

U.S. Information Security Law, Part Four

Steven Robinson 2003-07-09

This is the last article in a [four-part series](#) looking at U.S. information security laws and the way those laws affect the work of security professionals. This installment continues the discussion of information security in the public sector and provides an overview of national security law in the United States as it pertains to information security.

National Security and Critical Information Infrastructure

It is easy to think of "national security" as meaning the security provided by military and intelligence gathering capabilities, and in certain specific legal contexts, that specific definition is both accurate and complete [1]. But as the threat of terrorism became clear, even before the attacks of September 11, 2001 national security came to mean, in addition to national defense, the protection of the public and private sector facilities essential to delivering the goods and services that maintain the quality of life in the United States, or as officially defined, the nation's "critical infrastructure." [2] Executive Order No. 13231 [3], entitled, Critical Infrastructure Protection in the Information Age, issued by the President five weeks after the September 11, 2001 attacks, addressed itself to the information technology systems that form part of the nations' critical infrastructure. The Executive Order noted that information technology had "changed the way business is transacted, government operates, and national defense is conducted. Those three functions now depend on an interdependent network of critical information infrastructures." The order went on to authorize "continuous efforts to secure information systems for critical infrastructure." As we begin the discussion of the law in this area, it is useful to understand that the information technology we are talking about operates in three general arenas: (1) the business environment, (2) the environment for the delivery of government services, and (3) national defense.

Understanding the many complexities involved in making law to protect critical information technology infrastructure begins with the observation widely recognized by information security professionals that information technology itself, its legitimate uses, the threats to those uses, and the response to those threats all evolve continuously. Information technology infrastructure is critical support for the operation of "the telecommunications, energy, financial services, manufacturing, water, transportation, health care, and emergency services sectors" of the United States economy [4]. This list covers a tremendous amount of ground, in both business and legal terms.

The law as it applies to these areas involves statutes enacted by the Congress and state legislatures, and regulations promulgated by federal and state government agencies, many of which were put in place to address specific issues characteristic of each regulated area. In short, many parties have jurisdiction to make law concerning some part of the nation's critical information technology infrastructure.

In addition, because the protection of critical information technology infrastructure is a new and evolving priority, lawmakers and regulators have the smallest body of analogous pre-information age law to use as a starting point in their attempts to provide that protection. Addressing this task on behalf of a population that is understandably jittery and is likely to remain so for the foreseeable future, in tough budgetary times, is all the more difficult. In short, of all the information security contexts discussed in this series, making law to protect the nation's critical information technology infrastructure is an area in which lawmakers and regulators are regularly forced to try to hit a moving target. Nevertheless, it was clear long before September 11, 2001 that such protection was required. The terrorist attacks indicated that the need was more urgent than some had previously appreciated.

The government entities concerned have not been idle. By one estimate, at the federal level alone there are sixteen statutes, six executive orders, and more than fifty other statements of policy that address information security concerns related to national security and that are generally applicable to information systems run by agencies of the federal government and their contractors. In specific areas, there are additional requirements imposed by government agencies with pertinent regulatory responsibilities. The legal landscape also includes applicable state and local law. Obviously, a comprehensive review of this body of law is beyond the scope of this article. The discussion below addresses the major themes and developments of the law at the federal level, where primary jurisdiction for national security matters resides.

The Computer Security Act

Before September 11, 2001, the law of information security at the level of national security had primarily concerned the development of appropriate security standards, and it is easy to see why. Given the enormous range of the critical information technology infrastructure and the substantial number of federal agencies that address various aspects of the nation's critical infrastructure, it was not inherently clear who had the authority to establish standards, how standards should be initiated, and once in place, how the implementation of standards should

be coordinated between agencies. The Computer Security Act of 1987 [5] (the "Computer Security Act") was the initial Congressional attempt to address these questions.

