115TH CONGRESS
1st Session

SENATE

REPORT
115–12

ACTIVITIES OF THE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

R E P O R T

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

AND ITS

SUBCOMMITTEES

FOR THE

ONE HUNDRED FOURTEENTH CONGRESS

MARCH 28, 2017—Ordered to be printed

U.S. GOVERNMENT PUBLISHING OFFICE
69–010 WASHINGTON : 2017

porated into a larger cybersecurity information sharing bill the Chairman and Ranking Member negotiated with the Senate Select Committee on Intelligence called the Cybersecurity Information Sharing Act of 2015. The final legislation, including the Committee-approved measure, was signed into law in December 2015 as part of the 2016 Consolidated Appropriations Act, P.L. 114–113. This legislation, which includes liability protection when sharing information on cyber threat indicators, is an important first step toward combatting our cyber adversaries.

In addition to the major cybersecurity legislation passed in 2015, the Committee worked to approve several smaller bills to improve our partnership with Israel as it pertains to research on cybersecurity issues, P.L. 114–304, and reduce duplication of DHS spending on information technology, P.L. 114–43. The Committee also approved the Federal Information Systems Safeguards Act of 2016, important legislation that would give Federal agencies broader authority to implement policies to improve cybersecurity, including by restricting employees' access to certain websites.

The issue of encryption was also an important topic in the 114th Congress. The Committee gathered facts from all sides of the debate, hearing from experts at the Federal Bureau of Investigation (FBI) and private technology companies at a series of roundtables to inform policy decisions on this complex issue.

C. CRITICAL INFRASTRUCTURE

The United States depends on its critical infrastructure, particularly the electric power grid, as all critical infrastructure sectors are to some degree dependent on electricity to operate.[16] A successful nuclear electromagnetic pulse (EMP) attack against the United States could cause the death of approximately 90 percent of the American population.[17] Similarly, a geomagnetic disturbance (GMD) could have equally devastating effects on the power grid.[18] Chairman Johnson has made it a priority to examine the threats, both man-made and natural, to the country's critical infrastructure.

In July 2015, the Committee held a hearing titled *Protecting the Electric Grid from the Potential Threats of Solar Storms and Electromagnetic Pulse*, to learn from industry experts about EMP and GMD threats. The hearing examined what actions DHS and the Department of Energy are taking to address these threats and mitigate potential vulnerabilities. The Committee later held a hearing in May 2016 titled *Assessing the Security of Critical Infrastructure: Threats, Vulnerabilities, and Solutions*, to evaluate the state of information-sharing mechanisms used by DHS and private stakeholders to plan for threats against critical infrastructure.

Based on the information learned from the Committee's oversight, Chairman Johnson introduced, and the Committee approved, the Critical Infrastructure Protection Act of 2016. The legislation requires DHS to develop and submit to Congress a strategy to pro-

---

[16] U.S. Dep't of Energy, Office of Electricity Delivery & Energy Reliability, *Cybersecurity*, http://energy.gov/oe/services/cybersecurity (last visited Sept. 21, 2016).

[17] Critical National Infrastructures, Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack (Apr. 2008), http://www.empcommission.org/docs/A2473-EMP—Commission-7MB.pdf.

[18] Gov't Accountability Office, GAO–16–243, Critical Infrastructure Protection: Federal Agencies Have Taken Actions to Address Electromagnetic Risks, But Opportunities Exist to Further Assess Risks and Strengthen Collaboration (2016), http://www.gao.gov/assets/680/676030.pdf.