Attorneys:

- **Timothy G. Ronan**
  tronan@pullcom.com
  203.674.7933

CYBER LAW TRACKER: June 2010

The Latest in Cybersecurity and Infrastructure Protection Legal Developments

KEY CYBERSECURITY LEGISLATION UNANIMOUSLY APPROVED BY UNITED STATES SENATE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENT AFFAIRS

Posted on June 25, 2010, by T. Scott Cowperthwait

On June 24, 2010, the U. S. Senate Committee on Homeland Security and Governmental Affairs unanimously approved an altered version of the Protecting Cyberspace as a National Asset Act of 2010 (PCNAA), S. 3480, a bill introduced by U.S. Senators Joseph Lieberman (I-Conn.), Susan Collins (R-Me.) and Thomas Carper (D-Del.) which would amend the Homeland Security Act of 2002, 6 U.S.C. 101, et seq. Notably, the PCNAA would establish in the Executive Office of the President an Office of Cyberspace Policy (the "Office"). The Office would be tasked with developing and updating a national strategy to increase the security and resiliency of the cyber and communications infrastructure of the United States. The Office would be led by a presidential-appointee and Senate-confirmed director with specialized ability and knowledge in information technology, cybersecurity, and the operations, security and resiliency of communications networks. The PCNAA would also create a new center within the Department of Homeland Security (DHS), the National Center for Cybersecurity and Communications (NCCC), which would have authority over critical infrastructure owners and operators.

CYBER LAW TRACKER: June 2010

The PCNAA, as introduced in Committee earlier this month, contained controversial language which provided the president with the authority to take undefined emergency actions, including the power to essentially shut down Internet communications with respect to covered (but again undefined) critical infrastructure systems. The Cybersecurity Act of 2009, S. 773, similarly contained unilateral presidential "kill switch" authority; however, that provision created such controversy it had to be modified before S. 773 was approved by the Commerce Committee. In like fashion, the Senate Committee on Homeland Security and Governmental Affairs has amended the president's authority to shut down or limit communications over the Internet involving critical infrastructure systems in the PCNAA by adding language requiring the president to seek congressional approval to extend emergency measures beyond 120 days.

The PCNAA now moves to the Senate floor where it is expected to be taken up in conjunction with the Cybersecurity Act of 2009.

For a copy of the PCNAA as introduced in the Senate, please click here. The amended version of the PCNAA has been ordered and will be reported to the Senate at a future date.

For a copy of the fact sheet prepared by Senators Lieberman and Collins describing the intent and impact of the PCNAA, please click here.

THE HIGH TECHNOLOGY CRIME INVESTIGATION ASSOCIATION PUBLISHES ITS 2010 REPORT ON CYBER CRIME INVESTIGATION

Posted on June 25, 2010, by T. Scott Cowperthwait

On June 22, 2010, the High Technology Crime Investigation Association (HTCIA) published the results of its membership survey addressing a variety of cyber crime issues, including members' levels of experience and training, job functions and the problems members experience in their day-to-day work. The survey's major findings identified the following issues:

(1) an increase in criminal use of digital technology;
(2) a lack of dedicated personnel responsible for cyber crime investigations;
(3) the need for better training among cyber crime professionals concerning digital forensics, online investigations, computer and network security, collection and imaging of digital evidence, and on-site evidence preview or triage;
(4) the need for improvements in information sharing and collaboration between the public and sectors; and

(5) the need for better cyber crime reporting, strategy and policy measures.

As the survey results reveal, now is the time for businesses to take proactive measures to address the cybersecurity challenges facing the economic, physical and human infrastructures within the United States.

The HTCIA is designed to encourage, promote, aid and effect the voluntary interchange of data, information, experience, ideas and knowledge about methods, processes and techniques relating to investigations and security in advanced technologies among its membership. The HTCIA membership is comprised of public and private sector security professionals who are tasked with investigating technology related crimes.

OMB ISSUES A CYBERSECURITY BUDGETING DIRECTIVE

Posted on June 17, 2010, by Timothy G. Ronan

Last week, Peter Orszag, Director of the Office of Management and Budget (OMB), sent a memorandum to the heads of all U.S. departments and agencies with budget guidance for Fiscal Year 2012. This OMB memo includes predictable language about "eliminating low-priority programs" and "squeezing out waste," but it also includes a directive that all submissions with regard to the FY 2012 budget should include, among other things, 1) funding for the timely execution of agency plans to consolidate data centers; 2) an evaluation of IT infrastructure including the potential to adopt cloud computing solutions where they represent the best value and an acceptable level of risk; and 3) funding for the cybersecurity "tools necessary to enable continuous monitoring of agency IT system security."

ELECTRICAL GRID SECURITY BILL APPROVED BY U.S. HOUSE OF REPRESENTATIVES

Posted on June 16, 2010, by T. Scott Cowperthwait

In May 2008, the U.S. General Accounting Office (GAO) released a report examining the information security practices in place at the Tennessee Valley Authority (TVA) designed to protect the control systems and networks used to operate the TVA's critical infrastructures. The GAO report revealed several weaknesses making the TVA's critical infrastructure vulnerable to disruption, including but not limited to 1) security

weaknesses associated with the interconnectedness of its corporate network with its control system networks; 2) the lack of key software patches and inadequate security settings on its corporate network; 3) significant limitations with respect to its intrusion detection system; and 4) insufficient physical security at site locations. In April 2009, U.S. intelligence officials reported that cyber spies from China, Russia and other countries had penetrated the U.S. electrical grid and its control systems.

Spurred by the GAO report and the real threat of a cyber attack capable of sabotaging the U.S. electrical grid, the U.S. House of Representatives passed the Grid Reliability and Infrastructure Defense Act (the GRID Act), H. R. 5026, on June 9, 2010. If enacted, the GRID Act would amend the Federal Power Act, 16 U.S.C. § 824, et seq., and provide the president with sweeping new authorities to authorize the Federal Energy Regulatory Commission (FERC), with or without notice, hearing, or report, to issue immediate emergency measures to protect the reliability of the bulk-power system or defend the electric critical infrastructure whenever the president issues a written directive or determination identifying an imminent threat to the U.S. electrical grid. The GRID Act would also mandate FERC to issue a rule within 180 days of enactment of the Act requiring high-voltage electric transmission companies to address the " Aurora" vulnerability, a critical systems vulnerability to cyber attacks that could cause severe physical damage to electric control systems. The GRID Act also empowers the president with the authority to designate up to 100 electric facilities identified as "defense critical electric infrastructure" that the president deems as vulnerable to a potential disruption of the supply of electric energy in the event of a malicious act using electronic communication or an electromagnetic pulse. Designated facilities would be required to implement measures to protect the critical electric infrastructure against such vulnerability under the supervision of FERC.

Stay tuned for more developments about the GRID Act and its potential impact on power companies in the New England region.

For a copy of the GAO Report to Congressional Requesters entitled "Information Security: TVA Needs to Address Weaknesses in Control Systems and Networks," you should visit the GAO's Web site at http://www.gao.gov/new.items/d08526.pdf. For a copy of the GRID Act as referred to the U.S. Senate, you should visit The Library of Congress' THOMAS Web site at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_bills&docid=f:h5026rfs.txt.pdf.