A Message from the Chair: The Tasks Ahead

On October 26, 2001, the President signed a sweeping antiterrorism bill entitled the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001. Based on legislation sent to the Hill by the Department of Justice, the bill includes provisions to expand authorities for criminal investigations and intelligence collection, lower the barriers between these two kinds of activities, and authorize funding to improve the capabilities of key federal agencies.

This legislation was passed with unusual speed—though not as quickly as many had predicted—and under unusual circumstances. There were no committee votes so there are no committee reports to provide insight as to legislative intent. It was negotiated and voted on in the aftermath of the most devastating terrorist attack this country has ever suffered, amidst warnings of reprisals for US military action and a biological attack that forced the offices of the Congressional negotiators to close down. In this high-pressure environment, the drafters worked to balance the obligation to protect the people of this nation and the responsibility to preserve their civil liberties. How well the Act accomplishes these objectives depends not only on the compromises reached by the negotiators but also on the way the law is implemented and overseen.

Implementation and Oversight

The executive branch will have to draft guidelines and develop procedures governing the use of the authorities granted by this new law. For example, new authority with respect to the use of pen registers and trap and trace devices for computer transmissions prohibits the interception of the “content” of a communication. However, content is not defined. The Attorney General has reportedly indicated that the subject line, which is often included in the routing information of an email, is considered “content” and will somehow be excluded. Less clear is how investigators will treat the URLs of Internet sites visited by a surveillance target. Is the URL of a particular news article on a host site more like content or a phone number? These issues may ultimately have to be resolved by the courts but, in the interim, the Department of Justice will need to provide guidance to investigators.

The Act contains some explicit requirements for the development of guidelines, but little or no direction regarding their objective or content. It is important that implementing measures provide clear guidance to officers in the field as well as those at the headquarters of the relevant agencies. A vague line between permissible and impermissible activity carries the risk of over-reaching or under-achieving. These new authorities will fail to achieve their purpose if agents are so worried about crossing a blurry line that they are reluctant to exercise the full scope of permitted authority. By the same token, lack of clear guidance can lead to unwarranted infringement of civil liberties. These guidelines should be reviewed periodically in light of reports from the field and clarified when necessary.

Nor has the Congress completed its task with the passage of this legislation. Effective oversight of the use of the authorities contained in this Act is particularly important given the haste with which it was drafted and the requirement to reconsider many of the provisions in four years. The key oversight committees should develop criteria with which they will measure the effectiveness and appropriateness of these laws over the coming years. Some reporting requirements are already specified in the legislation, others may have to be added. Executive branch oversight, such as that mandated in Title X with regard to civil rights complaints compiled by the DoJ Inspector General and reported to Congress, can supplement this legislative responsibility. Moreover, while the sunset provisions only require reconsideration of specified provisions in four years, Congress has the ongoing prerogative—and obligation—to oversee the broad range of activities undertaken in the war against terrorism and strengthen or modify laws as appropriate.
Standing Committee Activities

The Standing Committee will continue its mission of providing a forum for informed discussion and debate on these and other key issues of law and national security. Immediately after the initial draft of the antiterrorism legislation was introduced, the Committee gathered a group of national security law experts together to discuss the provisions and begin to analyze their implications. Individuals were then better able to respond to requests from the Hill for input on the bill and other terrorism-related legislation. This was followed on September 28 by a special breakfast meeting, attended by over 175 members and friends of the Committee, to identify and discuss issues raised by the attacks of September 11 and their aftermath. Congressional and executive branch officials were among those who attended and participated in the dialogue. A summary of that meeting is included in this newsletter.

The Committee is also involved in the efforts of the broader American Bar Association community. We participated in the ABA Task Force on Terrorism and the Law, established by the President of the ABA to provide comments to the Congress on the antiterrorism legislation. In addition, the Standing Committee has been asked to put together a panel on terrorism for the Mid-Year meeting of the ABA in February. This program will be held on Saturday, February 2, from 2:00 - 4:00 p.m. at the Philadelphia Marriott.

