SEC

SECURITY EXECUTIVE COUNCIL

A research and advisory firm

Compliance Scorecard: Legislation on Critical Infrastructure Cybersecurity

Security Executive Council

Originally Published in Security InfoWatch

June 2011

Compliance Scorecard: Legislation on Critical Infrastructure Cybersecurity

Presidential Policy Directive 8
http://www.dhs.gov/xabout/laws/gc_1215444247124.shtm
Presidential Policy Directive 8 (PPD-8) directs the development of a national preparedness goal and a national preparedness system. The national preparedness goal will define the core capabilities necessary to prepare for the types of incidents that pose the greatest risk to national security, with a focus on achieving an integrated, layered and all-of-nation preparedness approach. PPD-8 replaces HSPD-8.

White House Cybersecurity Legislative Proposal
http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/law-enforcement-provisions-related-to-computer-security.pdf

The Obama administration's legislative proposal on cybersecurity, released May 12, draws on the Cyberspace Policy Review completed in 2009. The proposal would standardize state laws on data breach reporting; clarify the penalties for computer crimes, setting mandatory minimums for cyber intrusions into critical infrastructure; clarify and authorize quick DHS assistance to private businesses suffering intrusions; protect entities sharing information about cyber threats or incidents with the government; and allow DHS and NIST to oversee and possibly modify cybersecurity protection plans in critical infrastructure, among other actions. One controversial section would give the President emergency powers to shut down the Internet to protect vital networks from attack.

Bingaman-Murkowski Joint Staff Draft Legislation, Senate Committee on Energy & Natural Resources
http://www.gpo.gov/fdsys/pkg/CHRG-112shrg67362/pdf/CHRG-112shrg67362.pdf

In April, the Senate Committee on Energy & Natural Resources released a 12-page discussion draft of proposed legislation to give the Department of Energy and the Federal Energy Regulatory Commission (FERC) limited cybersecurity oversight of state-jurisdictional electric lines. The legislation would direct FERC to determine whether existing reliability standards are adequate to protect critical electric infrastructure from cybersecurity vulnerabilities. If FERC finds that they are not sufficient, it would be given the authority to direct the North American Electric Reliability Corp. (NERC) to propose new or modified standards and set a deadline for NERC to act. Hearings were held May 5.

Chemical Facility Anti-Terrorism Standards
http://www.dhs.gov/files/laws/gc_1166796969417.shtm
Through CFATS, DHS screens facilities to identify those that deal with "chemicals of interest," ranks them into one of four tiers according to the level of risk they present, and then requires them to complete risk assessments that must be approved by DHS. They must then develop security plans that specifically address the vulnerabilities they have identified. These plans must in turn be approved and must then be implemented on an approved schedule. As of this writing, Congress is considering an extension of CFATS to 2017.

The Implementing Recommendations of the 9/11 Commission Act of 2007
https://www.nsa.gov/civil_liberties/_files/pl_110_53_sec_803_9_11_committee_act.pdf

This act implemented the recommendations of the 9/11 Commission. A wide-ranging bill with a variety of impacts, it touches multiple critical infrastructure markets and includes some requirements that are still unmet. One of these is the requirement that the Transportation Security

Administration (TSA) establish procedures to ensure screening of 100 percent of the cargo shipped on passenger aircraft. The deadline for 100-percent inbound cargo screening has now been extended to December 2011.

USA PATRIOT Act

http://thomas.loc.gov/cgi-bin/bdquery/z?d107:H.R.3162:

The USA PATRIOT Act of 2001 enhances powers of both domestic law enforcement and international intelligence agencies to deter and punish terrorism. In May, Congressional leaders reached a deal to extend the Patriot Act another four years with no changes to some controversial sections of the law, which allow investigators to get "roving wiretap" court orders to help them track terrorism suspects who switch phone numbers; and to get orders allowing them to seize "any tangible things" relevant to a security investigation, like the customer records of a business.

About the Security Executive Council

We are a research and advisory firm for security leaders. We have a collective of close to 100 security subject matter experts that have been successful security executives or are recognized industry experts in their field. The resources and tools we develop are constantly evolving to provide maximum value. Some engage with us by way of multi-year "retained" services agreements (Tier 1 Stakeholders). Tier 1 Stakeholders are those that want support on an ongoing basis but also want to have an active role in identifying solutions for the industry. Others come to us seeking a specific solution to a contained issue. In all the ways people engage with the SEC the bottom line goal is to help define and communicate the value of the Security organization.

Contact us at: contact@secleader.com
Learn more about the SEC here: https://www.securityexecutivecouncil.com