Hearing on the USA PATRIOT Act

Committee on the Judiciary

United States Senate

Tuesday, September 22, 2009

Testimony
of
Suzanne E. Spaulding, Esq.

Subcommittee on the Constitution, Civil Rights, and Civil Liberties

Judiciary Committee

United States House of Representatives

Hearing on the USA PATRIOT Act

Tuesday, September 22, 2009

Testimony
of
Suzanne E. Spaulding, Esq.

Chairman Nadler, Ranking Member Sensenbrenner, and members of the Committee, thank you for inviting me to participate in today's hearing on the USA PATRIOT Act and related provisions. Four years ago, I testified in Congress, including in front of the House Judiciary Committee, regarding the provisions of the PATRIOT Act that were designated to sunset in 2005. A number of the concerns with the original language in the Act were addressed in the Reauthorization Act of 2006. However, some remain, particularly some of the overarching issues, and some were compounded in subsequent legislation.

As I attempt to address these issues this morning, I am mindful that we recently marked another anniversary of the attacks of September 11, 2001. This indelible manifestation of the terrorist threat continues to fuel our determination to ensure that those in our government who work so tirelessly to protect us from another attack have the tools they need and that we are not undermining their efforts by failing to consider strategic as well as tactical objectives. In the eight years since 9/11, we have learned a great deal about the nature of the terrorist threat and the best ways to combat it. Armed with that wisdom, and with determination rather than fear, it is appropriate--and important for our national security-- that we continue to reexamine our response.

We have to demonstrate that we still believe what our founders understood; that respect for civil liberties is not a luxury of peace and tranquility. Instead, in a time of great peril, it was seen as the best hope for keeping this nation strong and resilient. The men who signed the Constitution and those who developed the Bill of Rights were not fuzzy-headed idealists but individuals who had fought a war and knew that they faced an uncertain and dangerous time. Respect for the Constitution and careful efforts to ensure that our laws protect the rights enshrined therein are a source of strength and can be a powerful antidote to the twisted lure of the terrorist's narrative. In fact, after spending nearly 20 years working terrorism issues for the government, I am convinced that this approach is essential to defeating the terrorist threat.

With this understanding of the national security imperative, I support this committee's intention not to limit its review to those few provisions that are scheduled to sunset. Instead, Congress should use this opportunity to examine ways to improve other domestic intelligence laws as well, such as the various provisions for national security letters. As I have urged before, Congress should undertake a comprehensive review of domestic intelligence activities, and I would encourage the Administration to do the same.

The legal framework for domestic intelligence has come to resemble a Rube Goldberg contraption rather than the coherent foundation we expect and need from our laws. The rules that govern domestic intelligence collection are scattered throughout the US Code and in a multitude of internal agency policies, guidelines, and directives, developed piecemeal over time, often adopted quickly in response to scandal or crisis and sometimes in secret. They do not always reflect a firm understanding of why intelligence collection needs to be treated differently than law enforcement investigations, the unique intelligence requirements for homeland security, the impact of dramatic changes in technology, and the degree to which respect for civil liberties, fundamental fairness, and the rule of law is essential to winning the battle for hearts and minds--and, therefore, essential to our homeland security.

The various authorities for gathering information inside the United States, including the authorities in FISA, need to be considered and understood in relation to each other, not in isolation. For example, Congress needs to understand how FISA surveillance authority relates to current authorities for obtaining or reviewing records, such as national security letters, Section 215, the physical search and pen register/trap and trace authorities in FISA, and the counterparts to these in the criminal context, as well as other law enforcement tools such as grand juries and material witness statutes.[1]

Executive Order 12333, echoed in FISA, calls for using the "least intrusive collection techniques feasible." The appropriateness of using electronic surveillance or other intrusive techniques to gather the communications of Americans should be considered in light of other, less intrusive techniques that might be available to establish, for example, whether a phone number belongs to a suspected terrorist or the pizza delivery shop. Electronic surveillance is not the "all or nothing" proposition often portrayed in some of the debates.

In addition, President Obama has already committed to asking his Attorney General to conduct a comprehensive review of domestic surveillance. If that review is not already underway, Congress should encourage its initiation. The IG Report on the Terrorist Surveillance Program clearly indicated that there were programs beyond its scope. These need to be examined and a report made to Congress and, to the maximum extent possible, to the public.

