of occurrence) is identified, as there is a clear lack of authority on the part of other decision makers to manage this vulnerability.

5. If new federal authority is needed in this area, should it extend beyond the bulk power system to distribution system assets and/or Alaska, Hawaii, and U.S. territories? If any such extension beyond the bulk power system is warranted, should such extension be limited to some subset of "critical" assets, such as those serving defense facilities or major metropolitan areas? If so, how should such "critical" assets be defined?

With regards to cyber security, Alaska and Hawaii may also be subject to geographically dislocated attacks, and therefore emergency basis federal authority may

well be warranted. With regards to other physical and emerging threats, such as EMP, no such authority is relevant.

The question of cogently defining "critical assets" has eluded experts and specialists for a decade — it is a moving target dependent on circumstance. Most utility assets are critical at some level to some operation or constituency. Identification of essential assets is a routine element of utility and transmission operator activities, with hundreds of multiple failure level scenarios being modeled in real-time. The existing standards and practices that govern the level of preparedness by these operators is adequate and no new authority is needed unless a near-term threat, of significant consequence and probability, is identified

6. If new federal authority is needed in this area, how should treatment of sensitive information be addressed?

State commissions continue to deal with the treatment of sensitive information. While commercially sensitive and security sensitive information must be protected from FOIA and public release, a real risk emerges when those holding the information fail to connect decision-makers with the information that they need to take action. A partnership approach is warranted where any new authority is granted

7. If new federal authority is needed in this area, how should utilities' recovery of costs for compliance with federal directives be addressed, if at all?

Recovery of costs need not be addressed in this legislation. Currently, State rate regulated utilities have the ability to recover federally mandated costs, for example the Nuclear Waste Fund fees and acid rain mitigation costs. We do not see the necessity for different cost recovery treatment in this legislation.

CONCLUSION

A long-standing mission of the State public utility commissions is to ensure the physical viability of the utility plant under their supervision. A less traditional responsibility, cyber security and information systems standards and development, is increasingly thrust into the mix, yet this newer responsibility clearly envelops a broader range of industries and specific expertise. Utility regulators recognize the dependence of sound cyber security practices and cyber reporting on sound construction practices and utility-outage reporting, and visa versa.

A concern that I wish to leave with you for consideration is that protocols intended to distinguish between disruptions to critical infrastructure related to cyber events and those related to physical events, e.g., a denial-of-service attack as opposed to a fiber-optic cable failure, have not kept up with the fast-emerging nature of cyber threats. Such protocols are easier to craft than to implement. The first evidence of disruption is the disruption itself, and such events do not often present themselves with the root cause clearly visible.

In the critical "golden hours" after a possible new developing threat is detected, or immediately following an event, it may not always be clear what is actually happening or why. For this reason, close coordination between the utility sector and the cyber sector is essential to the response. As the State public utility commissions have traditionally served as the gateway to the utility sector and have their own independent core of expertise and relationships key to understanding in real-time events affecting that plant, close coordination among the operators of our cyber networks, the federal government, and State homeland security partners, including utility commissions, is essential.

Mr. Chairman and members of the Subcommittee, this concludes my testimony. State public service commissions take the issues of cyber security and reliability seriously. We believe a federal-State, public-private partnership is essential to meeting these challenges over the long term. I am now happy to answer any questions from the Subcommittee. Thank you.