Committee Task Forces

As a follow up to the breakfast meeting, the Standing Committee is establishing several task forces that will examine ongoing issues in particular subject areas. These September 11 task forces can provide input for the implementation and oversight efforts of the executive and legislative branches, as well as fostering discussion of issues not addressed in this legislative package. It is our hope that these task forces will inform the national debate and discussion through speakers, symposiums, papers, and/or articles in the National Security Law Report or other publications. Where appropriate, these task forces may propose policies for adoption by the Standing Committee or the American Bar Association as a whole. A list of the task forces and their coordinators is provided below. If you are interested in participating in one or more of these task forces, please visit our Web Site at www.abanet.org/natsecurity.

<table>
<thead>
<tr>
<th>Topic</th>
<th>Coordinator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Law Enforcement and Intelligence</td>
<td>Mike Smith and Stewart Baker</td>
</tr>
<tr>
<td>Terrorist Assets</td>
<td>Steve Kroll and Pam Parizek</td>
</tr>
<tr>
<td>Immigration and Border Patrols</td>
<td>David Anderson</td>
</tr>
<tr>
<td>Public Health/Domestic Responses</td>
<td>Dale Bosley and Gene Matthews</td>
</tr>
<tr>
<td>Critical Infrastructure Protection</td>
<td>Lee Zeichner</td>
</tr>
</tbody>
</table>

National Security Law in a Changed World

On November 29-30, 2001, the Standing Committee will hold its 11th Annual Review of the Field Conference entitled “National Security Law in a Changed World.” It has become almost trite to note that the world was forever changed on September 11. What is less well understood is the implication of that change for every aspect of national security. At this year’s annual conference, we will examine these changes as reflected in new challenges for the military; the foreign policy roles of the President, Congress, and the States; the importance of international law in preserving our national security; and the evolving relationship between law enforcement and intelligence. As always, we will again hear from key executive and legislative branch lawyers about the issues with which they have been dealing and those on the horizon.

Bioterrorism Laws

For over 15 years, the Standing Committee has held numerous conferences, panels, and symposiums on terrorism. For example, in June of last year, the Committee, in conjunction with the McCormick Tribune Foundation, held a two-day symposium on the legal issues raised by the threat of catastrophic terrorism. As a follow-up, a second conference this past April with the Centers for Disease Control brought together public health officials from across the country, along with their lawyers, to examine the legal framework for the public health response to a bioterrorism attack and develop a plan of action. Recently, some of the conference participants, fulfilling a commitment made at the conclusion of that conference, circulated an initial draft of a model emergency public health law for consideration by states. This is just one example of the kind of concrete progress that can be achieved when the right people come together to identify and address issues of common concern.
Conclusion
The issues raised by our responses to the attacks of September 11 are among the most challenging our nation has ever faced. Decisions policymakers make today will have far-reaching consequences. Organizations like the Standing Committee can play an important role in informing those decisions and enhancing public understanding of the issues at stake.

Summary of Key Provisions in USA PATRIOT Act of 2001

(Chair’s note: The Standing Committee is indebted and offers special thanks to Dale Bosley, Stephen Kroll, Gordon Lederman, Joshua Levy, and Michael Smith for their very quick assistance in summarizing the key provisions)

Title I — Enhancing Domestic Security Against Terrorism

- Establishes a Counterterrorism Fund to reimburse DOJ for costs incurred in counterterrorism efforts.
- Authorizes $600 million over three years for the FBI’s Technical Support Center.
- Sense of the Congress condemning discrimination against Arab and Muslim Americans.
- Directs Secret Service to develop a national network of electronic crime task forces.
- Provides for military support to law enforcement under certain emergency circumstances where required to enforce prohibition on use of chemical or biological weapons.
- Expands President’s authority under IEEPA to include any property subject to US jurisdiction, allow orders to block assets during an investigation, and provide for the confiscation of property of foreign persons, organizations, or countries determined to be involved in armed hostilities or attacks against the US.

Title II — Enhanced Surveillance Procedures

- Seeks to significantly enhance the government’s ability to collect, analyze and share intelligence information concerning international terrorism.
- Amends Title III of the Omnibus Crime Control and Safe Streets Act (18 U.S.C. 2501 et seq) (Title III) to:
  - provide new criminal statute predicates that would support an application for a warrant;
  - permit seizure of voice mail pursuant to a warrant;
  - permit the results of surveillances to be shared with intelligence agencies, subject to Attorney General procedures if the information concerns a United States person; and
  - expand authority to intercept “computer trespasser communications.”
- Amends the Foreign Intelligence Surveillance Act (50 U.S.C. 1801 et seq) (FISA) to:
  - enable surveillances to be implemented against targets who attempt to thwart surveillance, e.g., by switching phones, without going back to the Foreign Intelligence Surveillance Court;
  - lengthen, in certain cases, the duration of initial surveillances and renewals;
  - broaden the use of pen registers and trap and trace devices “to protect against international terrorism or clandestine intelligence activities”; this authority may not be used against USP’s solely on the basis of activities that are protected by the First Amendment. A similar change is made to the FISA provision that permits access to records and other items; and
  - permit surveillance under FISA when foreign intelligence is “a significant purpose” rather than “the purpose”.

