Balancing Privacy, Public Safety, and Network Security Concerns after September 11

Mark A. Rush and Lucas G. Paglia

In the aftermath of the September 11, 2001, terrorist attacks on America, Congress and the President acted swiftly to pass new legislation to make it easier for federal, state, and local law enforcement to investigate and avert suspected acts of terrorism. On October 26, 2001, President Bush signed into law the U.S.A. PATRIOT Act of 2001 (PATRIOT Act, or “the Act”). As indicated by its short title — “Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism” — the PATRIOT Act was promulgated with the paramount goal of seriously enhancing the ability of America’s intelligence and law enforcement communities to proactively prevent terrorism. True to its aim, the Act provides literally scores of amendments to existing federal statutes, all of which, to varying degrees, remove obstacles to investigating terrorist acts and acts related to or in furtherance of terrorism.

At the same time, the PATRIOT Act’s broad amendments present a number of new concerns for all businesses operating in the Internet age. As critical financial and technological infrastructures continue to serve legitimate and illicit needs — from legitimately driving America’s struggling economy to unwittingly serving as the platforms for illegal international money laundering by terrorists and their sympathizers — business owners face the threat of a “dragnet” approach to surveillance and investigation of suspected terrorists and terrorism.

Mark A. Rush, a partner at Kirkpatrick & Lockhart LLP’s Pittsburgh office, litigates commercial litigation and white-collar crime cases and represents and litigates on behalf of various corporations and individuals. From 1991 to 1995, Mr. Rush served as an assistant U.S. attorney for the Western District of Pennsylvania, where his responsibilities included the investigation and prosecution of various types of fraud and organized crime.

Lucas G. Paglia, an associate at Kirkpatrick & Lockhart LLP, practices in the area of intellectual property litigation on behalf of a variety of sports, entertainment, and technology companies.

The views expressed in this article are the authors’ own; the article does not necessarily reflect the views of any client of Kirkpatrick & Lockhart LLP or the firm itself. For more information about Kirkpatrick & Lockhart’s white-collar crime/criminal defense practice, please visit www.kl.com/PracticeAreas/WCCrime/wcrime.stm.
ensure they are prepared to withstand the tightrope walk of balancing overwhelming national security concerns with their own network integrity and privacy issues, all businesses that rely in any way on computers should understand the full implications of the Act. This article is designed to help you navigate these uncharted waters by:

- Summarizing the most significant, salient features of the PATRIOT Act as they relate to computer network integrity and the prevention of cyberterrorism
- Discussing various business, legal, and practical issues that private industry is likely to face in the coming months and years under the Act
- Exploring the ways in which businesses can ensure full comprehension of and compliance with the many provisions and mandates of the PATRIOT Act
- Concluding with a discussion of the many federal resources available to businesses as they prepare to address the concerns noted above arising from the Act

THE U.S.A. PATRIOT ACT OF 2001
The Act contains a number of specific amendments to existing criminal laws and enabling statutes, all of which are designed to streamline early detection and investigation of suspected terrorist activity. The following is a summary of those provisions of the new law most pertinent to network security and privacy concerns.

Electronic Surveillance
Title I of the PATRIOT Act directs the head of the U.S. Secret Service to “take appropriate actions to develop a national network of electronic crime task forces” throughout the country. The main thrust of this initiative is the prevention, detection, and investigation of various forms of electronic crimes, especially potential terrorist attacks against critical technological infrastructures and financial systems.

Along with its increased focus on eliminating cyber-terrorism, Congress significantly increased funding for the Federal Bureau of Investigation’s Technical Support Center (TSC), which provides computer and related technological support for the Bureau’s tactical operations against terrorism. The PATRIOT Act authorizes the appropriation of $200 million to the TSC for each of the fiscal years 2002 through 2004. Such appropriations are in addition to the new “Counterterrorism Fund,” created with a broad mandate to reimburse any federal government expenditures incurred in the course of investigating, prosecuting, or countering domestic or international terrorism.

Finally, under Title I, the Act broadens presidential authority under the International Emergency Powers Act, enabling the federal government to seize the property of any foreign person, organization, or country that the President determines was used to plan, authorize, aid, or engage in armed hostilities or attacks against the United States. Under this broad provision, the President may confiscate not only financial assets and real property of suspected terrorists but also computers and other hardware, computer files and related software and whatever other components of technological infrastructures and network systems that the government believes were used to facilitate terrorist activity.