I understand that today's hearing, however, is particularly focused on the provisions that will sunset at the end of this year, so the balance of my testimony will address those.

---

[1] See, for example, the May 2008 OIG Report on Section 215, which cites concerns about the FBI's use of NSLs to get information "after the FISA Court, citing First Amendment concerns, had twice declined to sign Section 215 orders in the same investigation." The IG questioned the appropriateness of this "because NSLs have the same First Amendment caveat as Section 215 requests and the FBI issued the NSLs based on the same factual predicate, without further reviewing the underlying investigation to ensure that it was not premised solely on protected First Amendment conduct." OIG Report at 5.

Distinguishing between domestic intelligence operations and criminal law enforcement investigations

Sections 215 and 206 of the PATRIOT Act, like most domestic intelligence authorities, both have corollaries in the criminal context. This was often cited as justification for providing for these authorities in the intelligence context: "if we can do these kinds of things when investigating drug dealers, certainly we should have this authority for intelligence operations against terrorists." It's a compelling argument. But sometimes important elements get lost in the translation from the criminal to intelligence realm.

Intelligence operations are often *wide-ranging* rather than specifically focused—creating a greater likelihood that they will include information about ordinary, law-abiding citizens; they are conducted in *secret*, which means abuses and mistakes may never be uncovered; and they *lack safeguards* against abuse that are present in the criminal context where inappropriate behavior by the government could jeopardize a prosecution. These differences between intelligence and law enforcement help explain this nation's long-standing discomfort with the idea of a domestic intelligence agency.

Because the safeguards against overreaching or abuse are weaker in intelligence operations than they are in criminal investigations, powers granted for intelligence investigations should be no broader or more inclusive than is absolutely necessary to meet the national security imperative and should be accompanied by rigorous oversight within the executive branch, by Congress and, where appropriate, in the courts.

Unfortunately, this essential caution was often ignored in the FISA amendments contained in the PATRIOT Act. The authority actually became *broader* as it moved into the intelligence context and oversight was not always accordingly enhanced.

Section 206: Roving Wiretaps

Section 206 was intended to bring the roving wiretap authority that is available in criminal investigations into the realm of intelligence surveillance under FISA. This was an essential update but some important safeguards in the criminal provisions were lost in the transition.

In a criminal investigation, under Title III, roving wiretap applications must definitively identify the target of the surveillance. FISA roving wiretaps need only provide "a description of the target" if the identity is not known. This less rigorous standard increases the prospect that the government may wind up mistakenly intercepting communications of innocent persons.

In addition, Title III permits surveillance only when it is reasonable to assume that the suspect is "reasonably proximate" to the instrument that is being tapped--and only one instrument can be tapped at a time. This requirement, like the requirement to identify the target, was designed to reduce the likelihood that communications of innocent persons would be intercepted. This requirement is not in section 206.

Title III also differs from the FISA roving wiretap in requiring that the target be notified of the surveillance, generally 90 days after the surveillance ends. This notice requirement is understandably absent in the intelligence context but so, too, is the safeguard that notice provides as a mechanism to deter and detect mistakes or abuses.

Deterrence is also weakened in the intelligence context because prosecution is usually not the goal. In the criminal context, where the focus is on successful prosecution, the exclusionary rule serves an essential function, one that is largely absent in intelligence operations. As the Supreme Court explained in *Terry v. Ohio*, 392 U.S. 1 (1968):

> Ever since its inception, the rule excluding evidence seized in violation of the Fourth Amendment has been recognized as a principal mode of discouraging

> lawless police conduct. *See Weeks v. United States*, 232 U.S. 383, 391-393 (1914). Thus, its major thrust is a deterrent one, *see Linkletter v. Walker*, 381 U.S. 618, 629-635 (1965), and experience has taught that it is the only effective deterrent to police misconduct in the criminal context, and that, without it, the constitutional guarantee against unreasonable searches and seizures would be a mere "form of words." *Mapp v. Ohio*, 367 U.S. 643, 655 (1961).
>
> …
>
> Regardless of how effective the rule may be where obtaining convictions is an important objective of the police, it is powerless to deter invasions of constitutionally guaranteed rights where the police either have no interest in prosecuting or are willing to forgo successful prosecution in the interest of serving some other goal.