-3-
• Amends the Electronic Communications Privacy Act (ECPA) (18 U.S.C. 2701 et seq) to:
  - broaden the scope of subpoenas for records of electronic communications to cover internet sessions but not the content of those sessions;
  - permit emergency disclosure of electronic communications to protect life and limb; and
  - permit nationwide service of warrants for electronic surveillance.

• Modifies the Federal Rules of Criminal Procedure (FRCP) to:
  - permit delayed notification of the execution of a warrant when the warrant prohibits a seizure and disclosure may have an adverse result on the investigation ("sneak and peek");
  - expand the scope of court orders for pen registers and trap and trace devices to collect information on internet sessions but not including the content of those sessions; and
  - give nationwide effect to search warrants issued in terrorism investigations.

• Enhances sharing of information between the intelligence and law enforcement communities through the change to Title III noted above and through a modification to Rule 6 (e) of FRCP to permit the passage of information obtained by a grand jury to any intelligence or national defense official provided it is "foreign intelligence information" (a defined term).

• Permits "aggrieved persons" to seek money damages in a civil action against the United States for improper disclosure of information obtained pursuant to FISA, ECPA and Title III.

• Contains a sunset provision (December 31, 2005) for most of the changes to FISA and certain changes to ECPA and Title III.

Title III - International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001

• Seeks to increase significantly the strength of U.S. measures to prevent, detect, and prosecute international money laundering and the financing of terrorism, and to facilitate dissemination of financial information to the intelligence community in connection with efforts to fight international terrorism.

• Amends the Bank Secrecy Act (12 U.S.C. 1951-59 and 1829b, 31 U.S.C. 5311-5332) in a number of ways, most importantly to:
  - give the Secretary of the Treasury, in consultation with other senior government officials, authority to impose one or more of five new "special" recordkeeping, reporting, and account restriction "measures" against foreign jurisdictions, financial institutions, transactions or types of accounts that the Secretary, after consultation with Secretary of State and the Attorney General, determines to be of a "primary money laundering concern" to the United States.
  - require a U.S. financial institution that maintains a correspondent account or private banking account for a non-United States person to establish appropriate, specific, and, where necessary, enhanced due diligence procedures that are reasonably designed to detect and report instances of money laundering.
  - mandate additional, more specific controls and monitoring for accounts opened by offshore banks or banks from countries with substandard money laundering controls and for private banking accounts, especially those potentially owned by foreign political figures.
  - bar any depository institution or registered broker-dealer operating in the United States from establishing, maintaining, administering, or managing a correspondent account in the United States for a foreign "shell" or "brass plate" bank, i.e., a bank that does not have "a physical presence in any country."
  - require foreign banks with U.S. accounts to appoint U.S. agents for service of process in connec-
tion with records relating to U.S. account transactions, and require the closing of any such account upon notice from the Department of Justice or Treasury that a subpoena served on such agent has not been either complied with or challenged.

-require issuance within one year of regulations for uniform identity verification requirements for U.S. nationals opening financial institution accounts, and ask Treasury to recommend within six months similar requirements (and perhaps a uniform identification number system) for non-United States nationals opening such accounts.

-require financial institutions in the U.S. to set up anti-money laundering programs.

-require issuance by July 1, 2002, of regulations requiring reporting by securities broker-dealers of suspicious transactions.

-clarify application of the Bank Secrecy Act to underground banking and money transmission systems.

- Amends Title 18 in a number of ways, most importantly to:

- add a number of “specified unlawful activities,” including corruption directed at foreign governments, support for designated terrorist organizations, and criminal export control violations, to the criminal money laundering statutes.

-mandate a “law of the U.S.” solution to disputes involving forfeitures of funds in interbank accounts.

-make banks that do not operate in the U.S. subject to the extraterritorial jurisdiction provisions of the criminal money laundering statutes.

