WRITTEN TESTIMONY
OF
TODD A. SNITCHLER
CHAIRMAN, PUBLIC UTILITIES COMMISSION OF OHIO
BEFORE
THE U.S. SENATE COMMITTEE ON ENERGY AND NATURAL RESOURCES
FULL COMMITTEE HEARING ON CYBERSECURITY
TUESDAY, JULY 17, 2012

Chairman Bingaman, Ranking Member Murkowski, and Members of the Committee, thank you for this opportunity to appear before you today as you examine the status of action taken to ensure that the electric grid is protected from cyber attacks. My name is Todd Snitchler, and I am the Chairman of the Public Utilities Commission of Ohio (PUCO), the State agency responsible for:

- assuring residential and business consumers access to adequate, safe, and reliable utility services at fair prices;

- ensuring financial integrity and service reliability in the Ohio utility industry;

- promoting utility infrastructure investments (including investments in IT infrastructure); and,

- related items like fostering of competition, safety, and even mediation responsibilities.

I am pleased to have been given this opportunity to discuss cybersecurity issues for the electric grid. We take for granted the reliability of our nation's grid and we are hyper-sensitive when we lose power because we are not generally accustomed to it – nor should we be.

Should Congress decide to pass legislation on cybersecurity, however, it must distinguish between imminent threats, which require immediate action, and vulnerabilities, which can be addressed and resolved more deliberately. Particularly regarding the electric grid, one-size solutions for cybersecurity may not be the most effective means to mitigate and reduce known vulnerabilities. Additionally, the

desired outcome for such legislation should be the establishment of a foundation that contemplates at least four basic considerations.

First, let us protect diamonds like diamonds and apples like apples. That is, we must prioritize accordingly to ensure that the appropriate level of security is provided to all areas that require protection.

Second, States and the owners of the critical infrastructure we regulate cannot protect the infrastructure to the maximum extent possible unless relevant Federal agencies provide the actionable information necessary to identify and address the threat and/or vulnerabilities – in other words true information sharing between those that have critical information (the Federal agencies) and those that need such information to protect their systems.

Third, our utilities can provide a "gold-plated" or even a "platinum-plated" system which is ultra-cyber secure. However, this raises the question of just how much more do we want a kilowatt hour of electricity to cost? While we understand that if the lights are not on it does not matter what the cost of the electricity is, do we really want the critical infrastructure to be so expensive that due to cost constraints it is no longer considered critical?

Fourth, preparedness should not focus solely on response capabilities, but should also ensure that resilience is built into our infrastructure - 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 significant storms, hurricanes, earthquakes, wildfires, and even acts of terrorism.

As a State regulator, my fellow Commissioners and I, as well as our Staff, have many responsibilities. Some items of significance today are resolved and become less significant down the road. Other items that are less significant today may become of paramount importance in the near future with a major change in one variable like weather, for instance. This is true for many things, including the provision of electricity in a safe, reliable and economic fashion. Focusing on reliability, there are many factors that impact that aspect – physical infrastructure in place and operational considerations, such as generators, wires, substations, transformers, and meters. Also greatly impacting reliability is equipment failure. Equipment may fail due to its age, its overuse or underuse, physical vulnerabilities, and as we are aware, perhaps due to cyber vulnerabilities. Many of these vulnerabilities have existed and are known, while other weaknesses are more recently being better understood. Just as the electric utilities cannot protect against all threats, neither can they eradicate all susceptibilities. But we must recognize there are different parts of these systems that require different levels of protection. This is why we must ensure that there is adequate protection for the electric grid, especially the most valuable parts, while we must not expend undue levels of resources in protecting other, less important parts of the system.

Another important point of consideration that must be recognized is that State agencies like the PUCO, along with the owners of our critical infrastructure, are unable to provide the full measures of protection necessary to help secure our nation's critical infrastructure if the relevant Federal agencies do not provide actionable information to address imminent threats. 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, 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.

