



OLR RESEARCH REPORT

September 7, 2012

2012-R-0395

CYBERSECURITY

By: Lee R. Hansen, Legislative Analyst II

You asked for background information on the federal cybersecurity bill recently considered in Congress and similar state-level measures.

SUMMARY

“Cybersecurity” generally refers to the measures taken to protect the network of interdependent information technology infrastructures, telecommunications networks, and computer processing systems that make up “cyberspace.” While public awareness of large-scale cyber-threats has increased in the wake of the 2010 [Stuxnet attack](#) on Iran’s uranium centrifuges, to date there are no national or state-wide cybersecurity standards imposed on the private sector industries that own and operate most of the nation’s energy and utility infrastructure. Instead, these companies rely on voluntary adherence to industry-wide best practices that involve measures that are highly confidential for proprietary commercial reasons and to help prevent against potential threats.

If passed, the federal Cybersecurity Act of 2012 (S. 3414) would require the development of national cybersecurity standards and allow private entities to more easily share information on cyber-threats. Compliance with the standards would not be mandatory under the bill, although companies that did comply would receive certain protections from legal liability. In August 2012, the bill failed to garner the 60 votes necessary to overcome a filibuster in the Senate.

Although some states have begun to address cybersecurity measures for their own governmental computer networks, no state has implemented cybersecurity standards that would apply to their privately owned utility infrastructure. In Connecticut, the Public Utilities Regulatory Authority (PURA) is currently investigating the cybersecurity measures of the utility companies it regulates. It hopes to conclude its investigation and issue a report on its findings some time during the first half of 2013.

THE CYBERSECURITY ACT OF 2012

According to the [Congressional Research Service](#), the Cybersecurity Act of 2012 directs the Secretary of Homeland Security, in consultation with critical infrastructure owners and operators, the Critical Infrastructure Partnership Advisory Council, and other federal and private-sector entities, to:

1. conduct a top-level assessment of cybersecurity risks to determine which sectors face the greatest immediate risk;
2. establish a procedure designating critical infrastructure;
3. identify or develop risk-based cybersecurity performance requirements; and
4. implement cyber response and restoration plans.

The bill defines “critical infrastructure” as the physical or virtual systems and assets whose destruction would have a debilitating impact on the nation’s security, economic security, or public health and safety. The definition would include utility companies such as electric, gas, and water companies.

In addition to establishing security standards and plans, the bill establishes a process to designate cybersecurity exchanges for distributing, receiving, and exchanging threat information. It authorizes private entities to disclose or receive lawfully obtained cybersecurity threat information on the exchanges.

Although the bill does not require critical infrastructure owners and operators to comply with the cybersecurity performance requirements or cybersecurity exchanges, it encourages them to comply by providing legal protections, including a good faith defense from civil actions, for companies that do comply. In particular, it bars civil or criminal causes

of action based on the (1) cybersecurity monitoring activities it authorizes or (2) voluntary disclosure of a lawfully obtained cybersecurity threat indicator to a (a) cybersecurity exchange, (b) provider of cybersecurity services, or (c) private or government entity that provides or manages critical infrastructure.

For federal agencies, the bill creates a National Center for Cybersecurity and Communications to secure, protect, and ensure the resiliency of the federal information technology infrastructure. The center must also support private sector efforts to protect their infrastructure. The bill also revises information security requirements for federal agencies and provides for their continuous monitoring of cybersecurity risks.

Among other things, the bill also requires:

1. the Department of Homeland Security (DHS) to implement cybersecurity outreach and awareness programs,
2. DHS and the Commerce Department to establish a program to recruit and train cybersecurity professionals,
3. the National Science Foundation to establish a program to stimulate innovation in cybersecurity research and development,
4. the Office of Personnel Management to assess the federal workforce cybersecurity capacity and establish education curriculum for all federal employees and contractors, and
5. the Department of Education to develop model curriculum standards to address cybersecurity issues.

The bill's opponents argued that it would impose an unnecessary burden on private sector industries by requiring them to focus on meeting government standards instead of keeping up with the latest threats. Other opponents argued that it threatened personal privacy by allowing private entities to monitor their information systems for any cybersecurity threats, regardless of federal wiretapping and surveillance laws, and share any threat indicators with other private entities. On August 2, 2012, the bill failed to secure the 60 votes needed to bring it up for a vote in the Senate.

STATE-LEVEL MEASURES

If enacted, the Cybersecurity Act would supersede any conflicting state laws regulating cybersecurity services or the acquisition, interception, retention, use or disclosure of communications, records, or other information by private entities for the cybersecurity-related purposes detailed in the bill. However, to date, no state has imposed state-wide cybersecurity standards on its utility companies.

State legislative efforts to address cybersecurity issues have mainly focused on securing public-sector computer networks while offering voluntary assistance to the private-sector. Some states have created special offices to address the cyber security issues facing state governmental entities. In 2010, New York created an [Office of Cyber Security](#) within its Division of Homeland Security and Emergency Services. The office is responsible for developing and overseeing cybersecurity standards for state agencies, programs, and services. It collects information on cybersecurity breaches and issues threat advisories to state agencies and state government entities. For the private sector, it also conducts cybersecurity awareness training programs and links to other resources.

Similarly, New Hampshire is currently considering a bill ([H.B. 1593](#)) that would require the state's Department of Information Technology to develop and implement a strategy to address cyber security risks to the state's data, information, and technology resources.

PURA Docket 10-11-08

In Connecticut, PURA initiated docket 10-11-08, "Determination of a Public Service Company-Specific Cyber Security Policy," late in 2010. The docket proposes to review and develop an understanding of the utility companies' cyber security policies and practices and to establish an ongoing dialog between PURA and the companies concerning their cybersecurity procedures. The investigation is ongoing, although PURA hopes to issue a report on its findings sometime during the first half of 2013.

In its investigation, PURA issued interrogatories to the various utility companies under its jurisdiction seeking information on their:

1. cybersecurity policies,
2. experience with cyber attacks,
3. knowledge of and adherence to industry standards,

4. system vulnerability,
5. participation in federal cybersecurity programs,
6. opinions on the pro and cons of state oversight, and
7. various technical aspects of their computer networks.

According to PURA, the companies have been generally cooperative, although the highly confidential nature of the information requested has caused significant delays. Because PURA proceedings and the documents filed with them are typically considered public records subject to the state's Freedom of Information Act (FOIA), PURA has been conducting in-person interviews with the companies to preserve the confidentiality of the proprietary and security-related information being discussed.

When its investigation is complete, PURA's report should address the need, if any, for (1) state-wide oversight and standards; (2) a means for utilities to share information and situational awareness on cyber threats, vulnerabilities, and best practices; and (3) federal or state legal issues, particularly regarding confidentiality, that must be addressed to improve cybersecurity practices.

LH:ts