- Amends the purpose and disclosure provisions of the Bank Secrecy Act to include as a statutory purpose the preservation of records and dissemination of required reports “for use in the conduct of intelligence and counterintelligence activities, including analysis, to protect against international terrorism.”

- Amends the Right to Financial Privacy Act (12 U.S.C. 3401 et seq.) (the “RFPA”):

- to permit records obtained pursuant to the RFPA’s terms by one agency (e.g., a law enforcement agency) to be transferred to another agency if the records are relevant to an “intelligence or counterintelligence activity, investigation or analysis related to international terrorism,” as well as to a law enforcement inquiry (as under existing law).

-to extend existing special RFPA procedures for requesting records relevant to counter-intelligence or foreign-positive intelligence inquiries, and protective function inquiries, to requests from “a government authority authorized to conduct investigations of, or intelligence or counterintelligence analyses related to, international terrorism” for the purpose thereof.

-to permit records obtained by grand jury subpoena to be used for one of the purposes for which RFPA contains such special procedures.

- Amends the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.) to require consumer reporting agencies to furnish information to “a government agency authorized to conduct investigations of, or intelligence or counterintelligence activities or analysis related to, international terrorism,” upon receipt of an appropriate certification from that agency.

- Requires the Secretary of the Treasury to issue regulations, within 120 days of the date of enactment, to encour-
age cooperation among financial institutions, financial regulators and law enforcement officials, and to permit the sharing of information by law enforcement and regulatory authorities with such institutions regarding persons reasonably suspected, based on credible evidence, of engaging in terrorist acts or money laundering activities.

- Allows (with notice to the Secretary of the Treasury) the sharing of information among banks involving possible terrorist or money laundering activities.

**Title IV – Protecting the Border**

- For the Canadian border, triples INS-personnel, increases facilities supporting them, and improves monitoring technology.
- Requires DOJ to provide INS and State access to data on visa-applicants' criminal histories.
- Requires Attorney General and the Secretary of State to create identity-confirming technology for aliens, within two years.
- Requires the Attorney General to report to Congress on the feasibility of enhancing the fingerprinting system used for those aliens entering or exiting the U.S.
- Bars admission of aliens who endorsed or espoused terrorist activities, persuaded others to support terrorist activities or terrorist organizations, or are influential members of groups whose public endorsement of terrorism has undermined the U.S. effort to fight terrorism.
- Broadens definition of “engaged in terrorist activity” to include providing material support or encouragement to groups that the individual knew or should have known were terrorist organizations.
- Mandates detention of aliens that the AG certifies as threats to national security, but must charge with criminal or immigration offenses within seven days, in which case detention may continue for six months unless found removable, in which case detention continues until removed or no longer a threat; allows limited judicial review in DC Circuit.
- Gives the Secretary of State discretion to share visa lookout database information and other records on aliens with reciprocating countries.
- Authorizes appropriations for AG’s rapid and full implementation of integrated exit and entry data system for airports, seaports, and land ports of entry.
- Authorizes AG to collect information from flight schools, language schools, and other vocational schools on alien students in the same manner in which AG can collect information on alien students in higher educational institutions.
- Requires SecState to monitor checking of passports and issuing of consular visas.
- Creates special immigrant status for certain aliens, whose relatives have lived in the U.S. before September 11, 2001 and whose same relatives died as a result of a terrorist attack. Neither this status nor any other government benefit shall be conferred to relatives of the terrorists.

**Title V – Removing Obstacles to Investigating Terrorism**

- Authorizes the Attorney General, and broadens the Secretary of State’s authority, to pay rewards to combat terrorism.
- Authorizes officials engaged in FISA surveillance to consult with Federal law enforcement officers to coordinate efforts to investigate or protect against specified threats from a foreign power or an agent of a foreign power, such as an actual or potential attack, sabotage or international terrorism, or clandestine intelligence activities.
- Gives the Secret Service concurrent authority with FBI to investigate cyber-terrorism crimes against government computers.
- Authorizes an Assistant Attorney General to obtain a court order for the purpose of collecting educational records that are relevant to the investigation or prosecution of a grave felony or terrorism.
- Allows FBI Deputy Assistant Director or higher (or Special Agent in Charge) to issue National Security Letters for telephone toll and transaction records, financial records, and consumer reports.