However, identification of vulnerabilities is only one part of the main equation; equally, or even more importantly, is a need by the States and especially by the asset owners to recognize the threats to the nation's grid. We hear consistently from asset owners who provide information about their systems to Federal agencies in the spirit of cooperation, all the while seeking reciprocity, yet they never receive truly meaningful, actionable, timely information in return. They cannot protect all of their systems against everything; none of us can. They have to target their defenses and we have to help them understand the actionable threats so that they may bolster their defenses where needed.

As with most sectors of the economy, information systems are rapidly merging with utility systems, potentially heightening the risks of service disruption. Cybersecurity is an emerging area of risk for our utilities and for State Commissions as well; 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 this merging of information systems into the electric and other utility sectors improves their resilience, reliability and efficiency.

National security roles and responsibilities have been subject to the purview of Emergency Management Agencies, State Police, and Departments of Homeland Security. However, 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 now. 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 – both physical and cyber. Breaches of security, obviously, can have extremely serious reliability consequences. From my vantage point, State commissions can identify certain key areas of concern about cybersecurity. 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 have been and remain an inextricable 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, susceptibilities in these SCADA systems have been repeatedly highlighted.

Over the past several years, State 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 are not going to introduce new and unmanageable 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 weaknesses, 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, through the North American Electric Reliability Corporation (NERC), are continuously in a process of developing and updating standards for cybersecurity 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. NERC's cybersecurity ("CIP") standards are extensive and thorough. Over the past five 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 security 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 cybersecurity. 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 cybersecurity, among other issues. Commissions may be confronted with expenditures on cybersecurity 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 cybersecurity investments. Because we are driven by our obligation to assure the reliability of service for our ratepayers, we must better understand the prudence of the costs in ensuring reliability (including expenditures for cyber-security) that goes into their rates. As a result, our agency has expended significant time and resources to become better educated regarding cybersecurity. Over the past several years, as the electric industry aptitude has grown regarding cybersecurity, so too has that knowledge base grown across State commissions.

In Ohio, for instance, regarding the smart grid discussion above, an extensive audit was conducted to assess the degree to which Duke Energy Ohio's Smart Grid system complied with the NISTIR 7628 and industry best practices and identify potential areas of improvement, which was a precursor to the action items in the stipulation. An internal audit was also provided during the audit and included penetration testing on a number of Smart Grid assets. An extension stipulation was reached regarding Duke's cybersecurity plan and the implementation of that plan, including the role of the Commission. This effort was massive and will become a best practices model for other commissions and utilities in their cybersecurity analyses and efforts.

We have been very involved in the NIST's and now the Smart Grid Interoperability Panel's (or SGIP's) Cyber Security Working Group. My agency has been very active in pursuing cybersecurity training opportunities with Idaho National Labs, NIST & NIST's ITL Computer Security Division, the SGIP, EnerNex, NERC's Grid Security Conference, and others, as well as participating in the development of the initial NIST-IR 7628, the most recent version being a multi-volume compendium of Smart Grid Cyber Security Strategy and Requirements. We have actively participated in the National Association of Regulatory Utility Commissioners (NARUC) Cybersecurity Boot Camps. Additionally, our Staff participates in two different sets of regular, twice-monthly conference calls with our colleagues from across the country. These calls address critical infrastructure protection issues, cybersecurity issues for utilities, as well as smart grid development and implementation issues. Our Staff participates in monthly threat briefings for both the electric sector as well as the oil and natural gas sector. Also, our Staff regularly participates in weekly briefings with Ohio Homeland Security. Through this partnership, our agency has a permanent seat at the State of Ohio's Strategic Analysis and Information Center (or SAIC), just as it does in our State of Ohio Emergency Operations Center. Presently, the State of Ohio has developed a Statewide Cybersecurity Strategy and our Staff has been actively engaged in both the development as well as the on-going implementation of that strategy. Over a year ago, my agency conducted a cybersecurity workshop for our

utilities as well as for our State and Federal partners. Leading part of that workshop was a representative from the U.S. Department of Energy's Cybersecurity for Energy Delivery Systems program. Also participating was Ohio's Homeland Security Advisor, as well as representatives from the cyber squads from both of the FBI divisions in Ohio. In addition, the two U.S. Department of Homeland Security (DHS) Protective Security Advisors stationed in and serving Ohio addressed not only their physical protective security program, but also DHS's cybersecurity advisor program and the related cyber resources and tools available from DHS for asset owners. Our efforts in strengthening the cybersecurity posture of Ohio's utilities continue.

