Legislative Council Staff
Nonpartisan Services for Colorado's Legislature

IssueBrief

Number 20-04

February 2020

Energy Infrastructure Security

By Andrea Denka

Cyberattacks on critical infrastructure like the electrical grid are increasing as advanced technology becomes more integrated into how energy systems operate. This *issue brief* provides an overview of critical infrastructure, discusses a 2019 cyberattack on the U.S. electrical grid, and summarizes state and federal legislation addressing security for critical infrastructure.

Critical Infrastructure

The U.S. Department of Homeland Security (DHS) defines critical infrastructure as the assets, systems, and networks essential for the functioning of American society and its economy. In 2013, DHS developed the National Infrastructure Protection Plan to assess the vulnerabilities of 16 identified critical infrastructure sectors in the United States, which include, but are not limited to:

- the emergency services sector;
- the energy sector;
- the food and agriculture sector;
- the health care sector; and
- the transportation systems sector.[1]

DHS developed this plan to inform these sectors of risk management activities that can mitigate future unplanned impacts. The plan also discusses the types of threats that such sectors can face, such as extreme weather, acts of terrorism, technical failures, and cyberattacks.

The electrical grid. The DHS defines the energy sector as the critical infrastructure sector essential for the production, refining, storage, and distribution of oil, gas, and electric power across the country. DHS also states that the energy sector is considered the most important critical infrastructure system due to its integration with almost all other sectors.[2]

Electric power is produced and distributed on a variety of infrastructure across the country, such as transmission lines and power plants, commonly referred to as the electrical grid. The grid is regulated by the U.S. Department of Energy (DOE), and DOE states that about 70 percent of this infrastructure is over 30 years old.[3]

According to the National Conference of State Legislatures (NCSL), grid modernization efforts are beginning to incorporate advanced technologies into grid management systems to improve the electrical grid's operations without replacing costly, aging equipment. New technologies such as smart meters, for example, allow an electric utility to monitor and control systems remotely. These devices, however, may also make the grid more vulnerable to cyberattacks without proper precautions.

[1]"Partnering for Critical Infrastructure Security and Resilience", Department of Homeland Security, https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf

[2]"Presidential Policy Directive 21 Implementation: An Interagency Security Committee White Paper", Interagency Security Committee, https://www.dhs.gov/sites/default/files/publications/ISC-PPD-21-Implementation-White-Paper-2015-508.pdf

[3]"Infographic: Understanding the Grid", Department of Energy https://www.energy.gov/articles/infographic-understanding-grid

2019 Cyber Attack

On September 4, 2019, the North American Electric Reliability Corporation (NERC), an international nonprofit regulatory authority, revealed that on March, 5, 2019, remote online hackers caused a U.S. utility with operations in multiple states to lose visibility of certain wind and solar energy systems for ten hours.[4] According to NERC, the utility's firewall had not been updated, allowing the attackers to gain access into the utility's entire electrical grid control system. Although this incident did not result in lasting impacts on the utility's infrastructure, it highlighted the vulnerability of an electrical grid increasingly dependent on advanced technology. In order to prevent similar cyber incidents in the future, states and the federal government have begun proposing legislation to secure critical infrastructure, including the electrical grid.

Recent Legislation

According to NCSL, numerous states and the federal government have considered legislation to mitigate cyberattacks. Examples of recently enacted and pending legislation are listed below.

Colorado. Senate Bill 17-040 which was enacted, exempts certain information about critical infrastructure in the state from the Colorado Open Records Act (CORA) to increase infrastructure security.

Arkansas. Senate Bill 19-632, which was enacted, required the Arkansas Economic Development Commission to create a cyber-initiative to mitigate cyber risks on critical infrastructure and to encourage the development of cybersecurity technology in the state.

California. Assembly Bill 18-2813, which was enacted, established the California Cybersecurity Integration Center to monitor and mitigate cyber incidents on critical infrastructure in the state. This center is tasked with coordinating and monitoring the state's cybersecurity efforts and implementing a statewide cybersecurity strategy to help identify cyber threats and strengthen emergency preparedness.

Texas. Senate Bill 19-475, which was enacted, created an Electrical Grid Security Council to mitigate the risk of both cyber and physical attacks on the state's electrical grid system. This council is tasked with developing electrical grid security best practices and preparing for events that may threaten the state's grid security.

Senate Bill 19-936, which was enacted, requires the state utility commission to contract with an outside entity to act as the commission's cybersecurity monitor. This entity must manage a comprehensive cybersecurity outreach program for all utilities in the state and must regularly meet with utilities to discuss emerging cyber threats, best practices, and training opportunities.

Cybersecurity and Infrastructure Agency Act of 2018. The federal act, which was enacted, designates DHS's National Protection and Programs Directorate as the Cybersecurity and Infrastructure Security Agency. The act requires this new agency to lead cybersecurity and critical infrastructure security programs and operations across the United States.

Securing Energy Infrastructure Act. The federal act, which is pending, would establish a pilot program to identify security vulnerabilities of certain entities in the energy sector. The act would create a two-year pilot program within the National Laboratories System to develop a strategy to secure the most vulnerable critical infrastructure in the country.

[4]"Lesson Learned: Risks Posed by Firewall Firmware Vulnerabilities", North American Electric Reliability Corporation, https://www.nerc.com/pa/rrm/ea/Lessons%20Learned%20Document%20Library/20190901_Risks_Posed_by_Firewall_Firmware_Vulnerabilities.pdf