**Title VI – Providing for Victims of Terrorism, Public Safety Officers, and Families**

- Expedites government payments to beneficiaries of public safety workers who were catastrophically injured or killed in connection with the prevention, investigation, rescue, or recovery effort related to a terrorist attack.
- Increases death benefits for such workers’ beneficiaries from $100,000 to $250,000.
- Enlarges the fund for victims of terrorist acts and their beneficiaries. Creates fund to compensate response to September 11, 2001 events.
Title VII – Increased Information Sharing for Critical Infrastructure Protection

- Authorizes $150 million over the next two years for DOJ to establish secure information sharing systems with state and local law enforcement entities to enhance investigation and prosecution of multi-jurisdictional terrorist conspiracies and activities.

Title VIII—Strengthening the Criminal Laws Against Terrorism

- Expands criminal sanctions to include possession of biological agents, toxins, or delivery systems for other than, or of a type or quantity not justified for, peaceful purposes.
- Adds special penalties for criminal possession of biological materials by “restricted persons” defined to include fugitives, illegal aliens, felons, and others.
- Expands definition of domestic terrorism to include “mass destruction” and requires intent to intimidate or coerce civilian populace or to influence government policy or conduct.
- Adds a list of specified crimes to definition of “federal crime of terrorism” in 18 U.S.C. 2332b(g)(5)(B) (which already contains a requirement that the activity “is calculated to influence or affect the conduct of government by intimidation or coercion, or to retaliate against government conduct.”)
- Adds terrorism crimes listed in 18 U.S.C. 2332b(g)(5)(B) as predicates under RICO.
- Makes it a crime to engage in terrorist attacks on mass transportation systems.
- Adds special penalties for harboring or concealing persons known or reasonably believed to be terrorists.
- Expands authority to go against all assets used to support, plan, conduct or conceal acts of domestic or international terrorism.
- Extends statute of limitations to bring indictments in noncapital terrorist offenses (8 years) and capital terrorist offenses (no time limit).
- Increases maximum penalties for terrorism offenses including “for any term of years or for life” in capital cases.
- Provides that parties to a conspiracy to commit certain terrorism offenses may be punished to the same extent as actual perpetrators.
- Defines threshold damages for acts of cyberterrorism as $5000, physical injury, threat to public health or safety, or damage of any kind to a government computer system used in administration of justice, national defense or national security.
- Authorizes $50 million annually to enable the Attorney General to establish regional computer forensic laboratories to assist in defense against cyberterrorism.

Title IX – Improved Intelligence

- Gives DCI explicit authority to establish requirements and priorities for foreign intelligence (FI) collection under FISA and work with the AG to ensure dissemination.
- Requires AG, in consultation with DCI, to develop guidelines to ensure (1) prompt disclosure to the DCI of FI acquired during a criminal investigation and (2) timely notice to DCI of decision whether to commence a criminal investigation based on information provided by the DCI to DOJ regarding possible criminal activity by a current or potential FI source.
- Directs AG and DCI to develop a program to train appropriate federal, state, and local officials to identify FI that may be encountered in the course of their official duties.
- Requires a report from the AG, DCI, and Secretary of Treasury on feasibility and desirability of reconfiguring current foreign asset tracking and control entities so as to improve analysis and dissemination of FI related to terrorist financing.
- Requires a report on the establishment of a virtual translation center within the intelligence community.
- Sense of Congress encouraging intelligence relationships with terrorists.
Title X—Miscellaneous

- Requires the DOJ Inspector General to designate an official to receive complaints alleging abuses of civil rights and liberties by DOJ employees and submit reports to Congress.
- Defines “electronic surveillance” in FISA to exclude the acquisition of computer trespassers’ communications.
- Endeavors to enhance states and local governments' ability to respond to and prevent terrorism through various DOJ grant programs.
- Requires FBI to report to Congress on feasibility of providing airlines with names of passengers who are suspected to be terrorists.
- Enhances statutes making it unlawful to fraudulently solicit charitable contributions.
- Requires determination by Transportation Secretary that licensee poses no security risk before states can issue licenses to transport hazardous materials.
- Establishes National Infrastructure Simulation and Analysis Center in DOD to protect United States’ critical infrastructure from terrorist attacks.