Ohio also has one of the premier military bases in the country – Wright-Patterson Air Force Base. Located in the south-western portion of the state, this base employs a significant number of personnel and performs mission-critical work for the Department of Defense. My agency has worked with this base in the past, and will do so in the future, to ensure that it has what it needs to accomplish its objectives.

While I am not an expert on what other States are doing with regard to cybersecurity, I am aware of a few examples of activity that State commissions have engaged in, to ensure that companies are focused on this issue. In most instances these activities are coordinated with other State agencies that also have a jurisdictional responsibility for safety and/or security.

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. The Pennsylvania PUC has issued orders on cybersecurity 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. Pennsylvania has also 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 has queried its utilities about steps taken or planned regarding cybersecurity as it relates to company operations. The Missouri Commission required the utilities to furnish Staff with a verified statement affirming whether the company is in compliance with NERC Order No. 706 or what remedial actions are to be taken and how long it will take the company 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 New York, they are sharing the responsibility for critical infrastructure protection at the Department of Public Service. Since 2003, when it was created, the New York State Public Service Commission Office of Utility Security has carried out a regular program of oversight of both physical security and cybersecurity 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, that office utilizes the existing NERC CIP standards as benchmarks to form its own judgments about the quality of cybersecurity measures in place at New York's regulated utilities. Its Staff adheres 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.

The Public Utility Commission of Texas has established a stakeholder working group (comprised of utilities and ERCOT Staff) designed to work on issues specific to cybersecurity. This effort is lead by Texas Commission Staff. The group meets regularly to discuss the cybersecurity assessments performed on Smart Meter Texas, which is the common portal that provides end-user access to energy usage data sourced from the AMI that was deployed by the respective utilities. Each utility is responsible for securing its own AMI and cybersecurity assessments are required of the utilities by rulemaking once deployment of AMI and other smart grid technology is approved. Regulations include requirements for end-to-end assessments, performed independently and annually of the utility system. These results are kept confidential but shared with the Staff.

In addition commission staff participates in the discussions at the ERCOT ISO Critical Infrastructure Protection Working Group (CIPWG), in which NERC CIP issues are discussed. While this concerns the bulk electric system, other topics related to cybersecurity that are broached include: newly discovered vulnerabilities; emerging threats to critical infrastructure; cybersecurity standards development from outside NERC; mission assurance for the military; and any cybersecurity training opportunities, conferences, workshops, or exercises.

A long-standing mission of State public utility commissions is to ensure the physical viability of the utility plant under their supervision. A less traditional responsibility, that of cybersecurity 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 cybersecurity practices and cyber reporting on sound construction practices and utility-outage reporting, and vice 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, for example, a distributed-denial-of-service (DDOS) 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 State utility commissions, is essential. Resolving cybersecurity issues will require significant efforts on the parts of all of us, not just one or two of us. We all are part of the solution. Working with the asset owners and with our Federal partners, the States have been successful in the past in enhancing the overall reliability of our nation's electric grid. Our Federal government possesses significant assets that can provide States and the critical asset owners with timely and actionable threat information necessary to better secure these assets. We are partners in this struggle to maintain and enhance the reliability of our electric grid and to increase its resiliency, and we must all work together to achieve our collective goal.

Mr. Chairman and members of the Committee, this concludes my testimony. We at the Public Utilities Commission of Ohio take the issues of cybersecurity and reliability very seriously. As such, we believe a Federal-State, public-private partnership is essential to meeting these challenges over the long term.

Thank you again for the opportunity to provide testimony here today and I would be happy to answer any questions that you or members of the Committee may have.