Title II of the PATRIOT Act provides sweeping enhancements to existing laws governing criminal surveillance procedures, in particular the Electronic Communications Privacy Act. Under this Title, the federal government is granted increased authority to intercept wire, oral, and electronic communications relating to suspected
terrorist activity. In addition, the Act amends the Computer Fraud and Abuse Act (CFAA) to broaden government authority to intercept such communications if they relate to suspected computer fraud and abuse as well. Thus, the Act places special focus on the investigation of computer systems and networks that are or may be tools of terrorism.

Importantly, the PATRIOT Act amends existing search warrant law to allow for “roving” warrants to intercept wire, oral, and electronic communications. No longer will such warrants be limited to one particular wire fund transfer or telephone exchange or computer. Instead, the government may exercise its broad investigative authority under the Act to intercept any communications by any suspected terrorist or terrorism accomplice, with access to any financial, telephone, or computer system or network used by such suspects. Obviously, the reach of an investigation into suspected terrorism could extend into literally hundreds of different technology systems throughout the country.

Other key aspects of Title II include:

■ Expanding the scope of allowable seizures of voice mail messages pursuant to warrants
■ Expanding the scope of subpoenas for records of electronic communications
■ Allowing for delayed notice of search warrants to permit “sneak-and-peek” searches of real and electronic property in antiterrorism investigation and surveillance
■ Allowing ex parte application for court orders requiring the disclosure and production of business records and tangible things belonging to any person or entity
■ Broadening the reach of permissible interception of computer trespass communications
■ Providing for nationwide service of search warrants for electronic evidence

**Money Laundering and Financial Records**

Title III of the PARTIOT Act is called the “International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001.” This portion of the Act makes it more difficult for foreign terrorists and criminals to launder funds through U.S. financial systems. The new legislation empowers the Treasury Department with broad discretion to create and enforce regulations regarding compliance programs and recordkeeping requirements. As a result, government scrutiny will increase dramatically on financial institutions dealing with suspect foreign countries deemed to be of “primary money laundering concerns,” and all institutions that terrorists potentially could use to launder money may be required to maintain records, file reports, or both, with respect to foreign transactions.

In addition, Title III requires financial institutions that open, maintain, administer, or manage private accounts for non-U.S. persons to establish “appropriate, specific and, where necessary, enhanced due diligence policies, procedures and controls” reasonably designed to detect and report money laundering via such accounts. Financial institutions also must share information on suspected money laundering with law enforcement and each other to optimize antiterrorism efforts. Finally, Title III requires all financial institutions to improve verification of account holders and to enhance anti-money-laundering practices and procedures.

As a result of all these new requirements, financial institutions now must develop specific programs to comply with the Act or face harsh consequences if they do not. If financial institutions fail to adopt enhanced due diligence, screening, verification, reporting, and compliance procedures under the Act, they will invite government and law enforcement scrutiny and may open themselves to investigation, prosecution, and conviction if they are anything less than vigilant about insulating their own networks from terrorist-supporting money laundering.
Under Title V, entitled “Removing Obstacles to Investigating Terrorism,” the Act broadens government access to private financial records and private credit reports sought for counterterrorism purposes. The Act also empowers the Secret Service with independent authority to investigate offenses under the antiterrorism bill. Thus, the number and types of government agencies that may have access to a company’s business and financial records — including the FBI, the CIA, the IRS, the National Security Administration, and now the Secret Service as well — has increased along with the permitted scope of such access.

**Protecting Critical Infrastructures**

Title VII of the PATRIOT Act provides for increased information sharing among federal, state, and local law enforcement to facilitate better detection, investigation, and prosecutions of multi-jurisdictional terrorist conspiracies and acts. Congress has authorized the appropriation of $150,000,000 to help law enforcement establish and operate secure information sharing systems for this purpose.

Title VIII of the Act focuses on deterrence and prevention of cyber-terrorism, or the use of computer networks to facilitate terrorist acts. The Act amends the CFAA to broaden and clarify the scope of protected computers, which now includes any computer located outside the United States that is used in a manner affecting interstate commerce or foreign commerce or communication of the United States. The Act also broadly covers any computer-related offense that poses a threat to public health or safety, thus making antiterrorism investigations of suspected hackers, disruptions of service, economic cyber-espionage, and affected networks easier for the government. In addition, the Act increases criminal penalties for violations of the CFAA. Thus, the PATRIOT Act provides a heightened deterrence against cyber-terrorism.

