USA PATRIOT Act
Considerations for Business
CSI November 2004 Alert

Rebecca Herold, CISSP, CISM, CISA, FLMI

October, 2004

U.S. Federal Judge Victor Morreo on September 29, 2004 ruled that portions of the USA PATRIOT Act were unconstitutional. The ruling found that the portion of the law that provided for the use of a "national security letter" (NSL) in lieu of a court-issued search warrant or subpoena violates both free speech and unreasonable search protections. Such NSLs can be issued under the expanded surveillance activities created through the Act without court review, and have been widely interpreted to provide for no discussion with a lawyer upon receipt of such an NSL. Among other actions, NSLs have been used to "require" ISPs to provide personal information about their subscribers and barred the ISPs from disclosing to anyone that they had received the subpoena-like order. In his ruling, Marrero is quoted as saying such NSLs were unique in U.S. law in their "all-inclusive sweep" and have "no place in our open society."

What have organizations done, and are now doing, with regard to the sweeping changes in surveillance activities that the USA PATRIOT Act spawned over three years ago? Have businesses even considered the potential impact of the Act yet? This topic is huge, and books have been written about it. I had dozens of pages written for this article before I knew it. However, for the brief space provided here, I cut out much of my philosophical discussion, and now just focus on a few commonly asked questions and examine just a few issues that have impact upon businesses and processes.

How many laws and regulations were amended by the Act?

There are at least 34:

1. Title 18, United States Code (Crimes and Criminal Procedure)
2. International Powers Act
3. Federal Rules of Criminal Procedure
4. Foreign Intelligence Surveillance Act of 1978
5. Communications Act of 1934
6. Trade Sanctions Reform and Export Enhancement Act of 2000
7. Executive Order 12947 of January 23, 1995
8. Title 31, United States Code (Money and Finance)
9. Controlled Substances Act
10. Title 28, United States Code (Judiciary and Judicial Procedure)
11. Bank Holding Company Act of 1956
12. Federal Deposit Insurance Act
13. Bank Secrecy Act (Public Law 91-508)
14. Right to Financial Privacy Act of 1978
15. Fair Credit Reporting At
16. Federal Reserve Act
17. Immigration and Nationality Act
18. Justice Appropriations Act
19. Immigration and Naturalization Service Data Management Improvement Act of 2000
20. Illegal Immigration Reform and Immigrant Responsibility act of 1996
21. State Department Basic Authorities Act of 1956

© 2004 Rebecca Herold, CISSP, CISM, CISA, FLMI All rights reserved.

22. DNA Analysis Backlog Elimination Act of 2000
23. General Education Provisions Act
24. National Education Statistics Act of 1994
25. Public Law 107-37 (To provide for the expedited payment of certain benefits for a public safety)
26. Omnibus Crime Control and Safe Streets Act of 1968
27. Public Law 105-277 (Making omnibus consolidated and emergency appropriations for the fiscal year ending September 30, 1999, and for other purposes.)
28. Public Law 106-113 (Making consolidated appropriations for the fiscal year ending September 30, 2000, and for other purposes.)
29. Victims of Crime Act of 1984
30. Atomic Energy Act of 1954
31. Title 49, United States Code
32. National Security Act of 1947
33. Telemarketing and Consumer Fraud and Abuse Prevention Act
34. Crime Identification Technology Act of 1998

Does your business fall under the jurisdiction of any of these regulations? It's likely most businesses do either directly or indirectly. Have you examined how the changes the Act made within these laws impact your business?

What businesses are impacted by the USA PATRIOT Act?
Virtually any business that handles personal information, provides connection to the Internet or does business internationally is impacted by the Act. The previously listed laws apply to a very wide swath of businesses, not to mention the other Act requirements within the regulation itself. However, the Act specifically identifies a few types of businesses specifically, such as the following:

- Financial institution: according to the Act "includes (A) any financial institution, as defined in section 5312(a)(2) of title 31, United States Code, or the regulations promulgated there under; and (B) any foreign bank, as defined in section 1 of the International Banking Act of 1978 (12 U.S.C. 3101)".
- International financial institution: according to the Act "means an institution described in section 1701(c)(2) of the International Financial Institutions Act (22 U.S.C. 262r(c)(2))."
- Money transmitting business: according to the Act, "Section 19 5330(d)(1)(A) of title 31, United States Code, is amended 20 by inserting before the semicolon the following: "or any other person who engages as a business in the transmission of funds, including any person who engages as a business in an informal money transfer system or any network of people who engage as a business in facilitating the transfer of money domestically or internationally outside of the conventional financial institutions system"."
- Nonfinancial trade or business: according to the Act includes any trade or business other than a financial institution that is subject to the reporting requirements of

© 2004 Rebecca Herold, CISSP, CISM, CISA, FLMI All rights reserved.

section 5313 and regulations prescribed under such section," receiving "more than $10,000 in coins or currency in 1 transaction (or 2 or more related transactions)."

What must businesses do for compliance with the Act?