Combine this with a statutory standard that is less rigorous than the criminal standard, both as regards the identity of the target and the proximity to the instrument, and you compound the risk of mistake or abuse. This highlights the care that must be taken when importing criminal authorities into the intelligence context, and why it may be necessary to include more rigorous standards and/or other safeguards.

For example, Congress should consider tightening the language to require the judge to determine that the target has been described with sufficient particularity to distinguish him or her from other potential users of the instrument or facility being surveilled.

Similarly, while it is possible that the proximity requirement is somehow included in the minimization procedures that are called for in section 206, Congress may want to consider explicitly including this requirement in the statute, as it is in Title III.

Finally, perhaps the FISA judge should have the discretion to impose a time limit on the lack of notice, giving the government an opportunity to argue for an extension if circumstances warrant it.

Section 215: Tangible Things Orders

Section 215 of FISA also imported into the intelligence realm authority similar to that traditionally exercised in criminal investigations, in this case attempting to mimic the use of grand jury or administrative subpoenas.

However, the criminal investigative tools require some criminal nexus. Not necessarily that a crime has already been committed, but that the activity that is being investigated would violate a criminal statute. Under our constitution, criminal activity must be well defined so that individuals are clearly on notice with regard to whether their actions may violate the law and thus invite government scrutiny.

When the authority moved into the intelligence context, however, the requirement for a criminal nexus was dropped. Instead, section 215 orders require only that the information demanded by the government is "relevant to an authorized investigation (other than a threat assessment) … to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities"

Consider this language. It does not say "an investigation into international terrorism activities"—which would at least mean there was some specific international terrorism activity being investigated. Instead, it says "an investigation *to protect against* international terrorism." This very broad language may or may not involve criminal activity and provides potentially far greater flexibility than criminal subpoenas. Again, this may be appropriate for the wide-ranging nature of intelligence collection-- but it also provides greater opportunity for abuse and mistakes. Amending the language to read "an investigation of international terrorism activities" should meet the national security imperative and provide better protection for innocent persons.

The Reauthorization Act of 2006 attempted to address this concern by adding a provision that the things being sought are "presumptively relevant to an authorized investigation if the applicant shows in the statement of the facts that they pertain to **(i)** a foreign power or an agent of a foreign power; **(ii)** the activities of a suspected agent of a

foreign power who is the subject of such authorized investigation; or **(iii)** an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigation."[2]

The impact of this added language is not entirely clear. First, the third category, which includes anyone "known to" a suspected agent of a foreign power, is extremely broad and clearly could include completely innocent Americans. David Kris and Doug Wilson cite the example of the bank records of a grade-school teacher of the child of a suspected agent of a foreign power.[3] But it could also apply to your daughter's diary if she is in that child's class and known to the parent.

Moreover, this provision does not preclude the issuance of orders pursuant to facts that do not fall within any of these three categories. In other words, this language, by creating a presumption rather than a requirement, does not restrict the extremely broad scope of the term "relevant to" an investigation.

The weak safeguard provided by the "presumptively relevant" language also stems from the context in which Section 215 orders are considered. Creating a "presumption" generally implies a shift in the burden of proof from one party to another in an adversarial proceeding. Section 215 orders are considered in an ex parte proceeding, not in an adversarial context. Once served, an order can be challenged by the recipient but, if served on a third-party record holder, there is very little incentive for that record holder to challenge the order. In fact, the letter from the Department of Justice concedes that "no recipient of a FISA business records order has ever challenged the validity of the order." These record holders cannot be considered as fully representing the interests of the individual whose records are being sought.

---

[2] 50 USC 1861(b)(2).

[3] *National Security Investigations & Prosecutions*, David S. Kris and J. Douglas Wilson, Thomson West (2007) at 18:3.

Congress should consider changing the language to remove the presumption and make it clear that the tangible things being sought must be relevant to an authorized investigation *and* fall into one of these three categories.