Title VIII also fosters the development and support of regional cyber security forensic capabilities. Under the Act, the Attorney General must establish regional computer forensic laboratories to:

- Support and improve existing examinations of seized or intercepted computer evidence relating to suspected cyber crimes, including cyber-terrorism.
- Provide training and education for federal, state, and local law enforcement and prosecutors regarding investigations, forensic analyses, and prosecutions of computer-related crimes, including cyber-terrorism.
- Assist enforcement of federal, state, and local criminal laws relating to computer crime.
- Facilitate and promote the sharing of federal law enforcement expertise and information about the investigation, analysis, and prosecution of computer-related crime with state and local law enforcement and prosecutors, including the use of multi-jurisdictional task forces.

Finally, under Title X of the Act, Congress specifically finds that “a continuous national effort is required to ensure the reliable provision of cyber and physical infrastructure services critical to maintaining the national defense, continuity of government, economic prosperity, and quality of life in the United States.” To assist in this effort to preserve critical infrastructures, the Act establishes the National Infrastructure Simulation and Analysis Center (NISAC), a public/private partnership to combat cyber-terrorism and serve as a “source of national competence” to support counterterrorism,
threat assessment, and risk mitigation activities designed to address infrastructure protection and continuity concerns.35

Critical to the success of NISAC will be the modeling, simulation, and analysis of technological infrastructures to enhance understanding of the complexities and vulnerabilities of such systems and to facilitate modifications thereof to mitigate threats to critical infrastructures across the board.36 The Act contemplates state and local government, and the private sector will contribute to NISAC data as necessary to create and maintain models of such systems and of critical infrastructures generally, so that NISAC can educate and train policymakers and the private sector alike on: (1) the implications of disturbances to such infrastructures, (2) optimal responses to such incidents, and (3) enhancing the stability of, and preserving, critical infrastructures.37 The modeling, simulation, and analysis resources of NISAC will be available to all federal, state, and local entities responsible for critical infrastructure protection and policy.38

IMPACT OF THE PATRIOT ACT ON AMERICAN BUSINESSES

The expanded reach of electronic surveillance authority under the PATRIOT Act presents a myriad of new concerns for financial institutions, high-technology companies, and non-technology entities alike. For example, because the Act expands law enforcement’s authority to intercept suspected terrorists’ communications by telephone, e-mail, Internet, or other means, financial institutions that are subject to unauthorized network access (hacking) also should expect more frequent law enforcement inquiries and requests to cooperate with new computer forensics efforts under the PATRIOT Act. These entities in particular will be impacted, as law enforcement will pay particular attention to any remotely suspect accounts and transactions, as well as employees associated with them. Under the Act’s broad reach, all such individuals are likely to be monitored closely.

Further, because law enforcement is now permitted to obtain warrants for “roving wiretaps” to monitor nationwide any communication devices employed by suspected terrorists, all systems and institutions used by suspects are susceptible to surveillance as well. This surveillance will extend to all individuals and groups having any contact with such suspects. As a result, law enforcement can access and monitor private computer system networks, telecommunication systems, and Internet accounts of any individual suspected of engaging in or furthering terrorist activity. Virtually every owner and operator of integrated network or communication systems may be impacted by this broader authority.

In addition, all such institutions must cooperate with law enforcement officials investigating such communications. Thus, an ISP or long-distance carrier may be compelled to turn over customer information if the FBI claims the records sought “are relevant to an authorized investigation to protect against international terrorism.” Clearly, the reach of an investigation into suspected terrorist activity will extend to nearly every sector of the digital and telecommunications industry, and beyond.41

Restrictions on Encryption?

An even more basic concern to all businesses relying on network systems and Internet communication is the threat of restrictions on encryption in the wake of the terrorist attacks. Encryption is the process by which data is encoded so that it cannot be read by unintended third parties. It is the principal means by which financial institutions and E-businesses alike ensure private, secure transactions over the Internet and via
other electronic means (e.g., wire transfers). Since September 11, some legislators have called for restrictions on encryption technology unless it permits law enforcement access to otherwise coded data.42

Although such anti-encryption language was not included in the PATRIOT Act, it may well appear in the next wave of legislation aimed at helping the government fight terrorism.43 Indeed, in light of strong suspicions that terrorist networks use encryption tools to shield their communications and transactions from law enforcement and given the federal government’s broad investigative mandate under the Act, such legislation appears imminent. If banks and other businesses are compelled to adapt encryption technology to facilitate law enforcement access to highly sensitive but potentially suspect financial, communication, and other data, the landscape of the Internet and its support structures will change forever. As a result, secure online banking and commerce undoubtedly will be affected and may be compromised absent proactive efforts to maintain security in new and different ways.