---

**Standing Committee on Law and National Security**

*Chair: Suzanne E. Spaulding*


*Advisory Committee Chair: Richard E. Friedman*

*ABA Board of Governors Liaison: Saul A. Wolfe*

*ABA Law Student Division Liaison: Michael Stransky*

*Staff Director: Holly Stewart McMahon*

740 15th Street, NW
Washington, DC 20005
(202) 662-1035 — FAX (202) 662-1032

*E-mail: natsecurity@abanet.org*

*Web page: http://www.abanet.org/natsecurity*
THE TERRORIST THREAT AT HOME: LEGAL RESPONSES

Editor’s Note: On September 28, 2001, members of the American Bar Association Standing Committee on Law and National Security met in the wake of the greatest terrorist attack in the history of our nation. The Committee has been discussing legal and policy responses to the threat of terrorism, particularly catastrophic terrorism, for many years. The Standing Committee again came together to discuss how we can contribute to the debate that is underway regarding the next steps for responding to this attack and preventing future attacks. A summary of that breakfast meeting follows.

The World Trade Center/Pentagon attack of September 11 emphasizes our great need for homeland security. Members and friends of the ABA Standing Committee on Law and National Security, with years dedicated to addressing the legal responses to terrorism in a domestic context, represent a body of significant expertise. At an exceptional breakfast meeting on September 28 in Washington DC, the Committee sought to harness this valuable resource for the benefit of national policymakers.

Using the breakfast program as an “issue spotting” session, twelve speakers began the two hour program with observations on legal issues to be considered to better prepare the nation against terrorist attacks at home. Additional comments from an audience of experts followed. This report catalogs the set of issues thus identified; we hope it will serve as a first step in assisting the Committee to provide expertise and analysis to policy makers at a time of national crisis.

As one participant aptly observed, “action” responding to the terrorists and their accomplices is a certainty, but in going forward “our decision-makers must never cut the legal process where one exists.” As those best equipped to safeguard that process, lawyers “must not get out of the way at this time, but assert themselves” to achieve legal solutions.

State Sponsorship of Terrorism

Standing Committee Counselor and former Director of Central Intelligence R. James Woolsey began by exploring the possibility of Iraq’s involvement in the 1993 bombing of the World Trade Center. He pointed out that the idea of state sponsored terrorism had been initially raised in one prosecution theory, but never fully explored. A successful prosecution was possible without inquiring into the ultimate perpetrators of the original World Trade Center bombing. Woolsey thus highlighted an important difference between a law enforcement investigation and intelligence collection and analysis. An investigation can be successful without exploring all possible angles of an event while intelligence must go further in order to discover the root causes of an attack such as the original World Trade Center bombing. Because intelligence agencies are not restricted by the evidentiary burdens of proof required for a conviction in a court of law, they may explore a subject more broadly than could a prosecutor. Still, even though there may be no evidentiary burden to consider as intelligence is obtained, if military action is to be taken in response to it, certain questions must be answered. How much proof is necessary to establish state participation in an act of terrorism? To what extent is state sponsorship of terrorism the work of, or disguised as, rival bureaucracies competing within a state? If someone who appears to be the agent of a state is himself culpable, does principal-agency law make the principal per se culpable for the acts of terror committed by the agent? Should Operation Enduring Freedom respond differently to states than it does to non-state actors, such as al-Qaeda or the Taliban?

Authority of Law Enforcement and Intelligence

Christine Healey, Senior Counsel, the House Permanent Select Committee on Intelligence, briefed the Committee on the Administration’s bill, drafted and being considered with unparalleled speed. Already consensus on a number of the proposals is apparent, but disagreements among congressional representatives and executive branch officials on other proposals is likely to ensure a second round of legislative activity. Among the less controversial issues: a requirement that the DCI revise regulations on the recruitment of operatives with histories of violence. More controversial: an expansion of the president’s foreign intelligence collection authority under the Foreign Intelligence Surveillance Act, and an increase in the amount of time for alien-detentions. Healey added that lawmakers have proposed the establishment of an independent commission, comprised of “outsiders,” to assess the roles and performance of those government agencies responsible for preventing the attacks of September 11. While some question whether energy should be exerted on another commission, supporters see the commission’s work as important for public understanding of the attack and the continuing threat.
John Elliff, now of the Senate Judiciary Committee, formerly with the Senate Intelligence Committee, discussed the bill proposed by Senator Pat Leahy (D-VT). Elliff predicted that the ultimate bill will be passed by consensus, not just a majority. Accordingly, plans are now underway to introduce one bill acceptable to all, which would draw upon the provisions of all of the existing and proposed legislation. As an example of one of the more difficult issues, concerns have been raised by the “Internet privacy community” about allowing government investigations to follow hyperlinks through a computer address or cookie. What level of Fourth Amendment protection does such surveillance merit? Is it similar to a “trap and trace” in law enforcement where a certification of relevance to an investigation is sufficient, or is such activity more similar to intrusive surveillance of content requiring a judicial warrant or court order based on probable cause? If Congress remains uncertain about issues such as these, some have suggested that they be subject to a “sunset provision,” thus expiring after a fixed period. But, Elliff asked, are sunset laws appropriate in this context and how have they been used in the past with respect to law enforcement and intelligence?

