22 out of the state’s 118 electric utility companies serve the NewsChannel 7 viewing area: Wisconsin Public Service; Northern States Power - (Xcel Energy); Clark Electric COOP; Marshfield Utilities; Startford Muni Water & Electric Utility; Wisconsin Power & Light (Alliant Energy); Central Wisconsin Electric COOP; Adams-Columbia Electric COOP; Wisc. Rapids Water Works & Lighting Commission; Oakdale Electric COOP; Price Electric COOP; Taylor Electric COOP; Medford Electric Utility; Jump River Electric COOP; Gresham Muni Light & Power Utility; Shawano Muni Utilities; Wisconsin Electric Power Co. (WE Energies); Jackson Electric COOP; Bayfield Electric COOP; New Lisbon Muni. Electric COOP; Elroy Muni. Electric & Water Utility; Wonewoc Electric & Water Utility

Following the Trump administration’s electric grid cyber hacking warning, 7 Investigates requested comments from all utilities. Additionally, 7 Investigates also requested comment from Midcontinent Independent System Operator, MISO, who manages Wisconsin’s electric grid and NextEra Energy, who operating company for Wisconsin’s nuclear power plant. The following responses were received:

**WEC Energy Group (Wisconsin Public Serive & We Energies)**

Cybersecurity is a critical focus for WPS and its parent company, WEC Energy Group. We have dedicated an array of tools and personnel to cybersecurity, and we incorporate the latest technologies to maximize the safety of our systems. These tools include advanced persistent threat detection, restricted delivery of critical information outside our corporate network, and rigorous monitoring to alert us to threats across our IT systems. We also isolate our critical infrastructure control systems from the internet and our corporate computing network, and restrict the connection of devices to those control networks.

Additionally, we work closely with other members of the energy industry, as well as senior officials from federal and law enforcement agencies, to best understand potential cybersecurity threats. We also partner with these groups to focus on preparing for, preventing, responding to and recovering from potential cyber and physical threats. The agencies we partner with include our trade associations (Edison Electric Institute and the American Gas Association), Department of Homeland Security and Electricity Information Sharing and Analysis Center.

Aside from prevention, we regularly participate in training exercises designed to simulate our response to physical and cyberattacks on the electric grid. In addition to holding internal training, we have participated in several exercises administered by the North American Electric Reliability Corporation designed to test our response and recovery from an attack on our facilities.

**Xcel Energy**

Ensuring our energy grid is secure from cyber and physical threats is a top priority for Xcel Energy and our partners across the electric industry. Maintaining cyber and physical security is a complex, ever-evolving responsibility that demands constant vigilance and partnerships. We will continue to work collaboratively with our industry and government partners on an array of efforts to enhance security and resilience.

**Alliant Energy**

We regularly plan for emergency situations (both physical and cyber) that could impact our ability to operate and protect customer information. In managing cybersecurity risks, we continuously monitor and use prevention when we can; when specific events occur, we use a planned and practiced approach to respond.

The Russian hacking warning from the federal government is an example of a specific event where our standard practice is to put a plan in place, which we’ve done.

Whenever these types of situations occur, we immediately:

* alert our response teams from our IT and other departments within the company
* begin more aggressive monitoring efforts to identify any potential threat
* begin preparing in the event a threat does occur
* share information and closely coordinate with government and industry stakeholders so threats are identified and preventative measures can be taken. This collaboration is critical.

We have not encountered any issues with our network or other systems at this time, but we continue to monitor them for any threat or unusual occurrence.

Cybersecurity is a top priority for our company. We work together with other utilities and with our government partners on preparation, prevention and detection, information sharing, and response and recovery of the grid and its systems. Business continuity planning is a critical component of our utility operations. We are regularly working to make our computer systems and the electric grid stronger, more reliable, and more resilient in the face of a threat.

**Adams-Columbia Electric Cooperative (ACEC)**

Adams-Columbia Electric Cooperative (ACEC) monitors all segments of our cyber systems and are continually improving our processes to protect our infrastructure and member information. In the event of an attack, we will use a planned approach to respond to the threat and contact the proper authorities. Being that ACEC is a Distribution Cooperative, we also work in conjunction with our affiliated providers, Alliant Energy and American Transmission Company (ATC).

**Marshfield Utilities**

Marshfield Utilities' mission focuses on providing reliable electric service to our customers. We plan, educate, guard and react to situations on a regular basis including regular Incident Response drills.

**Taylor Electric Cooperative**

As a small rural electric distribution service provider, we have no remotely-operated line equipment that is tied to Internet access. One of the only functions that could potentially be disrupted is through a server that collects meter readings (over the powerlines) from all of our meters, the cash registers of our business, so to speak.

Our Application Service Provider (ASP) remotely hosts the servers that provide the business software needs. They also provide all the security and protection protocols needed with firewalls, etc. for those systems. Access to customer information is protected by the ASP provider.

The main grid security concerns would be through the generation, transmission, and substation control systems, which are provided to us by our wholesale power provider, Dairyland Power Cooperative, La Crosse, Wisconsin. Dairyland has very comprehensive physical controls, as well as layers of strong electronic/cyber security protections, including 24-hour systems monitoring.

**MISO (manages Wisconsin’s electric grid)**

As recent global events demonstrate, the energy industry is among many sectors combatting the increase and rapid evolution in cyber attacks.

As part of our mission and commitment to grid reliability, MISO partners closely with industry leadership to stay on the forefront of cyber security and protective technology. We benefit from knowledge sharing among governmental, regulatory and academic partnerships to stay ahead of continuously advancing threats.

Implementing robust cyber security measures that aim to shield the grid and protect reliability is a top priority.

**NextEra Energy (operates Wisconsin’s nuclear power plant)**

NextEra Energy’s number one priority is the safe and efficient operation of our facilities, and that includes robust defenses from a variety of potential attacks and threats. Nuclear power plants are among the best-protected private sector facilities in the nation, and all nuclear plants have extensive cybersecurity features, multiple back-up safety systems, and highly trained operators and security forces.

While we would never discuss specific steps that we have taken to guard against cyberattacks, it’s important for the public to know that the computer systems that help operate nuclear reactors and their safety equipment are isolated from the internet to protect against outside intrusion.

We have comprehensive guidelines for protecting against cyberattacks, which are reviewed by the independent Nuclear Regulatory Commission.