There are many controls, procedures and related requirements detailed within the Act, in addition to all the changes that were made in the 34 laws that were impacted by the act, that covered businesses are required to implement. For example, just a few of these include the requirements are for implementation of:

- Due diligence policies, procedures, and controls that are reasonably designed to detect and report instances of money laundering, the identity of each of the owners of foreign banks, and to determine if such foreign banks provide correspondent accounts to other foreign banks.
- Customer identity verification procedures. The Department of Treasury, Office of Thrift Supervision, in 31 CFR Part 103, provides the guidance to comply with the rules for customer identification programs (CIPs) at http://www.ots.treas.gov/docs/2/25202.pdf.
- Procedures for cooperation and information sharing focusing on matters specifically related to the finances of terrorist groups and the means by which they transfer funds, between international narcotics traffickers and foreign terrorist organizations, facilitating the identification of accounts and transactions involving terrorist groups and facilitating the exchange of information concerning such accounts and transactions between financial institutions and law enforcement organizations.
- Designation of one or more persons to receive information concerning, and to monitor accounts of, certain individuals, entities, and organizations as directed within the Act, and establish procedures for the protection of the shared information, consistent with the capacity, size, and nature of the institution to which the particular procedures apply.
- Procedures governing the documentation of all transactions involving a concentration account that ensure any time a transaction involving a concentration account commingles funds belonging to one or more customers, the identity of, and specific amount belonging to, each customer is documented.
- Anti-money laundering programs, including, at a minimum: (A) internal policies, procedures, and controls; (B) the designation of a compliance officer; (C) an ongoing employee training program; and (D) an independent audit function to test programs.
- Procedures for improving financial institution utilization of the statutory exemption provisions for regular review of the exemption procedures and the training of personnel in its effective use.

How many times has the USA PATRIOT Act been used by law enforcement?

This is a hard question to answer. Many actions have likely occurred as a result of the 34 changed laws, new required procedures and additional powers created by the Act. For example, the Financial Crimes Enforcement Network (FinCEN) is identified within the Act as the agency to which financial organizations must submit Suspicious Activity Reports

© 2004 Rebecca Herold, CISSP, CISM, CISA, FLMI All rights reserved.

(SARs). According to the report, FinCEN's regulations to comply with the USA PATRIOT Act under Section 314(a) allows federal law enforcement agencies, through FinCEN, to make a reported 34,026 contacts within the financial industry to access information personal information to determine if persons are involved in terrorism or money laundering. FinCEN receives requests from federal law enforcement and upon review, transmits requests to designated contacts within financial institutions across the country. The requests contain subject and business names, addresses, and other identifying data. The financial institutions are required to query their records for data matches, including accounts maintained by the named subject during the preceding twelve months and transactions conducted within the last six months. Financial institutions have two weeks from the transmission date of the request to respond on a 314(a) Subject Information Form. The Form requires the financial institution to place only an "X" next to the particular named subject if a match was found, and to provide point-of-contact information. If the search does not uncover any matching of accounts or transactions, the financial institution is instructed not to reply to the 314(a) request. From these reports investigations are launched. The FinCEN 314(a) Fact Sheet issued August 31, 2004 reports the following activities:

> *The 314(a) system has processed 323 requests submitted by ten Federal agencies from February 18, 2003 – August 31, 2004. The federal law enforcement organizations (LE) have submitted cases in the conduct of the following significant criminal investigations:*
>
> *Terrorism/Terrorist Financing – 118 cases*
> *Money Laundering – 205 cases*
> *(02/01/2003 – 08/31/2004)*
>
> *There were 2,226 subjects of interest identified in the investigations. Of these, the Financial Institutions (FI) responded with 16,443 total subject matches: 15,587 positive and 856 inconclusive.*
>
> ***Feedback from Law Enforcement***
> *The 314(a) feedback from the LE requesters has been overwhelmingly positive and has resulted in the discovery and/or issuance of the following:*
>
> *1,277 New Accounts Identified*
> *73 New Transactions*
> *601 Grand Jury Subpoenas*
> *11 Search Warrants*
> *129 Administrative Subpoenas/Summons/Other*
> *9 Arrests*
> *2 Indictments*
> *(02/01/2003 – 08/31/2004)*

© 2004 Rebecca Herold, CISSP, CISM, CISA, FLMI All rights reserved.

What should businesses do?

Be sure to discuss the issues related to the USA PATRIOT Act with your organization's legal counsel. Ask the following questions:

- Could your organization be considered as a "financial institution" under the definitions created by the Act?
- Does your organization fall under the jurisdictions of any of the 34 impacted laws and regulations?
- Do you have the necessary procedures in place for complying with the Act?
- What impact do the Act requirements have upon your organization's offices that reside outside the U.S.?
- Are procedures in place to monitor the government watch lists as required? Currently there are at least ten separate watch lists. Multiple vendors have created software to search multiple watch lists. For more information about the watch lists, see the U.S. Office of Treasury site http://www.treas.gov/offices/enforcement/ofac/faq/.
- Are procedures in place to direct law enforcement requests to appropriate authorized persons within your organization? You need to ensure the authorized persons respond appropriately to requests for information; your organization may choose not to honor such requests depending upon the situation.

I have not even touched upon the questions related to the controls that are, or are not, in place to protect the information acquired by law enforcement activities using NSLs, or the repercussions of having names on the multiple watch lists that do not belong there, and if there are ways to correct such lists. These are important questions and worthy of scrutiny…and have been debated quite passionately in many different forums since October 2001. Such important discourses should continue. However, in the meantime, the reality is that the USA PATRIOT Act, and the affected laws, will impact businesses, and businesses need to address them.

Rebecca Herold, CISSP, CISM, CISA, FLMI is an independent information security, privacy and compliance consultant, author and instructor. She can be reached at rebeccaherold@rebeccaherold.com or 515-491-1564. Rebecca has a B.S. in Math & Computer Science, an M.A. in Computer Science & Education, created "The Privacy Papers," co-authored "The Practical Guide to HIPAA Privacy and Security Compliance," and authored "Managing an Information Security and Privacy Awareness and Training Program" all published by Auerbach.

© 2004 Rebecca Herold, CISSP, CISM, CISA, FLMI All rights reserved.