The Reauthorization Act also added a requirement that the Section 215 application include "*a statement of facts* showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation." (Emphasis added.) The requirement to provide facts to back up the government's assertion was an improvement over the PATRIOT Act language, but pre-PATRIOT Act language in this section required the government to provide "specific and articulable facts." This is the standard normally used[4] and should be restored. The "specific and articulable" language may have been dropped in a mistaken belief that Section 215 does not implicate Fourth Amendment or other constitutional concerns. While this argument may have carried weight before the PATRIOT Act changes, it is certainly not valid today.

Section 215 as originally adopted by Congress in 1998 applied only to "records" from "a common carrier, public accommodation facility, physical storage facility or vehicle rental facility." This was properly entitled the "Business Records" provision. The PATRIOT Act amendments now allow the orders to be issued to obtain "any tangible things" from any person. This could include your personal notes, your daughter's diary, or your computer.

Congress should change the title of this provision to "Access to tangible things," to more accurately reflect the broad scope of items now susceptible to such orders. It is certainly not limited to 3rd party records, for example. Thus, even if you accept as still valid the "3rd-party-record rule," a premise that needs serious re-evaluation in light of data aggregation/data mining technology, this section would still include things to which the Fourth Amendment clearly applies. Moreover, as the OIG Report concluded, Section 215

[4] See, e.g., *Terry v. Ohio*, 392 U.S. 1 (1968).

orders can also raise issues related to the Fifth and First Amendments. (See IG Report at 81.)

Finally, Section 215 also puts the burden on the recipient of order to challenge a gag order before the government even has to certify that there would be any harm from disclosure. Congress should consider requiring the government to set forth in the initial application the grounds upon which it believes disclosure will be harmful.[5] And the one-year time frame should apply to the duration of all gag orders, perhaps with the FISA judge having discretion to impose a shorter time frame, renewable indefinitely.

Lone Wolf

Four years ago I urged Congress to let the Lone Wolf provision sunset. I reiterate that plea today.

The Foreign Intelligence Surveillance Act (FISA) is an extremely important and extraordinary national security tool whose policy and constitutional justification is needlessly undermined by the Lone Wolf provision. The Administration's admission that they have never once used the authority seems to provide compelling evidence that it was not needed and is not an essential counterterrorism tool.

The common wisdom "if it ain't broke, don't fix it" was ignored when Congress enacted the "Lone Wolf" amendment to the Foreign Intelligence Surveillance Act (FISA), allowing its use against an individual acting totally alone, with no connection to any foreign power, so long as they are "engaged in international terrorism or activities in preparation therefor." Although the Lone Wolf provision is often referred to as the "Moussaoui fix," in fact, no "fix" was needed in the Moussaui case because it was not FISA's requirements that prevented the FBI from gaining access to his computer back in August of 2001. The problem was a misunderstanding of FISA. This conclusion is

[5] This would be consistent with the federal court decision that found national security letter gag orders that do not require the government to initiate judicial review of the order or provide facts to support its assertions of harm to be an unconstitutional infringement of the First Amendment. *Doe v. Muksasey*, 549 f3d 861 (2d cir. 2008).

supported by the findings of the Joint Congressional Intelligence Committee Inquiry into the 9/11 Attacks, an exhaustive Senate Judiciary Committee inquiry, and the 9/11 Commission.

In order to obtain a FISA order authorizing access to Moussaoui's computer, the FBI needed to show probable cause to believe that Moussaoui was acting "for or on behalf of a foreign power." A foreign power is defined to include a group engaged in international terrorism. There is no requirement that it be a "recognized" terrorist organization. Two people can be "a group engaged in international terrorism." (See *FBI Oversight in the 107th Congress by the Senate Judiciary Committee: FISA Implementation Failures, An Interim Report* by Senators Patrick Leahy, Charles Grassley, & Arlen Specter (February 2003) at p. 17.)

Moreover, the government does not have to "prove" the target's connection to a terrorist group. They must merely meet the "probable cause" standard, which, as the Judiciary Committee Report points out, does not mean "more likely than not" or "an over 51% chance," but "only the probability and not a prima facie showing." The Report concluded that "there appears to have been sufficient evidence in the possession of the FBI which satisfied the FISA requirements for the Moussaoui application" (p. 23). Thus, no "fix" was required to search Moussaoui's computer.

