

The Virtual Lawyer

Briefings on Technology and Business Law

April 2009



The Cybersecurity Act of 2009 Act II: Software Design and Configuration

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.

In the first installment, we discussed the grant of power to the executive to shut down and degrade portions of the Internet and other networks and to obtain “vulnerability” information from private networks without a warrant.

In this installment, we'll cover what could be a more important aspect of the bill: the government's ability to regulate software design.

Section 6: The Nub of the Problem

One year after the Act's passage, the National Institute of Standards and Technology must establish “measurable and auditable cybersecurity standards for all Federal Government, government contractor, or grantee critical infrastructure information systems and networks.” This is broken down into an number of subsections that are quite specific by type.

Here are relevant sections of the statute, selected portions of which I've highlighted. Keep in mind these important points: first, these standards apply not only to federal government computers, but to private sector systems and networks deemed by the executive as “critical information infrastructure”; second, the definition of “software” is completely vague in most instances. *As the bill is written, it could cover just about anything.*

(4) SOFTWARE CONFIGURATION SPECIFICATION LANGUAGE.—The Institute **shall establish standard computer-readable language for completely specifying the configuration of software** on computer systems widely used in the Federal Government, by government contractors and grantees, and **in private sector owned critical infrastructure information systems and networks.**

(5) STANDARD SOFTWARE CONFIGURATION.— The Institute **shall establish standard configurations consisting of security settings for operating system software and software utilities** widely used in the Federal Government, by government contractors and grantees, and **in private sector owned critical infrastructure information systems and networks.**

(6) VULNERABILITY SPECIFICATION LANGUAGE.—The Institute **shall establish standard computer-readable language for specifying vulnerabilities in software to enable software vendors to communicate vulnerability data to software users in real time.**

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: Software Design, continued

(7) NATIONAL COMPLIANCE STANDARDS FOR ALL SOFTWARE.—

(A) PROTOCOL.—The Institute **shall establish a standard testing and accreditation protocol for software** built by or for the Federal Government, its contractors, and grantees, **and private sector owned critical infrastructure information systems and networks** to ensure that it—

(i) meets the software security standards of paragraph (2); and

(ii) does not require or cause any changes to be made in the standard configurations described in paragraph (4).

(B) COMPLIANCE.—The Institute **shall develop a process or procedure to verify that—**

(i) **software development organizations comply with the protocol established under subparagraph (A) during the software development process;** and

(ii) testing results showing evidence of adequate testing and defect reduction are provided to the Federal Government prior to deployment of software.

Analysis

Under the Act, the NIST will jump straight into the software design business.

First, NIST is going to writing a new language that will completely specify the configuration on “software” - all software that might be used on a Federal system or private sector “critical” systems. You’re reading this correctly: the Feds get to set the configuration and the language doesn’t distinguish between network, platform, operating system, applications or anything in between. It’s “configuration”, period.

Second, NIST will establish standard security config settings for the OS and “utilities” widely used in both Federal systems and—there it is again—private sector systems deemed “critical infrastructure”. Since there are only a handful of operating systems out there, practically speaking, this means that the government is going to be setting operating system configuration standard.

Third, NIST will be the goalkeeper, determining whose “software” passes muster. They get to write the protocol.

Fourth, NIST is the enforcer. They get to establish a compliance regime to make sure that “software development organizations” do what they’re told.

Conclusion, if you don’t want the federal government as a partner in your development organization, you should be calling your congressperson right about now.

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