The Computer Security Act stated that the National Bureau of Standards, an agency of the Department of Commerce now renamed as the National Institute of Standards and Technology ("NIST"), was to "have responsibility within the Federal Government for developing technical, management, physical and administrative standards and guidelines for the cost-effective security and privacy of sensitive information in Federal computer systems," as part of its overall mission of "developing uniform standards for Federal computer systems." [6] NIST received no authority with respect to the information security for military and intelligence gathering systems, which remained with the Department of Defense and the National Security Agency. Notably, the Computer Security Act defined the term "Federal computer system" to mean both systems operated by an agency of the federal government and by contractors of federal agencies. [7]

The Computer Security Act contemplated that NIST would develop these standards in coordination with other federal agencies to maximize the use of security and privacy-related resources, reduce duplication and waste, and ensure that all standards and guidelines were consistent with the secrecy requirements of national defense and foreign policy. With respect to determining the vulnerabilities of Federal computer systems and for developing techniques for the cost effective security and privacy of sensitive information those systems contained, NIST was specifically instructed to call on technical guidelines developed by the National Security Agency, to the extent that NIST found those guidelines applicable to the protection of Federal computer systems.

The Computer Security Act envisioned that the Secretary of Commerce would use the standards and guidelines so developed to promulgate binding standards and guidelines as "necessary to improve the ? security and privacy of Federal computer systems." The authority to institute binding standards is subject to Presidential modification or disapproval. These standards were considered to be a required minimum, and heads of federal agencies were specifically authorized to adopt more stringent security measures, as long as they also implemented the measures the Secretary of Commerce deemed mandatory. The Computer Security Act also requires every federal agency to identify the Federal Computer systems under its supervision that contain sensitive information and to establish plans for their security and privacy that are "commensurate with the risk and magnitude or the harm resulting from the loss, misuse, or unauthorized access to or modification of that information." [8] The Computer Security Act

called for agency security plans are to be revised annually.

The Computer Security Act also established the Computer System Security and Privacy Board to identify issues related to information security, advise NIST and the Secretary of Commerce with respect to such issues, and to report its findings not only within the Department of Commerce, but also to the Director of the National Security Agency and Congress. [9]

All in all, the Computer Security Act put a framework in place that sought to combine the expertise of NIST in setting national standards with coordinated interagency communications to develop and implement information security standards for federal computer systems that reflected government-wide variations in computing environments, the sensitivity of the information to be protected, and the potential harm in the national interest in the event of security breaches as to that information.

Substantive Federal Protections for Information Infrastructure

National security in the information age also requires that criminal liability and appropriately severe sentences be imposed for individual wrongdoing concerning unauthorized access to, misuse, alteration or transmission of data stored by or in the national's critical information infrastructure. [10] This process was begun, in substantial part, by the enactment of the Computer Fraud and Abuse Act (the "CFAA") in 1984. From its inception, the CFAA criminalized breaches of information security with respect to classified information on government computers and certain information on the systems of financial institutions, imposing a fine or imprisonment for up to ten years for a first offense or attempt, and a fine or imprisonment for up to twenty years for a subsequent offense or attempt. The USA Patriot Act, enacted after the September 11, 2001 attacks, extended these same penalties to private sector computers. [11] As an additional aspect of the nation's response to the September 11, 2001 attacks, Congress passed the Cyber Security Enhancement Act of 2002, which among other things, altered the range of sentences under the CFAA to reflect the prospect that violations of information security might, either intentionally or recklessly, cause risks of serious bodily injury or death. [12]

In addition, Congress has recognized that private sector information is part of the nation's critical information infrastructure, and that securing that information is important to national security. To protect such trade secrets and other proprietary information from the theft or other misappropriation, the Economic Espionage Act of 1996 (the "Economic Espionage Act") criminalized the theft of trade secrets committed either: (a) with the intention to benefit or with

knowledge that it will benefit "any foreign government, foreign instrumentality, or foreign agent"; or (b) to the economic benefit of anyone other than the [trade secret's] owner." The Economic Espionage Act was an attempt to address the threat posed by such thefts conducted, directly or indirectly, by foreign governments. Senator Arlen Specter (R-Pa), speaking in the Senate on October 2, 1996 in support of the passage of the Economic Espionage Act, summarized the threat as follows:

