HOUSE
RESEARCH
ORGANIZATION

Interim News Briefs

February 2019, Number 86-1

General Government

States address grid security through open government laws

February 27 — Many state legislatures and the U.S. Congress in recent years have amended open government laws in an effort to protect critical energy infrastructure from cybersecurity threats and man-made physical threats, such as vandalism, theft, or attack. Open government or "sunshine" laws include open meetings laws, which allow public access to meetings of governmental bodies, and open records laws, which ensure public access to records maintained by governmental bodies.

Following the 9/11 attacks, Congress in 2002 passed the Critical Infrastructure Information Act as part of the larger Homeland Security Act. The act regulates the use and disclosure of information submitted by public or private organizations to the Department of Homeland Security about vulnerabilities and threats to critical infrastructure (6 U.S.C. secs. 671-673). Critical infrastructure includes physical or virtual systems that are vital to national security, economic security, public health, or safety.

Following the federal example, some state legislatures reassessed the information that could be released through state open records laws, especially critical energy infrastructure information, which includes specific engineering, vulnerability, or location information about infrastructure used to generate or distribute energy that could be useful to a person planning an attack.

More than half of U.S. states currently restrict sensitive information about critical infrastructure from release under open government laws. In addition, the Federal Energy Regulatory Commission (FERC) finalized a rule in 2016 that prohibits the unauthorized disclosure of critical electric infrastructure information under the federal Freedom of Information Act. Several states amended their open records laws in 2017 to include language similar to the FERC rule.

Texas law currently exempts certain meetings about critical infrastructure from state Open Meetings Act requirements. Under Government Code sec. 551.089, a governmental body is not required to conduct an open meeting to deliberate certain network security information, security assessments or deployments involving information resources technology, or the deployment of security personnel, critical infrastructure, or security devices. Information on critical infrastructure is not specifically exempted from disclosure under the Texas Public Information Act.

In 2015 and 2017, the Texas Legislature considered but did not enact bills that would have created committees and task forces to study electric grid security and would have made the meetings, work, and findings of these bodies confidential and not subject to state open government laws. Another bill would have allowed the Texas Public Utility Commission to conduct a closed meeting to discuss issues related to the security of the electric grid and associated computer systems and networks.

Supporters of proposals to keep information on securing critical energy infrastructure confidential said laws are needed to ensure that such information is protected from unwanted disclosure. Others expressed concern that these proposals would make it difficult for the public, electric customers, and the electric industry to be aware of the activities and findings of the study committees. Lawmakers in the 86th regular session this year may continue to discuss the balance between open governance and the security of critical energy infrastructure as concerns about cybersecurity threats grow.

— *MacKenzie Nunez*