Aggressive Government Enforcement
Recent examples of the government’s commitment to the war on terrorism illustrate the real-world impact of new computer crime laws on U.S. business and financial interests. In one case, the FBI arrested a computer hacker who attempted to sabotage Adobe’s eBook Reader software by allowing potential users to decrypt Adobe’s built-in copyright safeguards. Despite Adobe’s request that the government not prosecute Dmitry Skylarov, the government is aggressively pursuing the hacker and his employer under the criminal provisions of the Digital Millennium Copyright Act.44 Both men face up to ten years in prison and fines up to $250,000, and Adobe now remains in the middle of a criminal prosecution and potentially disruptive ongoing investigation over which it has no control.38

More recently, federal law enforcement officials raided a number of money-exchange operations throughout the United States in a sweep to halt the illegal transfer of funds suspected of aiding terrorist activity and also to gain more information on the sophisticated financial networks used by terrorists.46 Although the initial search-and-seizure efforts focused on two specific informal financial networks — and their American outlets — apparently associated with Osama bin Laden, the government’s affirmative action to disrupt the terrorists’ financial networks have touched and will continue to impact legitimate financial institutions and communications interests as well.

Privacy Concerns
Already there is some indication that the PATRIOT Act’s allowance of so-called “sneak-and-peek” search warrants might spark Fourth Amendment lawsuits. Such warrants, which permit delayed notice of a search for physical evidence if there is reasonable cause to believe notice will hamper the investigation, are not tied to antiterrorism investigations under the Act.47 As a result, some privacy advocates fear the government will extend “sneak-and-peek” authority well beyond the Act’s intended scope of detecting and preventing international terrorism.48 However, even if law enforcement limits such searches to antiterrorism efforts, the number and types of business interests and entities susceptible to such investigation are large indeed.

Practically speaking, each U.S. financial institution, telecommunication provider, E-business and high-tech company must operate under the assumption that its network is susceptible to covert search by law enforcement at any given time.
is susceptible to covert search by law enforce-
ment at any given time. Further, all such
entities must assume that every foreign cli-
ent who even remotely raises a suspicion of
questionable ties to terrorist activity or
funding may subject them to such investiga-
tion and scrutiny. Due diligence regarding
current customers and potential customers
will become a top priority.

Finally, private industry must consider
the likelihood of greater scrutiny of techno-
logical infrastructures by the newly created
White House Office of Homeland Security
(OHS) under the Foreign Intelligence Sur-
veillance Act (FISA). Under FISA, the
President may direct covert surveillance for
up to one year before obtaining a warrant, in
order to investigate any target suspected of
engaging in international terrorism or other-
wise threatening national security, as well
as any financial or computer resources used
by the target. Thus, in pursuit of the pro-
tection of national security and emboldened
by the PATRIOT Act’s broadening of
search-and-seizure powers generally, FISA
investigations are likely to intensify as well.
In the aftermath of September 11, courts
will likely find such covert surveillance —
and related law enforcement access to tar-
geted networks and infrastructures — “rea-
sonable” and proper more often than not.

As the foregoing illustrates, the
PATRIOT Act presents a multitude of new
weapons to aid intelligence and law
enforcement communities in the fight
against terrorism. At the same point, the
Act also presents a new set of concerns for
every business owner participating in
today’s technology-driven marketplace.
Fortunately, a number of public/private
cooperatives exist to assist law enforce-
ment and industry alike in optimizing anti-
cyber-terrorism efforts without unnecessar-
ily compromising network security and pri-
vacy interests.

FEDERAL RESOURCES TO PROTECT
NETWORK SECURITY AND
Privacy Concerns in the Fight Against
Cyber-Terrorism

Several federal agencies participate in the
investigation of cyber-crimes, including the
FBI, the Secret Service, U.S. Customs, the
Postal Inspection Service, and the Bureau of
Alcohol, Tobacco and Firearms, to name a
few. Each of these departments will play a
part in facilitating the investigation and
information sharing contemplated under the
PATRIOT Act and mandated by Attorney
General John Ashcroft at the recent Antiter-
rorism Coordination Conference in Wash-
ington, D.C.

