Resolution Regarding Cybersecurity

WHEREAS, The National Infrastructure Protection Plan (NIPP) identifies Energy, Communications, and Water as interdependent national critical infrastructures; *and*

WHEREAS, Extended interruption to reliable utility service has cascading secondary impacts capable of causing significant harm to public health, public safety, and the economy; *and*

WHEREAS, Threats to critical utility infrastructure from all extraordinary events, natural or man-made, have the potential to interrupt reliable utility service; *and*

WHEREAS, Man-made threats can take the form of attacks on both physical and cyber assets; *and*

WHEREAS, Cyber attacks may be undertaken to infiltrate the control systems which operate and maintain our most critical utility infrastructure including Supervisory Control and Data Acquisition systems (SCADA) which regulate our water and wastewater treatment and distribution, transmission and distribution of electricity and natural gas, and communication networks for the very purpose of causing disruption or harm to public health, public safety, government, and the economy; *and*

WHEREAS, Threats to control-systems through breaches of cyber security may be initiated by any number of sources including but not limited to hackers, disgruntled current or former employees, criminal enterprises, terrorists, and foreign governments; *and*

WHEREAS, Threat of cyber attack against control systems cannot be eliminated but actions can be taken to reduce the likelihood of a successful attacks, to mitigate the harmful consequences of an attack, and to improve a utility's ability to improve system protection and restoration from future attacks, and thus enhance the resiliency of critical utility systems; *and*

WHEREAS, Measures to prevent an attack or mitigate its consequences come with costs which must be balanced against the likelihood of the threat and the significance of the potential harm; *and*

WHEREAS, Recognized industry-specific standards exist which identify protocols for protection from the threat of cyber attack on critical electric, gas, telecommunications, and water infrastructures; *and*

WHEREAS, Federal Energy Regulatory Commission (FERC) Order No. 706, Mandatory Reliability Standards for Critical Infrastructure Protection, issued on January 8, 2008, approves eight Critical Infrastructure Protection (CIP) Reliability Standards submitted to FERC by the North American Electric Reliability Corporation (NERC) which require certain users, owners, and operators of the Bulk-Power System to comply with specific requirements to safeguard critical cyber assets; *and*

WHEREAS, The U.S. Department of Energy (DOE) has designated NERC as the electricity sector coordinator for critical infrastructure protection; *and*

WHEREAS, NERC has constituted a Critical Infrastructure Protection Program to coordinate all NERC efforts to improve both physical and cyber security, including standards development, compliance enforcement, assessments of risk and preparedness, disseminating critical information via alerts to industry, and raising awareness of key issues; *and*

WHEREAS, the U.S. Department of Commerce and National Institute of Standards and Technology (NIST) have issued a report on Smart Grid Cyber Security Strategy and Requirements that provides the NIST Smart Grid Cyber Security Coordination Task Group's overall cyber security strategy for the Smart Grid; *and*

WHEREAS, The gas industry largely relies upon the Security Practices Guidelines developed by the U.S. Department of Transportation's Office of Pipeline Safety[1] and the U.S. Department of Homeland Security's Transportation Security Administration; *and*

WHEREAS, The Network Reliability and Interoperability Council (NRIC) in collaboration with the Federal Communication Commission (FCC) maintains a repository of Best Practices[2] for the telecommunications industry; *and*

WHEREAS, The U.S. Environmental Protection Agency (EPA) oversees cyber protection efforts for the drinking water industry through mandated vulnerability assessments and support training for emergency response to threats from breaches of cyber security; *and*

WHEREAS, The threshold for measuring cyber security is unclear and industry compliance standards are constantly changing to meet the threats of cyber-attacks, making it increasingly difficult to ensure cyber-secure systems; *now, therefore be it*

RESOLVED, That the Board of Directors of the National Association of Regulatory Utility Commissioners, convened at its 2010 Winter Committee Meetings in Washington, D.C., recognizes the need for continued vigilance against all potential sources of cyber threat to be both prepared to prevent cyber attacks capable of disrupting utility services and to mitigate the harmful consequences of such attacks in order to protect public health, public safety, and the economy; *and be it further*

RESOLVED, That NARUC encourages commissions to make efforts to give the highest priority to ensure that cyber security will be consistently monitored and evaluated to remain effective to meet ongoing threats to the utility systems in collaboration with those agencies having expertise in cyber threat management and mitigation; *and be it further*

---

[1] "The Role of State Public Utility Commissions in Protecting the National Utility Infrastructure: Cost Recovery, Sensitive Information, and Security Guidelines," NRRI Briefing Paper (March 2005).

[2] See https://www.fcc.gov/nors/outage/bestpractice/ProcessBestPractice.cfm?RequestTimeout=500

RESOLVED, That NARUC encourages commissions to open a dialogue with their regulated utilities to ensure that these organizations are in compliance with standards, and where applicable, ensure that cost-effective protection and preparedness measures are employed to deter, detect, and respond to cyber attacks, and to mitigate and recover from their effects; *and be it further*

RESOLVED, That NARUC supports member commissions in becoming and remaining knowledgeable about these threats, and ensuring that their own staffs have the capability, training, and access to resources to adequately review and understand cyber security issues that enhances expertise in the review of cyber security aspects of filings by their jurisdictional utilities; *and be it further*

RESOLVED, That NARUC encourages commissions to regularly revisit their own cyber security policies and procedures to ensure that they are in compliance with applicable standards and best practices, such as those of the National Institute of Standards and Technology (NIST) and Certification for Information System Security Professionals (CISSP).

Sponsored by the Committees on Critical Infrastructure, Electricity, Telecommunications, and Gas
Adopted by the NARUC Board of Directors, February 17, 2010