Written Statement of Richard Dewey
Executive Vice President
New York Independent System Operator

Senate Standing Committee on Veterans, Homeland Security and Military Affairs
Senator Thomas D. Croci, Chairman

Senate Standing Committee on Codes
Senator Michael F. Nozzolio, Chairman

Senate Standing Committee on Consumer Protection
Senator Michael Venditto, Chairman

Public Hearing

"To Address New York State's Cyber Security Infrastructure"

May 20, 2015

I. INTRODUCTION

My name is Richard Dewey. I am Executive Vice President of the New York Independent System Operator. The NYISO is an independent not-for-profit corporation that carries out three key functions relating to the electric system serving New York State. We are responsible for the reliable operation of New York's bulk electric system in accordance with all national, regional and state reliability requirements. We administer and monitor competitive wholesale electricity markets to satisfy electrical demand, providing benefits to consumers. We plan for the reliability and power demands of the future and participate as technical advisor and

non-voting member of the New York State Energy Planning Board. As an independent resource, we provide authoritative information and objective analysis to market participants, regulators and policymakers.

The NYISO is governed by an independent Board of Directors and a shared governance structure comprised of representatives from every industry sector, including consumer interests, generators, transmission owners, municipalities, and environmental interests. The New York State Department of Public Service, the New York State Utility Intervention Unit, the New York Power Authority, the Long Island Power Authority and the New York State Energy Research and Development Authority actively participate in the NYISO's shared governance process.

I joined the NYISO in 2000. In my role, I am responsible for overseeing grid and market operations, system planning, information technology, and market structures. Until January 2015, I served as Senior Vice President and Chief Information Officer. The NYISO's Information Technology group delivers products and services to evolve the wholesale electricity markets; develops, supports, and secures all NYISO software, systems, and computing infrastructure; and manages the NYISO's physical facilities and enterprise security. I have a Master of Science in Computer Engineering from Syracuse University and a Bachelor of Science in Electrical and Computer Engineering from Clarkson University in Potsdam, New York.

II. Fifteen Years of Competitive Markets & Continued Evolution of the Grid

New York's 19 million consumers today enjoy benefits made possible by the decisions by policymakers in Albany and Washington in the 1990s to reinvent the electricity marketplace. Competitive markets have sustained and enhanced the vital reliability of the electric system in New York. Markets encourage investment where it is most needed to meet reliability needs and

markets support the development of cleaner, greener, more economically efficient power resources.

Several regulatory entities provide guidance and oversight on operation of our energy markets and the operation of New York's high-voltage grid including the Federal Energy Regulatory Commission (FERC), the New York State Public Service Commission (PSC), the North American Electric Reliability Council (NERC), the Northeast Power Coordinating Council (NPCC), and the New York State Reliability Council (NYSRC). In support of its mission, the NYISO maintains strict compliance with the rules and standards set forth by these entities.

II. IMPROVING CRITICAL ENERGY INFRASTRUCTURE CYBERSECURITY

The entities that own and operate America's critical infrastructure recognize the criticality of mature cybersecurity practices to protect the assets and systems that enable American life. As well-organized threats evolve and security breaches increase, nimble and multi-faceted defenses are essential. The electric industry is at the forefront of developing standards and best practices for protecting critical information and communication systems.

Enacted in response to the August 2003 Blackout that affected New York and the Northeastern United States, the Energy Policy Act of 2005 empowered FERC to oversee the development of mandatory, enforceable reliability standards to protect bulk electric systems nationwide. FERC certified NERC as the Electric Reliability Organization for the United States. Since 2006, NERC has promulgated reliability standards including critical infrastructure protection (CIP) cybersecurity standards. In 2016, NERC will begin enforcing Version 5 of the CIP standards. CIP Version 5 requires that entities conduct an in-depth, risk-based analysis to identify, classify and protect the cyber systems and cyber assets that support physical

infrastructure. These CIP standards set forth holistic security requirements such as access control, physical and electronic security perimeters for assets critical to system reliability, recovery plans, well-documented change management and information protection programs, security monitoring and alerting, and employee training and background checks. Additionally, NERC standards require incident management programs that support mandatory reporting of cyber and physical security incidents.

