Our Mission
Protecting Our Legacy
Building Our Future

31st Constitutional Convention, Las Vegas, NV

Strengthen Cyber and Physical Grid Security

WHEREAS, As the electric grid becomes more distributed and interconnected, inadequate cyber security is a cause for alarm. With the development of the smart grid, there is concern that if not implemented securely, the electric grid could become even more vulnerable to attacks and loss of service. Hackers have been increasing their attacks on energy and other critical infrastructure, as well as targeting supervisory control and data acquisition systems; and

WHEREAS, The greatest cyber threats to the grid have been intrusions focused on manipulating industrial control system (ICS) networks. Cyber intrusions on the electric grid have resulted in malware on ICS networks with the capability of causing damage or taking over certain aspects of system control or functionality. Recent concerns have extended to Internet of Things (IoT) — devices connected to networks; and

WHEREAS, Large, high voltage electric power transformers (LPTs) are a particularly critical component of the bulk electric system which could be targeted in physical and cyber attacks; and

WHEREAS, As far back as 2012, the National Research Council (NRC) recognized the vulnerability of the electric power delivery system to either cyber and/or physical attacks. An NRC report concluded that terrorists could black out a large region of the country for weeks or even months, leading to turmoil and widespread public fear. If such large extended outages were to occur during times of extreme weather, they could also result in hundreds or even thousands of deaths; and

WHEREAS, The 2013 attack on the Metcalf substation in California further exposed the physical vulnerabilities of the grid. After someone broke into a nearby underground vault to cut telephone cables, snipers opened fire on the substation, knocking out 17 large power transformers that provided power to the Silicon Valley; and

WHEREAS, In 2015, a cyber attack on distribution utility substations in Ukraine shut off power to over 225,000 utility customers for several hours. It was the first time that a cyber attack was publicly acknowledged to have caused a grid power outage. The potential for a similar attack on the U.S. grid was then seen as a possibility; and

WHEREAS, Reports of foreign hackers targeting the U.S. electric power system and other critical infrastructure are increasing. An alert based on analysis by the Federal Bureau of Investigation and the Department of Homeland Security warned that Russian hackers have mounted a methodical, long-term campaign to infiltrate and surveil critical U.S. infrastructure, including energy and nuclear. The private security firm Dragos issued a report noting a rise in targeted attempts to infiltrate utility systems coming from North Korea-related hackers; and

WHEREAS, Regulators rely on utilities to self-report violations and follow audit findings. The Federal Energy Regulatory Commission (FERC) has lodged about 250 penalty cases against U.S. utilities in the past decade for violating rules designed to protect essential infrastructure. Cyber attacks are happening in large numbers, but utilities seldom report successful attacks as required, even when assured of confidentiality. Recently, FERC has started requiring utilities to report even unsuccessful hacking attempts.

THEREFORE BE IT RESOLVED, The benefits of implementing reasonable cyber and physical security controls significantly outweigh the economic and national security risks associated with not having adequate controls; and

BE IT FURTHER RESOLVED, The UWUA applauds the additional steps the federal government has taken to improve grid security, including establishing a new office within the Department of Energy with responsibilities for both physical and cyber security; and

BE IT FURTHER RESOLVED, Relying on defensive techniques such as software patching, anti-malware tools, creating strong perimeters and air-gapped networks is not enough to ward off future attacks. We call on utilities and grid operators to consider a combination of tools and evolving countermeasures. Interaction with 3rd party vendors must be rigorously screened. Best practices must be implemented wherever possible to defend against the traps hackers set to access systems. Communications across the entire energy system must be made as secure as possible; and

BE IT FINALLY RESOLVED, The UWUA calls on utilities and grid operators to: safeguard the privacy of consumers' data; create a culture of constant cyber vigilance; share information with each other and appropriate authorities about existing and emerging threats; and to ensure they have the resources to acquire the requisite tools to accomplish these additional tasks, and staff and train accordingly.