Several commentators subsequently endorsed the concern that civil liberties be protected, especially in the wake of a serious security crisis. They commented favorably on the Department of Justice’s recently created Commission on Arab American Civil Rights, stressing that the government must be especially mindful of the civil liberties of this group of Americans at this time.

Frederick Manget, Deputy General Counsel, CIA, noted that the current legislative proposals have been rapidly assembled. Others may be required and introduced subsequently in a criminal prosecution. He noted the difficulty of identifying undifferentiated intelligence, and then making it useful as admissible evidence. Manget also addressed the limitations on the investigative powers of the FBI and CIA as well as the ability to exchange information between them. One Administration proposal would eliminate restrictions in Title III and Rule 6(e) which currently prevent regular sharing of FBI evidence with the intelligence community. Manget noted other efforts to allow the law enforcement and intelligence communities to work more closely together. One change proposed would alter the requirement that surveillance under FISA be undertaken for “the” purpose of intelligence collection, as opposed to the law enforcement purposes. The proposal would allow the use of FISA even if intelligence collection was only “a” purpose. Others commented later on the importance of continuing the separation between law enforcement and intelligence information, authorities and missions.

Finally, Manget suggested that Congress might be required to review how the government conducts covert relations with certain states, particularly states under economic sanctions.

Some from within the Administration suggested that the legislative proposals currently under consideration may only attack the problem of finding and prosecuting terrorists “at the margins.” Others noted that even marginal expansions of law enforcement authority for intelligence collection purposes will create a “slippery slope” effect. They claimed that FISA provides law enforcement with all the authority it needs, that expanding Title III serves little purpose in the fight against national security threats, and that, in fact, “the law is not the problem.”

**Government Resources**

While the scope of law enforcement and intelligence community’s authority must continue to be debated, several commented forcefully that the most important question was that of inadequate analytic and related resources at the FBI. M.E. “Spike” Bowman, Deputy General Counsel for Intelligence, FBI, reported a significant lack of both analysts and translators. Finally, how the FBI utilizes novel acquisition structures raises an even larger question of how efficient the federal government’s procurement process is in times of crisis.

Gary Milhollin, Director of the Wisconsin Project on Nuclear Arms Control, reinforced the theme that governmental institutions must be “bigger and better” if they are to be effective with their responsibility for critical infrastructure protection. Addressing this need, others advocated additional funds for the Immigration and Naturalization Service, which cannot adequately analyze and prepare to prevent the illegal entrance or presence of those connected to terrorist acts.

**Trade vs. Security**

Highlighting the tension between trade and security, Milhollin next criticized the proposed Export Administration Act, which would decontrol U.S. exports that could help countries with weapons of mass destruction. Milhollin also ques-
tioned how the U.S. ought to respond to a weapon of mass destruction attack. He also explained that while globalization has diminished the importance of national boundaries, national governments remain the sole protectorates of security within those borders. While national governments are armed with military and police forces, so is NATO. But are multilateral institutions, such as NATO, adequate and appropriate protectorates of security? Milhollin urged lawmakers to tighten controls on what technology leaves the country, and also focus more closely on what comes into the country. He concluded that it is not within the country's power to watch all goods and all persons that come into it; still a much better job could be done.

The tension between prosperity and security also underscores the policymaking debates regarding money laundering, according to Stephen Kroll, former Chief Counsel, Department of Treasury, FINCEN. Kroll stated that money is "the terrorists' oxygen," but noted that tracing the several million dollars (if that much) used to finance the crimes of September 11 in the midst of a trillion dollars exchanged daily is like "finding the atom on the needle in the haystack." That trillion-dollar cash flow reflects the dropping of global barriers to free capital movements that has been part of the base of our prosperity. Later a member of the audience questioned the scope of the Treasury Department's discretion to seize assets of persons "engaged in hostilities."

