INTERIM JOINT COMMITTEE ON NATURAL RESOURCES AND ENERGY

Minutes of the 1st Meeting of the 2021 Interim

June 3, 2021

Call to Order and Roll Call

The 1st meeting of the Interim Joint Committee on Natural Resources and Energy was held on Thursday, June 3, 2021, at 1:00 PM, in Room 154 of the Capitol Annex. Senator Brandon Smith, Chair, called the meeting to order, and the secretary called the roll.

Present were:

Members: Senator Brandon Smith, Co-Chair; Representative Jim Gooch Jr., Co-Chair; Senators C.B. Embry Jr., Denise Harper Angel, Adrienne Southworth, Johnnie Turner, Robin L. Webb, Whitney Westerfield, and Phillip Wheeler; Representatives John Blanton, Adam Bowling, Randy Bridges, McKenzie Cantrell, Myron Dossett, Ryan Dotson, Jim DuPlessis, Patrick Flannery, Chris Fugate, DJ Johnson, Norma Kirk-McCormick, Mary Lou Marzian, Suzanne Miles, Melinda Gibbons Prunty, Attica Scott, Pamela Stevenson, Bill Wesley, and Richard White.

Guests: Stephen Swick, Vice President and Chief Security Officer, American Electric Power; Keith Butler, Senior Vice President and Chief Security Officer, Duke Energy; David McCleod, Director IT Security and Risk Management, LG&E-KU; Caroline Clark, Director, External Affairs, LG&E-KU; and Linda Bridwell, Executive Director, Kentucky Public Service Commission.

LRC Staff: Stefan Kasacavage, Janine Coy, Tanya Monsanto, and Rachel Hartley.

Cyber Security and Protection of Kentucky's electric utility infrastructure

Stephen Swick stated the Colonial Pipeline ransomware event began appearing in news coverage on May 8, 2021. The ransomware event impacted the information technology (IT) systems and network, but the operation technology (OT) systems that manage the pipeline were not impacted. However, the pipeline was shut down as a precaution. This event dramatizes the importance of securing critical infrastructure from cyber threats.

American Electric Power (AEP) serves approximately 5.4 million customers in 11 states. AEP has the largest transmission network in the country and has a private internal IT network.

On a regular basis, internal penetration testing teams attempt to hack into the system to expose AEP's IT vulnerabilities. AEP also conducts annual external hack attempts by white hat hackers. White hat hackers are IT specialists employed by the company to expose IT vulnerabilities. The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) audits AEP at least once annually. This quasi-governmental organization was created to ensure the reliability of regional transmission networks.

In 2005, AEP established the Cyber Intelligence Response Center, which processes new intelligence, detects security events, and provides feedback to external sources including the Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS).

The changes in work practices at AEP due to COVID-19 have not impacted security. The cyber team is operating 100 percent remotely, and all user activity from the IT personnel's home is routed into AEP through secure communications. COVID-19 has created further opportunities for state-sponsored cyber actors to perform cyber espionage operations.

In response to Senator Smith, Mr. Swick stated AEP utilizes a virtual private network (VPN).

David McCleod stated the Cybersecurity and Infrastructure Security Agency and the FBI issued a joint advisory alert with recommended mitigations relating to DarkSide Ransomware. DarkSide Ransomware is the cybercriminal group situated in Eastern Europe responsible for the Colonial Pipeline hack.

Keith Butler stated "phishing" is currently the biggest risk of cyber ransom attacks. Phishing is when a user sends fraudulent emails to induce disclosure of personal information. Adversaries are breaching the more vulnerable vendor systems and are sending emails, which appear legitimate, to employees of Duke Energy.

Senator Westerfield stated on June 8, 2021, Amazon will be using all of its hardware devices that have Wi-Fi capabilities to expand its network. Amazon is creating a new kind of wireless network called "Sidewalk" that will share your home internet connection with your neighbor's devices. It is a major privacy concern and forces users to opt-out, rather than prompt for your permission first.

Senator Smith stated Kentucky should pass a law similar to the California Consumer Privacy Act passed in 2018. The law gives citizens of California more control over their personal information.

Keith Butler stated Duke Energy will participate in the Grid Security Exercise that is facilitated by NERC. The exercise will test the emergency response and recovery plans in response to simulated cyber and physical security attacks and other contingencies.

Duke Energy limits any type of remote access to its system and prohibits the crossover of networks and credentials between OT and IT systems. Risk-based models are used to determine potential impacts on Duke's system that could cause a disruption in service to critical national defense, public critical infrastructure, governmental essential services, and the general customer base.

In response to Representative Gibbons Prunty, Mr. Butler stated the FBI discourages the payment of any type of ransom. The United States Office of Foreign Assets Control publishes a list of terrorist organizations. It is a felony offense for a company to pay ransom to an organization on the list. Duke Energy will work with the FBI if there is a ransomware attack.

In response to Representative Dotson, Mr. Swick stated AEP has a full forensics team, and the FBI has forensic agents that assist. Mr. McCleod stated utilities can request technical assistance through DHS.

In response to Senator Southworth, Mr. Swick stated communities should leverage local experts to consult with election officials to ensure security. Mr. Butler stated local election boards only need protection during an election period.

In response to Senator Westerfield, Mr. Butler stated internet of things (IoT) devices at Duke Energy have protections. Mr. McCleod stated there is mitigation and control for IoT devices.

Linda Bridwell stated the utilities are obligated under KRS Chapter 278 to provide adequate service and only charge reasonable rates. Cybersecurity impacts both service and rate jurisdiction.

There being no further business, the meeting was adjourned.