Even if the FBI had not been able to meet the relatively low "probable cause" standard for showing that Moussaoui was working with at least one other person, the FBI could very likely have obtained a criminal warrant to search Moussaoui's computer. They did not pursue that because they were concerned that doing so would preclude them from getting a FISA warrant later if they were turned down for the criminal warrant or ultimately did develop what they thought was sufficient information linking him to a terrorist group. This concern was based on the "primary purpose" test—viewed as precluding the use of FISA if the primary purpose was criminal prosecution rather than intelligence collection—which was subsequently changed in the USA PATRIOT Act. Now

that this "primary purpose" test has been eliminated, and particularly in light of a subsequent opinion by the Foreign Intelligence Surveillance Court of Review, this would no longer be a concern and the government today could seek a criminal warrant without concern of precluding future use of FISA.

The Department of Justice in its letter to the Congress last week stated that this Lone Wolf authority had never been used but argued that we should keep it in FISA just in case. The problem with this reasoning is that it comes at a high cost. In addition to being unnecessary, the Lone Wolf provision—by extending FISA's application to an individual acting entirely on their own-- undermines the policy and constitutional justification for the entire FISA statute.

When Congress enacted FISA, according to the Senate Report, it carefully limited its application in order "to ensure that the procedures established in [FISA] are reasonable in relation to legitimate foreign counterintelligence requirements and the protected rights of individuals. Their reasonableness depends, in part, upon an assessment of the difficulties of investigating activities planned, directed, and supported from abroad ***by foreign intelligence services and foreign-based terrorist groups***." Senate Report 95-701, at 14-15 (emphasis added).

The Congressional debate, and the court cases that informed and followed it, clearly reflect the sense that this limited and extraordinary exception from the normal criminal warrant requirements was justified only when dealing with foreign powers or their agents. In 2002, the FISA Court of Review (FISCR) cited the statute's purpose, "to protect the nation against terrorists and espionage threats directed by foreign powers," to conclude that FISA searches, while not clearly meeting "minimum Fourth Amendment warrant standards," are nevertheless reasonable.[6] In its more recent case upholding the constitutionality of the Protect America Act *as applied*, the FISC again relied upon the

[6] *In re Sealed Case*, 310 F.3rd 717 (Foreign Intel. Surv. Ct. Rev. 2002).

government's decision to apply the authority only to *foreign powers or agents of foreign powers* reasonably believed to be outside the US.[7]

Individuals acting entirely on their own simply do not implicate the level of foreign and military affairs that courts have found justify the use of this extraordinary foreign intelligence tool. The FISA exception to the Fourth Amendment warrant standards was not based simply on a foreign nexus; it did not apply to every non-US person whose potentially dangerous activity transcended US borders. It was specifically limited to activities involving foreign powers.

The requirement that the Lone Wolf must be "engaged in international terrorism or acts in preparation therefore" does not solve this problem. Nowhere in FISA's definition of "international terrorism" is there any requirement for a connection to a foreign government or terrorist group. The definition of international terrorism merely requires a violent act intended to intimidate a civilian population or government that occurs totally outside the United States, or transcends national boundaries in terms of the means by which it is accomplished, the persons it appears intended to coerce or intimidate, or the locale in which the perpetrators operate or seek asylum. This would cover an individual inside the US who buys a gun from Mexico (in what would be an unusual reversal of the normal directional flow of guns) to threaten a teacher in a misguided attempt to get the government to change its policies on mandatory testing in schools.

Nor should we rely upon FISA judges to ensure that an overly broad standard is only applied in ways that are sensible, since the law makes clear that they must approve an application if the standards set forth in the statute are met.

[7] *In re Directives [redacted text] Pursuant to Section 105B of the Foreign Intelligence Surveillance Act*, No. 08-1, August 22, 2008.