Better communication and
coordination will strengthen the ability of
law enforcement to help all businesses
detect and prevent cyber-terrorism and
other network-related crimes.

Valuable Government Resources

In this vein, private industry has at its dis-
posal a number of cooperative government
resources specifically created to aid in the
fight against cyber-crimes. Chief among
them is the National Infrastructure Protec-
tion Center (NIPC), an interagency, pub-
lic/private entity designed specifically to
combine government and industry forces to
combat high-tech crimes. The NIPC
includes representatives from the FBI, the
Department of Defense, the Department of
the Treasury, and the Department of
Energy, as well as the intelligence commu-
nity, state and local governments, and the
private sector. NIPC agents work directly
with private-sector businesses to establish
computer crime crisis response procedures
and a coordinated, timely mechanism for
dealing with technological infrastructure
breaches and suspected cyber-crimes.

Other key resources include:

- The National White Collar Crime Center
  (NW3C), a nonprofit organization dedi-
cated to providing a nationwide support net-
work for enforcement agencies involved in
  the prevention, investigation, and prosecu-
tion of economic and high-tech crime.
The Internet Fraud Complaint Center (IFCC), a partnership between the FBI and the NW3C whose stated mission is to address fraud committed over the Internet. The FBI’s National Computer Crime Squad (NCCS), which investigates suspected intrusions into financial and commercial computer systems, especially violations of the CFAA and the Economic Espionage Act, and coordinates with FBI counterparts in foreign jurisdictions, especially when international computer espionage impacts U.S. public or private business interests. The Computer Emergency Response Team Coordination Center (CERT/CC), a federally funded research and development effort by the Department of Defense under contract with Carnegie Mellon University (CMU) that has developed systematized response mechanisms for incidents of computer system intrusion and methods for preventing future intrusions.

These agencies work with private industry to protect network security and maintain privacy interests that all Internet-dependent businesses value so highly.

According to Special Agent Dan Larkin of the FBI, early detection and reporting of suspected incidents of computer system intrusion are key to averting serious — and perhaps irreparable — technological damage and mounting a successful criminal prosecution. Moreover, proactive efforts by private businesses will enhance the government’s fight against terrorism on the ground and in cyberspace. All companies should vigilantly secure their computer networks and routinely upgrade the security systems that safeguard critical technological infrastructures. As Larkin notes, the federal government’s ability to assist private industry depends to a large degree on how much and how well the private sector has helped itself and shared its technological advances in the proactive safeguard area, as well as the reactive or forensic area.

Valuable Public/Private Resources

Two additional resources can further assist in the fight against cyber-terrorism. First is CMU’s new Institute for Homeland Security Research, a cooperative between the university and private industry that is designed to help the federal government, and in particular the OHS, strengthen national security mechanisms. In particular, the Institute already is developing a system for alerting the nation’s population about emergency health risks.

Second, the FBI is well on the way to finalizing formation of the National Cyber-Forensics Training Alliance (NCFTA, or “the Alliance”), a multistate laboratory and training alliance consisting of industry, academic, and government representatives engaged in cyber-forensic analysis, tactical response development, and technology vulnerability analysis. In addition to key participation from private industry giants and critical academic expertise from CMU, West Virginia University, and other universities, NCFTA has received substantial input and support from the Department of Justice’s Computer Crime and Intellectual Property Section (CCIPS), NW3C, and a broad range of federal and state law enforcement offices. In light of the PATRIOT Act’s mandate to enhance cyber-forensic capabilities, the Alliance is poised to play a critical role in bridging the gap between law enforcement cyber-forensics and private-industry efforts to prevent, detect, and investigate computer-related crime and terrorist activity.

According to FBI Special Agent Bill Shore, a focal point of the NCFTA project is the partnership established among the FBI, NW3C, and academic communities of CMU and WVU. This partnership facilitated a survey of industry, government, and academia to assess evolving cyber-crime and Internet-related vulnerabilities. As a result, the Alliance was able to formulate overlapping objectives and prioritize resource strengths to maximize the efficacy of the group to all three sectors.

