Protect Our Energy Infrastructure from Physical Disruptions and Cyber Attacks

ENERGY Works For US

A reliable grid is essential to U.S. energy security. New threats have emerged to our energy infrastructure in the form of cyber attacks and the potential for geomagnetic storms. Computer networks that control infrastructure are repeatedly attacked. To combat these challenges, information exchanges between government intelligence agencies and the private sector should be enhanced.

Cyber Incidents by Sector: Fiscal Year 2012

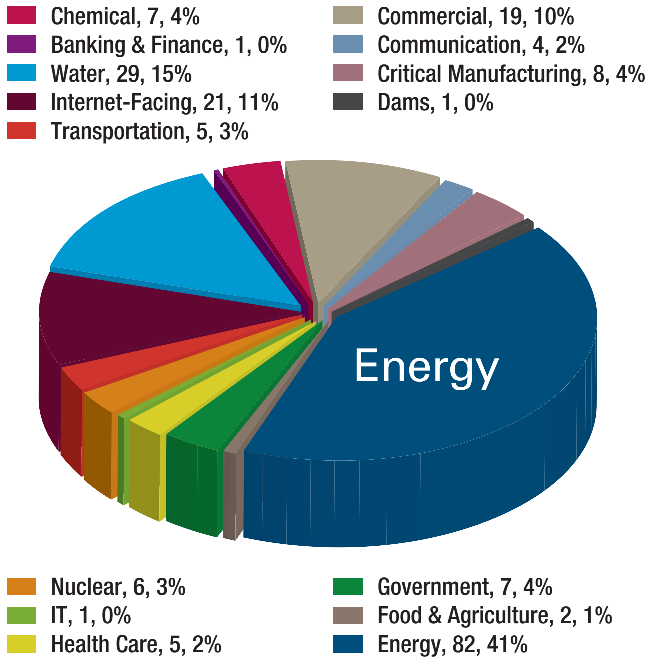

Image source: DHS Industrial Control Systems Cyber Emergency Response Team, ICS-CERT Monitor

Policy Recommendations

- ☑ Congress should enact legislation supporting the exchange of threat information between the government intelligence community and the private-sector owners and operators of critical energy infrastructure. Such legislation should include full liability protections and codify narrowly tailored measures to help business owners and operators harden critical infrastructure and adopt cutting-edge cybersecurity practices that serve to strengthen industry-specific efforts.
- ☑ Congress should direct DHS, in cooperation with DOE, to study the potential impacts of geomagnetic and electromagnetic disturbances on energy infrastructure and implement reasonable risk-based plans to insulate critical facilities from such threats in a cost-effective manner.

Securing the U.S. Energy Grid

DHS recently reported that in fiscal years 2011 and 2012, cyber attacks targeting energy and pipeline infrastructure were increasing around the world. According to the agency, cyber intrusions into pipeline and electric power infrastructure have been occurring at an "alarming rate," with attacks against energy-related systems comprising more than 40% of all reported incidents in fiscal year 2012.

The energy sector is one of the key infrastructure sectors identified in the National Infrastructure Protection Plan, now overseen by DHS. Through this framework, sector-specific plans are developed and implemented, providing cyber and physical infrastructure and supply-chain protections that are crafted to match sector-specific characteristics and conditions.

On February 12, 2013, the White House issued an executive order directed at improving critical infrastructure cybersecurity.

The executive order rightly elevates the importance of bidirectional information sharing, and it also calls on government officials to produce timely classified and unclassified reports on cyber threats for specific targets, such as U.S. critical infrastructure.

Legislation should codify and build upon these advances by providing legal certainty that businesses which voluntarily share threat information with the government will be provided safe harbor against the risk of frivolous lawsuits, will be exempt from public disclosure, and that cyber threat information will not be subject to use by government officials to regulate other activities.

With respect to the protection of critical energy infrastructure from threats such as geomagnetic and electromagnetic disturbances, an established public-private partnership with active and largely uninhibited information-sharing can also pay dividends. And in the case of an electromagnetic attack, the Department of Defense plays a primary role in prevention.

Want to know more about cyber security? Read the full report, *Energy Works for US.*

ENERGY Works For US

www.energyxxi.org/energyworksforus

Data referenced from the following sources: Department of Homeland Security; Department of Energy

MORE THAN

80%

OF THE NATION'S ENERGY INFRASTRUCTURE IS OWNED AND OPERATED BY THE PRIVATE SECTOR.

ATTACKS AGAINST ENERGY-RELATED SYSTEMS COMPRISED MORE THAN

40%

OF REPORTED INCIDENTS IN FY 2012.

From October 2009 to March 2012, the Department of Energy recorded

2,300

INCIDENTS

OF "UNAUTHORIZED COMPUTER ACCESS, IMPROPER USE OF COMPUTING RESOURCES AND THE INSTALLATION OF MALICIOUS SOFTWARE."