While the Administration admits to never having used this provision, and concedes that they cannot determine "whether any of the targets will so completely lack connections to groups that they cannot be accommodated under other definitions," the letter from the Department of Justice offers a couple of hypotheticals to justify the "just in case" argument. Keep in mind, however, that even if FISA surveillance and secret search authority were not available, the government can still investigate and, at least in the case of the "known" terrorist, make an arrest. For example, the government can find out all the people with whom each of those individuals is communicating, get their credit card information to see where they are at various times through the day and what transactions they engage in, and put them under physical surveillance. Finally, if there is an urgent need to conduct electronic surveillance before any indicia can be gathered that the person is working with someone else, Title III is a viable option.

If the government can make a compelling case that these investigative tools are inadequate, Congress could consider allowing the government to use authorities in FISA other than the most intrusive authorities of electronic surveillance and physical search to investigate a suspected Lone Wolf. In this way, the government could use Section 215 (and pen register/trap & trace authority, which does not require that the target is an agent of a foreign power), with the attendant secrecy, in order to gather indicia that at least one other person is involved--at which point the electronic surveillance and physical search authorities would be available.

Congress should let the terrorism Lone Wolf provision sunset. By defining an individual acting totally alone, with no connection to any other individual, group, or government, as "an agent of a foreign power," Congress adopted the logic of Humpty Dumpty, who declared: "When I use a word, it means just what I choose it to mean." Unfortunately, this legislative legerdemain stretched the logic of this important statutory tool to a point that threatens its legitimacy. If its use against a true Lone Wolf is ever challenged in court, FISA, too, may have a great fall.

Expansion of Lone Wolf

Unfortunately, instead of repealing or fixing the Lone Wolf provision, Congress expanded it. The FISA Amendments Act enacted last year added to the "agent of a foreign power" definition a non-US person "engaged in the international proliferation of weapons of mass destruction." This not only repeats the error of targeting an individual acting alone, it compounds the concern by removing any requirement that the activity constitute a crime.

The definition of "international terrorism" at least includes a requirement that the activity "involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State." As noted in the discussion above regarding Sections 206 and 215, the requirement for a criminal predicate is significant because, in our system, individuals are held to be on notice, through the careful definitions in the criminal code, of when they are engaging in criminal activity and thereby risking government intrusion, such as electronic surveillance of their communications.

"International proliferation of weapons of mass destruction" is not defined in FISA. Instead, the amendments included a definition of "weapons of mass destruction." The activity that puts an individual at risk of government surveillance, however, is "proliferation" of those weapons. The innocent, unwitting sale of dual-use goods to a foreign front company could be considered proliferation. If so, a non-US person working for an American company who is involved in completely legal sales of such dual-use goods could have all of their communications monitored and their home secretly searched by the US government.

I served as the Legal Adviser for the intelligence community's Nonproliferation Center and as Executive Director of a Congressionally-created WMD commission, so I fully understand the imperative to stop the spread of these dangerous technologies.

However, there are many tools available to investigate these activities without permitting the most intrusive technique--listening to phone calls, reading emails, and secret physical searches--to be used against people who are unwittingly involved and whose activities are legal. This overly broad extension of FISA raises significant constitutional issues.

Congress should add a "knowing" requirement, just as there is for aiding and abeting clandestine intelligence activities. Alternatively, Congress should define "proliferation" to include only activity that would constitute a crime.

Conclusion

Let me close by commending the committee for its commitment to ensuring that the government has all appropriate and necessary tools at its disposal in this vitally important effort to counter today's threats and that these authorities are crafted and implemented in a way that meet our strategic goals as well as tactical needs. With a new Administration that provokes less fear of the misuse of authority, it may be tempting to be less insistent upon statutory safeguards. On the contrary, this is precisely the time to seize the opportunity to work with the Administration to institutionalize appropriate safeguards in ways that will mitigate the prospect for abuse by future Administrations, or even this Administration in the wake of some event.

Thank you.

Suzanne E. Spaulding

6506 W. Langley Lane, McLean, VA 22101

Summary: *Suzanne Spaulding has spent nearly 25 years working national security issues at both ends of Pennsylvania Avenue, on both sides of the Capitol, on both sides of the aisle, and now in the private sector. She has run national commissions on terrorism and WMD, serves on numerous academic and professional advisory panels, and is a frequent commentator in publications, media, and before Congress.*

Before joining the private sector, Ms. Spaulding was Democratic Staff Director for the U.S. House of Representatives Permanent Select Committee on Intelligence. She had started working on terrorism and other national security issues 20 years earlier, in 1983, as Senior Counsel, and later Legislative Director, for Senator Arlen Specter (R-PA). After six years at the Central Intelligence Agency, where she was Assistant General Counsel and the Legal Adviser to the Director of Central Intelligence's Nonproliferation Center, she returned to the Hill as General Counsel for the Senate Select Committee on Intelligence.

