New Jersey Board of Public Utilities

NEWS RELEASE

For Immediate Release: March 18, 2016	**Contact:** Greg Reinert 609-777-3305

Christie Administration Adopts Comprehensive Cybersecurity Requirements for Regulated Utilities

The New Jersey Board of Public Utilities (Board) today adopted a set of comprehensive cybersecurity requirements for the regulated electric, natural gas, and water/wastewater utilities as part of the Christie Administration's efforts to further reduce the potential of cyber threats from impacting the reliability and resiliency of utility service and to protect customers' information. The requirements placed on the regulated utilities were developed in consultation with experts in utility cybersecurity, New Jersey Cybersecurity & Communications Integration Cell (NJCCIC) and the Federal Bureau of Investigation.

"As cyber-attacks against utility systems nationwide continue to increase in number and sophistication, addressing cybersecurity is a top priority to enhancing the security and reliability of utility service in New Jersey and across the nation," said Richard S. Mroz, President of the N.J. Board of Public Utilities. "To ensure that we continually meet the challenges of this ever changing threat, we have made certain that these policies are uniform yet flexible, promote information sharing and are capable of evolving as the threat landscape changes."

The Board's action directs electric, natural gas, and water/wastewater utilities to implement the following cybersecurity requirements:

- A cybersecurity program that defines and implements organization accountabilities and responsibilities for cyber risk management activities, and that establishes policies, plans, processes, and procedures for identifying and mitigating cyber risk to critical systems;
- Conduct risk assessments and implement appropriate controls to mitigate identified risks;
- Maintain situational awareness of cyber threats and vulnerabilities;
- Report cyber incidents and suspicious activity to Board Staff via the NJCCIC;
- Create and exercise Incident Response and Recovery Plans; and,
- Provide cybersecurity awareness and training programs.

Today's Board approved requirements are in addition to previous approved measures enacted to address the potential of cyber threats. In 2011, the Board directed the regulated utilities to identify their use of industrial control systems, including Supervisory Control and Data Acquisition (SCADA) to monitor and/or remotely control utility facilities and to report certain security events. Subsequently, the Board worked with the NJCCIC and utility workgroups to develop Cyber Best Practices. While the industry has a strong record of working together and with government partners to identify, assess, and respond to cyber threats, today's Board action requires a more comprehensive risk management approach to cybersecurity among the regulated utilities in New Jersey.

Additionally, the Board continues to participate in a cybersecurity collaboration with NJCCIC, the NJ Attorney General's Office, NJ State Police, FBI, US Department of Homeland Security, and the private sector as we continually assess the cyber threat environment and its impact on utilities.

###