"For years now, there has been mounting evidence that many foreign nations and their corporations have been seeking to gain competitive advantage by stealing the trade secrets, the intangible intellectual property of inventors in this country. The Intelligence Committee has been aware that since the end of the cold war, foreign nations have increasingly put their espionage resources to work trying to steal American economic secrets. Estimates of the loss to U.S. business from the theft of intangible intellectual property exceed \$100 billion. The loss in U.S. jobs is incalculable. [13]

The Economic Espionage Act addresses this threat by defining the foreign parties whose conduct may be targeted in sweeping terms [14] and by authorizing the imposition of sentences for those who commit or conspire to commit thefts of trade secrets prohibited by the act with fines of up to \$500,000, imprisonment for up to 15 years, or both. Organizations that violate the EEA may be fined up to \$10,000,000. [15]

The Response to September 11

All of which brings us, albeit in general terms, to the legal response to the events of September 11, 2001 as it pertains to information security. Some aspects of this response dealt primarily with ensuring that sentences for cyber terrorism would be appropriate, and as discussed above, that effort is still in progress. [16]

An interesting and potentially problematic aspect of that response indicates that the search for appropriate national legal standards for information security is not complete, and is now proceeding by way of a process that is undergoing substantial change. Under the Computer Security Act, NIST was charged with responsibility for setting standards for Federal computer systems, except with regard to military and intelligence gathering systems. However, in responding to the September 11 attacks, Congress enacted the Federal Information Security Management Act ("FISMA") of 2002 [17], which enacted a distinct change in approach and

redirects authority to the Office of Management and Budget ("OMB"), part of the Executive Office of the President.

FISMA was enacted to: "(1) provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets; (2) recognize the highly networked nature of the current Federal computing environment and provide effective government wide management and oversight of the related information security risks, including coordination of information security efforts throughout the civilian, national security, and law enforcement communities; (3) provide for development and maintenance of minimum controls required to protect Federal information and information systems; [and] (4) provide a mechanism for improved oversight of Federal agency information security programs." [18]

To accomplish these goals, FISMA gives the Director of the Office of Management and Budget the responsibility to oversee agency information security policies and practices, including by: (1) developing and overseeing the implementation of information security policies; (2) requiring agencies to identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems used or on behalf of an agency (including systems operated by agency contractors); and (3) coordinating the development of standards and guidelines between NIST and the NSA and other agencies with responsible for national security systems "to assure, to the maximum extent feasible, that such standards and guidelines are complementary with standards and guidelines developed for national security systems." [19] As the Computer Security Act had done, FISMA leaves responsibility for standards pertaining to national defense systems remains primarily with the Department of Defense and the National Security Agency.

Under FISMA, the Director of OMB has the responsibility for "coordinat[ing] the development of standards and guidelines ? [between NIST and] agencies and offices operating or exercising control of national security systems (including the National Security Agency) to assure, to the maximum extent feasible, that such standards and guidelines are complementary with standards and guidelines developed for national security systems." FISMA places the Director of OMB in overall charge of setting information security standards for the federal government's systems, other than those run by national defense agencies, a position that NIST had occupied under the Computer Security Act. This change delegates authority with respect to such standards directly to the President, rather than to the Department of Commerce or other

executive agency. This change may have been intended to address the perception that the approach of the Computer Security Act was not adequate, in the wake of September 11, 2001 or perhaps more generally, for the development or implementation of information security standards adequate to protect the nation's critical information technology infrastructure.

Nor are the prospective changes in the process of setting standards for the security of critical government systems likely to stop with FISMA. There are four bills before Congress related to information security as part of national security as of the date of this article, most notably, the National Cyber Security Leadership Act of 2003, S.187, which if passed, will require the Chief Information Officer of each federal agency to report annually to the Director of OMB on the "significant vulnerabilities of the information technology" of that agency and the procedures to eliminate them.

Summary

Those involved in providing security for government agencies or their contractors obviously need to keep close tabs on the security requirements applicable to their work. That said, FISMA was enacted to "provide effective government wide management and oversight of the related information security risks, including coordination of information security efforts throughout the civilian, national security, and law enforcement communities." Under FISMA, there may be additional appropriate opportunities for commercial, non-commercial, and governmental entities as well as concerned individuals to play a constructive role in the process of setting the legal standards for information security to protect the nation's critical information infrastructure.

