



**For Immediate Release**  
July 22, 2016

Bob Gough  
217-782-5793  
[bgough@icc.illinois.gov](mailto:bgough@icc.illinois.gov)

### **ICC Hosts Cybersecurity Policy Session**

CHICAGO – On Thursday, The Illinois Commerce Commission hosted a Cybersecurity Policy Session that focused on the specific roles of government, industry, and third-party stakeholders in protecting the nation’s critical energy infrastructure.

Following the December 2015 Ukrainian power outage, which left more than 225,000 customers powerless for six hours, as well as other recent indications of cyber espionage targeting the United States, state regulators have started asking questions of their utilities and taking steps to gauge the cyber vulnerabilities that exist in the Nation’s critical utility infrastructure, including electricity, gas, water and telecommunications.

While cybersecurity has not traditionally been addressed by state public utility regulators, this emergent threat has made it necessary for regulators to discern how to best protect the services, data and information valuable to the customers and companies they serve. In an effort to ensure adequate, safe and reliable public utility services, the ICC convened today’s policy session to address these cybersecurity concerns.

“Cybersecurity is a concern across all sectors, as hackers know how much we rely on utilities,” said ICC Commissioner Sherina Maye Edwards, who coordinated the policy session. “As such, today’s session serves the important purpose of beginning a strategic dialogue between cybersecurity leaders to encourage information sharing and illuminate how all parties must work together to contribute to the fabric of the nation’s cybersecurity policy.”

The session’s first panel, The Role of Government in Cybersecurity, moderated by ICC legal and policy advisor Annie McKeon, brought government officials at the state, federal and local level together to provide updates on ongoing security initiatives and how these efforts are coordinated between government and industry.

“The government’s role in cybersecurity is like a neighborhood watch,” said Robert Ivanauskas, an attorney-advisor with the Federal Energy Regulatory Commission’s Office of Energy Infrastructure Security. The key, he noted, is testing and developing ongoing plans to respond to potential threats. “We’re all looking out for the bad guys and you can stop them on a nationwide scale and potentially even further.”

Kirk Lonbom, Chief Information Security Officer for the State of Illinois, said the State’s new Department of Information Technology (DoIT) has a vision “to not just protect state agencies, but to make Illinois the most cyber-secure state in the country.”

The private sector then offered its perspective in the second session, Industry Response to Cyber Challenges, moderated by ICC legal and policy advisor Nakhia Crossley. Industry representatives discussed strategies, success stories, challenges, and opportunities to improve the nation's utility critical infrastructure.

"The next 9/11 will be a cyber-9/11," said John Goode, Senior Vice President and Chief Information Officer for MISO. "It's in everyone's best interest to be proactive in protecting these assets."

In the day's final panel, Strategies for Implementing Cybersecurity Measures, panelists discussed best practices, industry frameworks and opportunities to provide guidance for individual organizations to increase the cybersecurity posture of the nation's critical utility infrastructure as a whole.

Panelists noted that with increasing news of cyber-attacks, it is important for state regulators to use their position to coordinate efforts between government, utilities and industry experts alike to share best practices for responding to emerging threats and protecting critical utility assets.

"We have to be right 100 percent of the time," said Anabelle Lee of the Electric Power Research Institute. "The bad guys only have to be right once. In terms of cybersecurity, we will get attacked. The focus is on resilience."

Other Session participants included Tina Hauri, Chief Information Security Officer, City of Chicago; William Lucas, Director of Information Technology Security and Compliance, WE Energies; Nicholas Santillo, Vice President, Internal Audit and Chief Security Officer, American Water; Mary P. Heger, Senior Vice President and Chief Information Officer, Ameren; Jennifer Rathburn, Partner, Quarles & Brady; Bob Lockhart, Manager, Cybersecurity Programs, Utilities Technology Council; and Sharla Artz, Director of Government Affairs, Schweitzer Engineering Laboratories, Inc., United States Energy Association.

Presentations from the Session will be available at a later date at [www.icc.illinois.gov](http://www.icc.illinois.gov).

###

Follow the Illinois Commerce Commission on twitter [@ILCommerceComm](https://twitter.com/ILCommerceComm).

### ***About the Illinois Commerce Commission***

The Illinois Commerce Commission's mission is to pursue an appropriate balance between the interests of consumers and existing and emerging service providers to ensure the provision of adequate, efficient, reliable, safe and least-cost public utility services. The Commission pursues this mission through three bureaus: The Bureau of External Affairs, which provides educational information on utility issues for consumers, governmental entities and communities and through its Consumer Services Division, resolves customer/utility disputes and develops rules on utility service and consumer protection; the Public Utilities Bureau, which focuses on financial and operational analysis, policy development, public safety and enforcement activities related to electric, natural gas, water, sewer and telecommunications companies; and the Transportation Bureau, which includes trucking insurance and registration, railroad safety, relocation towing, safety towing and household goods moving company enforcement activities. The ICC's five commissioners are appointed by the Governor and approved by the Illinois State Senate for five-year terms.