Beyond mandatory standards, the electric industry is engaged with voluntary efforts led by the White House and federal agencies such as the Department of Energy (DOE), Department of Homeland Security (DHS), and Federal Bureau of Investigation (FBI) to improve sector-wide resilience for cyber threats. For instance, the industry—and the NYISO—have supported federal response to Executive Order 13636 and Presidential Policy Directive 21. Issued in March 2013, they represent an effort led by DHS to secure our nation's critical infrastructure by working with infrastructure asset owners and operators to prepare for, prevent, mitigate, and respond to threats. In response to EO 13636 and PPD 21, the federal government and industry are partnering to bolster cyber security by, among other things, promoting and incentivizing cybersecurity best practices and updating the National Infrastructure Protection Plan. The electric industry also devotes substantial resources to information sharing for enhanced security awareness. For instance, the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) receives and shares physical, operational and cybersecurity threat indications, analyses and warnings. Finally, the electric industry conducts sector-wide grid security exercises that execute the electricity sector's crisis response to simulated coordinated cybersecurity and physical security threats and incidents. These "GridEx" exercises strengthen utilities' crisis response functions and support continuous improvement through lessons learned.

The NYISO, working with its stakeholders, peer Independent System Operators and Regional Transmission Organizations, and the broader electricity industry, strives to be a leader in addressing cybersecurity issues related to the protection of critical infrastructure. To that end, the NYISO regularly participates in standards development processes, including development of the NERC CIP Version 5 standards. The NYISO works closely with industry groups and standards organizations, and engages in regional, national, and international planning initiatives addressing future technology and security integration. Keeping the lights on is always the primary focus for the NYISO. Cybersecurity is critical to that effort.

The NYISO's own cyber security posture is premised on continuous evaluation of its assets, vulnerabilities, and threats. Situational awareness enables real-time effective security risk assessment. The NYISO employs a "defense in depth" strategy that relies on processes, technologies, and people to protect our assets. Cutting-edge security technology and processes are critical; NYISO works with its developers, security professionals and vendors to identify the best and most responsive technical resources to support security and maintain reliability. Yet technology and processes are only as good as the employees and vendors that deploy them. Accordingly, the NYISO is always focused on maintaining a well-trained work force and carefully screening its vendors and employees to counter the risk of "insider threats."

III. LEVERAGING GOVERNMENT PARTNERSHIPS

While the energy industry is a leader in self-driven cybersecurity advances, partnerships with federal and state governments are essential to timely detecting and identifying threats as they occur and deploying effective responses.

As noted above, at the federal and national level the NYISO is engaged with the Electricity Subsector Information Sharing and Advisory Center (ES-ISAC), DOE, DHS, FBI and private vendors and partners such as Center For Internet Security (CIS), as well as its regulators FERC and NERC. In addition to supporting the policy and standard development advanced by these agencies, the NYISO relies on its collaborative relationships with them for classified briefings and real-time cybersecurity information sharing and threat detection.

On a state level, the NYISO works regularly and collaboratively on security initiatives with a number of state and local agencies including the Department of Public Service, Division of Homeland Security and Emergency Services, New York State Police, New York City Police Department SHIELD, and the New York Fusion Center. Given its commitment to ensuring reliable electric supply for all New Yorkers, the NYISO must rely on—and strongly supports—a well-coordinated local response to cyber threats. To that end, on October 22-23, 2014 the NYISO hosted the DOE-sponsored New York State Critical Infrastructure Cybersecurity Exercise. More than 120 participants from 13 electric and gas utilities, industry organizations, federal, state, local, tribal and neighboring territorial government entities participated. The Exercise walked participants through a facilitated scenario involving a cyber attack on critical infrastructure that led to both cyber and physical consequences for energy delivery systems. The Exercise tested incident response and demonstrated the need for, among other improvements, enhanced collaboration with and among New York state agencies in response to cybersecurity incidents, such as by formation of a New York or regional "decision tree" for incident response and information sharing. The NYISO, along with various New York utilities and in conjunction with government partners, are forming a New York State Security Working Group to address identified needs and hold future similar exercises.

IV. **CONCLUSION**

In support of its mission to serve New York and enhance reliability, the NYISO looks forward to supporting this Committee's efforts to enhance New York's cybersecurity infrastructure. Thank you for the opportunity to provide this testimony.