Relevant Links

[1] 44 U.S.C. §3542 (b)(2)(A).

[2] In 2000, the Critical Infrastructure Assurance Office (the "CIAO") of the White House, now part of the Department of Homeland Security, issued the *National Plan for Information Systems Protection, version 1.0*, in which "critical infrastructures" was defined as "[t]hose systems and assets - both physical and cyber - so vital to the Nation that their incapacity or destruction would have a debilitating impact on national security, national economic security, and/or national public health or safety." National Plan for Information Systems Protection, p. 186.

[3] Executive Order No. 13231, Critical Infrastructure in the Information Age.

[4] *Id.*

[5] The Computer Security Act amended the National Bureau of Standards Act, 15 U.S.C. §§271-278h, and the Federal Property and Administrative Services Act of 1949 (the Brooks Act), 40 U.S.C. § 759 (d).

[6] Computer Security Act of 1987, P.L. 100-235, Section 2 (b)(1).

[7] 15 U.S.C. § 278g-3 (d)(2).

[8] 40 U.S.C. § 759(d) repealed).

[9] 15 U.S.C. §§ 278g-4 (a)&(b).

[10] For more information on criminal liability for breaches of information security, see [article 3](#) of this series.

[11] USA Patriot Act, Section 808. The USA Patriot Act is the short form name of the statute entitled Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism, PL 107-56, signed into law on October 26, 2001, in response to the September 11, 2001 attacks. The USA Patriot Act amended many different federal statutes, including the CFAA and the Electronic Communications Privacy Act, to provide investigators with enhanced or expanded surveillance and investigative functions. As such, those amendments are beyond the scope of this series.

[12] The Cyber Security Enhancement Act, which is part of the Homeland Security Act of 2002, altered sentencing for CFAA violations in two respects. First, the act authorizes sentences for certain CFAA violations of: (a) a fine, imprisonment for up to twenty years, or both, where offenders "knowingly or recklessly cause or attempt to cause serious bodily injury;" and (b) a fine, imprisonment for any terms or years up to and including life imprisonment, or both, for offenders convicted of "knowingly or recklessly cause or attempt to cause death." Cyber Security Enhancement Act of 2002, Section 225 (g). Second, the Cyber Security Enhancement Act directs the United States Sentencing Commission (the "Commission") to review, and if appropriate, amend its guidelines for sentencing persons convicted of violating the CFAA. On January 17, 2003, the Commission issued a notice requesting additional comments as to how it should respond to this directive. Notice of Proposed Amendments, BAC2210-40/2211-01, U.S. Sentencing Commission, January 17, 2003, Section 6. Until the Congress considers and acts upon the final recommendations from the Commission, it is not clear what the full scope of changes in sentencing under the CFAA will be. More generally, as discussed in [article 3](#) of this series, in many cases, the same conduct that violates the CFAA also violates other federal criminal laws.

[13] Remarks of Senator Arlen Specter (R-Pa), <http://www.cybercrime.gov/EEAleghist.htm>.

[14] The Economic Espionage Act defines the term "foreign instrumentality" expansively to mean "any agency, bureau, ministry, component, institution, association, or any legal, commercial, or business organization, corporation, firm, or entity that is substantially owned, controlled, sponsored, commanded, managed, or dominated by a foreign government." 18 U.S.C. § 1839 (1).

[15] 18 U.S.C. §§ 1831(a)(5)&(b). Generally speaking, such conduct was, and remains, actionable as a civil matter under most states' law, and the Economic Espionage Act specifically preserves the rights of private parties to seek any and all applicable civil remedies. *Id.* at § 1838. The Economic Espionage Act provides

no private right of action for private parties injured by violations of the act, and designates the Attorney General as the sole party authorized to may bring civil actions to enjoin such violations. Id. at § 1836.

[16] See Notes 11-12, *supra*.

[17] 44 U.S.C. §§3541-48 (2002).

[18] 44 U.S.C. § 3541.

[19] 44 U.S.C. § 3543 (a).

[Privacy Statement](#)

Copyright 2006, SecurityFocus