Federal Control

September 11 also tested public health and emergency systems, which face even more daunting challenges to anticipate, protect, and control biological and chemical threats. Gene Matthews, Legal Advisor to the Centers for Disease Control, provided a primer on public health law, noting first that it falls under the "police powers" and thus is within the province of the several states. Matthews commented on the need to review state emergency health laws, some of which have not been updated since the 1930's. In addition, critical attention must be directed toward striking the appropriate balance between governmental duty and individual rights with respect to the use of emergency public health powers to obtain disease information, control access to property, or examine persons. Similarly, others championed federal coordination of state public health and emergency systems. Professor Vincent Brannigan, University of Maryland, Department of Fire Protection Engineering, urged federal coordination and increased research on building safety systems.

The appointment of Governor Tom Ridge as head of the Office of Homeland Security raised an additional set of questions. How will this agency be structured? How will it coordinate existing agency responsibilities and other policies and programs within the Executive Office of the President, such as those tasked to the Office of Cyber Security? Senior Counsel to the President’s Commission on Critical Infrastructure Protection, Lee Zeichner, then asked a central question, "what is critical in infrastructure and how should the nation construct an overarching legal and policy framework to manage critical infrastructure services, most of which are provided by industry and state/local governments?" He urged Congress to review the Stafford Act and other significant authorities, such as the Defense Production Act and the Communications Act of 1934 in order to modernize and align such laws with today's critical infrastructure needs, including, but not limited to, the Internet, energy, financial services, transportation, and water. Contained within this recommendation is the assumption that there must be more reporting and information sharing between the public and private sectors, but without new regulatory regimes, which consistently fail to generate near real-time and robust sharing of relevant information. As a related concern, the disclosure of information on the Internet has the potential to pose a security risk to a number of traditional or average governmental functions. For example, a successful FOIA release might be instantly posted on the Internet for mass viewing. Zeichner concluded urging that our methods of national risk assessment be updated. Finally, he suggested that the government should consider developing a reinsurance facility and act as the insurer of last resort for significant damages resulting from a terrorist attack.

As the federal government places more controls on certain industries, such as the airlines, additional legal questions arise with respect to security. If federal employees search bags in airports, must they be cleared? And should they continue to be "re-employed annuitants?" Elliff responded that the government should take advantage of an "army" of retired federal agents to conduct such clearance investigations. The question was not one of their competence and professionalism, but rather of quality controls for such investigations. Moreover, the standards for gaining a security clearance, established early during the Cold War, should also be examined.
Effecting Justice

Several participants wondered whether and when the current law enforcement phase will terminate, or give way, to a military phase in the “war” on terrorism. The answer provided was that both must go forward simultaneously. The former should not stop for the latter, but a “two-pronged attack” should go forward. Attention then turned to the possible capture of a principal terrorist. What would happen next? One participant suggested that a military commission might be used to try terrorists. Building on that suggestion, Manget wondered whether terrorist acts could be considered “war crimes.” Others urged that our national response to terrorism focus on diplomacy because the current conflict is one of ideas.

Judith Miller, former General Counsel to the Department of Defense, recommended more “red teaming,” preferably a multi-agency team devoted full-time to anticipating where and how terrorists might strike, using intelligence and other sources to get “inside their heads,” as well as running practice exercises to highlight and correct vulnerabilities. Endorsing Miller’s recommendation, another member of the audience reminded us that we should avoid focusing on how to fight the last war and consider instead how to fight the next one. Agreeing, Elizabeth Rindskopf Parker, former General Counsel to the CIA and NSA and past Standing Committee Chair, observed that such red teaming is used effectively within the military community but is largely absent from domestic agencies.

Conclusion

The President has urged the nation to be patient. Elizabeth Rindskopf Parker predicted in her concluding remarks that answers to many of these questions will not surface for at least another year. The Committee’s new Chair, Suzanne E. Spaulding, ended the session expressing the hope that this unique breakfast session would serve as a springboard for productive efforts by Committee members and friends that could assist decision makers and the American public to address issues of law and national security raised by the recent terrorist attacks.