

The Virtual Lawyer

Briefings on Technology and Business Law

April 2009



The Cybersecurity Act of 2009 Act I: Control of the Internet and Other Networks

Legal Disclaimer

- Law is ever-changing. This briefing is a synopsis only and cannot substitute for personal legal advice. Everyone's facts and circumstances are different and you should not rely on the contents of this publication to make substantive legal decisions. Please contact me for a further consultation.

When the right and the left agree on a particular piece of legislation, it always makes me sit up and take notice.

Both sides are taking a hard look at the **Cybersecurity Act of 2009** sponsored by Jay Rockefeller (D-WV), Bill Nelson (D-FL), and Olympia Snowe (R-ME). While the bill tries to address the important need to protect vital networks from cyber attack, it gives an awful lot of power to the executive branch — perhaps too much power.

The Act would give the president the ability to “declare a cybersecurity emergency” and shut down or limit Internet traffic in any “critical” information network “in the interest of national security.”

Here's the problem: the bill does not define a “critical information network” or a “cybersecurity emergency”. That definition would be left to the president and it would also grant to the Secretary of Commerce “access to all relevant data concerning [critical] networks without regard to any provision of law, regulation, rule, or policy restricting such access.”

This presumably means that the Secretary could monitor or access any data on private or public networks without regard to privacy laws.

Here are the sections raising eyebrows:

SEC. 14. PUBLIC-PRIVATE CLEARINGHOUSE.

(a) DESIGNATION.—The Department of Commerce shall serve as the clearinghouse of cybersecurity threat and vulnerability information to Federal government and private sector owned critical infrastructure information systems and networks.

(b) FUNCTIONS.—The Secretary of Commerce—

(1) shall have access to all relevant data concerning such networks without regard to any provision of law, regulation, rule, or policy restricting such access; ...

SEC. 18. CYBERSECURITY RESPONSIBILITIES AND AUTHORITY.

The President— ...

(2) may declare a cybersecurity emergency and order the limitation or shutdown of Internet traffic to and from any compromised Federal government or a United States critical infrastructure information system or net-

Attorney at Law
David P. Crocker
Solicitor of England and Wales



Business Address
Russell House
158 Pleasant Avenue
Portland, Maine 04103-3204 USA

Phone: 207.879.0708
Fax: 207.221.6417
Email: dpc@davidcrocker.com

Local and International
www.davidcrocker.com

First admitted to practice in 1989, David P. Crocker manages an international law practice in licensing, intellectual property, information technology and business law. He has experience in domestic and international licensing, technology development and general intellectual property law, including copyright, trademark and trade secret protection.

Crocker provides direct and timely assistance not only to technologists, but also to writers, artists, photographers and all creative people who wish to protect and license their work.



Crocker is currently qualified to practice in the United States and England and Wales. He advises United States, United Kingdom and other international clients in intellectual property, technology and business matters.

All Content © 2009 David P. Crocker. All Rights Reserved

The Cybersecurity Act of 2009: Internet Control, continued

work; ...

Section 18 certainly gets my attention. It gives the president power over two ill-defined networks—those belonging to the Federal government and those belonging to the “United States”. The first bit is not threatening and is indeed rather sensible: the Act would give the president the authority to disconnect *federal* networks *from* the Internet in the case of cyberattack.

It’s the second bit that’s more worrisome: a “United States” critical infrastructure information system or network is defined in the Act as:

“State, local, *and nongovernmental* information systems and networks in the United States designated by the President as critical infrastructure information systems and networks.”

The definition is a jaw-dropper: virtually any information system or network, *government or private* would be subject to presidential control in the event of an undefined or ill-defined “cyberemergency”.

And section 18 goes even further: it gives the president the authority to map all “United States critical information systems” - *whether or not there’s an emergency*. If you don’t mind having your systems mapped, then I suppose it’s not a problem.

But section 14 may be a bigger problem. It essentially revokes all privacy safeguards for “threat” and “vulnerability”

information on all *all* networks. And since “threat” and “vulnerability” are undefined, this leaves the Feds with wide discretion to probe and snoop through purely private networks.