Critical to the war on cyber-terrorism, NCFTA is designed to assemble an unparalleled pool of critical network-related data,
combining intelligence from the IFCC and CERT/CC to continually develop and update response strategies, forensics, and advanced training methods, so that private industry can proactively shield its technological infrastructures from cyber-crime. NCFTA aims to develop both proactive and reactive cyber-security mechanisms designed to facilitate communication and intelligence-sharing with law enforcement. Ultimately, Special Agent Shore and the FBI see NCFTA as a state-of-the-art project that joins public and private resources and law enforcement to create permanent synergies designed to: (1) optimize cyber-forensic analysis and critical infrastructure protection, and (2) provide a platform for enactment of broad-based regulations and internationally supportable law governing such proactive anti-cyber-terrorism efforts.

CONCLUSION

In a world of business and finance that depends on secure technological infrastructures for survival, computer network integrity will always be a top priority. Following passage of the PATRIOT Act, the federal government and law enforcement are likely to act in ways that seek to preserve such system integrity against the evils of terrorism but which may also have the unintended effect of compromising network access, security, and privacy concerns. A healthy understanding of the new law, including especially its due diligence and information-seeking and -sharing requirements, will help all businesses to minimize such concerns. Familiarity with the many federal and public/private resources available to help in the fight against cyber-crime will lower risk even more.

© 2001 Kirkpatrick & Lockhart LLP.

Notes

2. Ibid. at §105.
3. Ibid.
4. Ibid. at §103.
5. Ibid. at §101.
8. 18 U.S.C. §§2901 et seq.
9. PL 107-56, 2001 HR 3162 at §201 et seq.
12. See, e.g., Ibid. at §206, 219.
13. Ibid. at §209.
15. Ibid. at §213.
16. Ibid. at §215.
17. Ibid. at §217.
18. Ibid. at §220.
20. PL 107-56, 2001 HR 3162 at §§301 et seq.
21. Ibid. at §311(a).
22. Ibid. at §311(b).
23. Ibid. at §312.
24. Ibid. at §314.
25. Ibid. at §§326, 352. For more on the IMLA, see Rush and Hackett (note 19).
26. Under the PATRIOT Act, the maximum fine for money laundering, or any violation of money laundering laws by financial institutions, has been increased to $1 million (ibid. at §363).
27. PL 107-56, HR 3162 at §505.
28. Ibid. at §506.
29. Ibid. at §701.
30. Ibid.
32. Ibid. at §814(a), amending 18 U.S.C. §1030(a)(5).
33. Ibid. at §814(c), amending 18 U.S.C. §1030(c).
34. Ibid. at §1016(b)(3). The Act defines “critical infrastructure” as “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters,” ibid. at §1016(e).
35. Ibid. at §1016(d).
36. Ibid. at §1016(d)(2).
37. Ibid.
38. Ibid. at §1016(d)(3).
40. Ibid. at §§206, 219.
41. Ibid. at §215. On the other hand, in a recent development, the European Union declined to adopt the United States’ broadening of electronic surveillance and investigation capabilities, opting instead to maintain limited access provisions relating to telecommunications data in a Union-wide data-protection law currently in draft before the European Parliament. See “European Union Set To Vote on Data Law,” http://www.nytimes.com/2001/11/13/technology.
42. See Mike Godwin, “Just Say No: Will Strong Cryptography Be One of the First Casualties in...
What is IPSec? What's a VPN? Why do they need each other?

Virtual Private Network (VPN) has become one of the most recognized terms in our industry, yet there continuously seems to be different impressions of what VPNs really are and can become.

A Technical Guide to IPSec Virtual Private Networks provides a single point of information that represents hundreds or resources and years of experience with IPSec VPN solutions. It cuts through the complexity surrounding IPSec and the idiosyncrasies of design, implementation, operations, and security. Starting with a primer on the IP protocol suite, the book travels layer by layer through the protocols and the technologies that make VPNs possible. It includes security theory, cryptography, RAS, authentication, IKE, IPSec, encapsulation, keys, and policies. After explaining the technologies and their interrelationships, the book provides sections on implementation and product evaluation.

For only $54.95, A Technical Guide to IPSec Virtual Private Networks arms information security, network, and system engineers and administrators with the knowledge and the methodologies to design and deploy VPNs in the real world for real companies.

Call (800) 272-7737 and Order Catalog #AU0876 Today!
Order online at www.auerbach-publications.com

James S. Tiller
by James S. Tiller, CISSP, CCNA, CCDA, MSCE+I, Belenos, Inc.