Section 14 allows the government to obtain such information without search warrants. The section also doesn’t limit the jurisdiction to acute attacks, either. That jurisdiction exists at *all times*.

In the end, however, the real issue isn’t that this or any other president might shut down the Internet or other networks. Rather, it’s that the Act may well violate the Fourth Amendment’s prohibition on search and seizure, granting a warrantless search power to the Secretary of Commerce and giving vast discretion to executive branch officials to probe and snoop.

I’ve attached to this briefing relevant portions of the draft Act for your review.

In addition, I’ve posted the entire draft act on my web site, which you can obtain here.

Please continue to the next two installments: the second installment discusses federal control over software configuration design; the third deals with licensing of “cybersecurity professionals” (which could be just about anybody who touches a “critical” system).

1 gressional Committees containing the President’s, or the
2 President’s designee’s, findings, conclusions, and rec-
3 ommendations.

4 **SEC. 17. AUTHENTICATION AND CIVIL LIBERTIES REPORT.**

5 Within 1 year after the date of enactment of this Act,
6 the President, or the President’s designee, shall review,
7 and report to Congress, on the feasibility of an identity
8 management and authentication program, with the appro-
9 priate civil liberties and privacy protections, for govern-
10 ment and critical infrastructure information systems and
11 networks.

12 **SEC. 18. CYBERSECURITY RESPONSIBILITIES AND AUTHOR-**
13 **ITY.**

14 The President—

15 (1) within 1 year after the date of enactment
16 of this Act, shall develop and implement a com-
17 prehensive national cybersecurity strategy, which
18 shall include—

19 (A) a long-term vision of the Nation’s cy-
20 bersecurity future; and

21 (B) a plan that encompasses all aspects of
22 national security, including the participation of
23 the private sector, including critical infrastruc-
24 ture operators and managers;

1 (2) may declare a cybersecurity emergency and
2 order the limitation or shutdown of Internet traffic
3 to and from any compromised Federal Government
4 or United States critical infrastructure information
5 system or network;

6 (3) shall designate an agency to be responsible
7 for coordinating the response and restoration of any
8 Federal Government or United States critical infra-
9 structure information system or network affected by
10 a cybersecurity emergency declaration under para-
11 graph (2);

12 (4) shall, through the appropriate department
13 or agency, review equipment that would be needed
14 after a cybersecurity attack and develop a strategy
15 for the acquisition, storage, and periodic replace-
16 ment of such equipment;

17 (5) shall direct the periodic mapping of Federal
18 Government and United States critical infrastruc-
19 ture information systems or networks, and shall de-
20 velop metrics to measure the effectiveness of the
21 mapping process;

22 (6) may order the disconnection of any Federal
23 Government or United States critical infrastructure
24 information systems or networks in the interest of
25 national security;

1 (7) shall, through the Office of Science and
2 Technology Policy, direct an annual review of all
3 Federal cyber technology research and development
4 investments;

5 (8) may delegate original classification author-
6 ity to the appropriate Federal official for the pur-
7 poses of improving the Nation’s cybersecurity posture;
8

9 (9) shall, through the appropriate department
10 or agency, promulgate rules for Federal professional
11 responsibilities regarding cybersecurity, and shall
12 provide to the Congress an annual report on Federal
13 agency compliance with those rules;

14 (10) shall withhold additional compensation, di-
15 rect corrective action for Federal personnel, or ter-
16 minate a Federal contract in violation of Federal
17 rules, and shall report any such action to the Con-
18 gress in an unclassified format within 48 hours after
19 taking any such action; and

20 (11) shall notify the Congress within 48 hours
21 after providing a cyber-related certification of legal-
22 ity to a United States person.

23 **SEC. 19. QUADRENNIAL CYBER REVIEW.**

24 (a) IN GENERAL.—Beginning with 2013 and in every
25 fourth year thereafter, the President, or the President’s