She served as the Executive Director of two Congressionally-mandated commissions: the *National Commission on Terrorism*, chaired by Ambassador L. Paul Bremer III, and the *Commission to Assess the Organization of the Federal Government to Combat the Proliferation of Weapons of Mass Destruction*, chaired by former Deputy Secretary of Defense and CIA Director John Deutch, advised both the *Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction* ("Gilmore Commission") and President George W. Bush's *Commission on the Intelligence of the United States Regarding Weapons of Mass Destruction* ("Robb/Silberman Commission"). She is currently a member of the CSIS **Commission** *on* **Cyber Security** *for the 44th Presidency*.

In 2002, she was appointed by then-Virginia Governor Mark Warner to the *Secure Commonwealth Panel*, established after the attacks of September 11 to advise the Governor and the legislature regarding preparedness and response issues in the Commonwealth of Virginia.

Ms. Spaulding is on the Board of Directors of the Association of Former Intelligence Officers, the Steering Committee of the *Transnational Threats Initiative* of the Center for Strategic and International Studies (CSIS), the Steering Committee of the *Critical Incident Analysis Group* (CIAG), and is a member of the *Liberty and Security Initiative* of the Constitution Project**.** She also served on the Advisory Board of the Harvard Law School/Belfer Center *Long Term Strategy Project on Preserving Security and Democratic Freedoms in the War on Terrorism*. She is a past Chair of the American Bar Association's *Standing Committee on Law and National Security*. Ms. Spaulding also is a member of the ABA President's Task Forces on Enemy Combatants and Domestic Surveillance and served on the ABA Working Group on CFIUS Reform.

In addition, she has chaired, convened, and served on numerous other task forces, working groups, and conferences on a wide range of national security topics, is a frequent writer and lecturer, and has been quoted regularly in media outlets around the country and internationally. She was profiled in National Journal's *Homeland Security 100* (February 2004). Ms. Spaulding is often called upon to testify as an expert in front of Congress.

Suzanne Spaulding is currently a Principal in *Bingham Consulting Group* and Of Counsel to *Bingham McCutchen*, where she advises clients on issues related to national security. She received her undergraduate and law degrees from the University of Virginia.

Clearance: Top Secret/SCI

Congressional Testimony includes:

"Cyber Security and the Role of the Intelligence Community," US House Permanent Select Committee on Intelligence, September 18, 2008

"Domestic Spying: Insights for a New Administration," U.S. Senate Committee on the Judiciary, Subcommittee on the Constitution, September 16, 2008

"Moving from Plans to Action: The Imperative for Implementing Intelligence Reform," U. S. House Permanent Select Committee on Intelligence, Subcommittee on Intelligence Community Management, December 5, 2007

"Strengthening FISA: Does the Protect America Act Protect Americans' Civil Liberties and Enhance Security?", U.S. Senate Committee on the Judiciary, September 25, 2007

"Foreign Intelligence Surveillance Act," U.S. House Committee on the Judiciary, September 5, 2007

"Over-Classification and Pseudo-Classification: Making DHS the Gold Standard for Designating Classified and Sensitive Homeland Security Information," U.S. House of Representatives Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment, June 28, 2007

"Responding to The Inspector General's Findings of Improper Use of National Security Letters by the FBI," U.S. Senate Committee on the Judiciary, Subcommittee on the Constitution, April 11, 2007

"USA PATRIOT Act and the Legal Framework for Combating International Terrorism," U.S. Senate Committee on the Judiciary, May 10, 2005

"Implementation of the USA PATRIOT Act and the Lone Wolf Provision," U.S. House of Representatives Committee on the Judiciary, Subcommittee on Crime, Terrorism, and Homeland Security, April 26, 2005

Publications include:

Stuck in a September 12 Mindset, The Guardian, September 11 2008;

Power Play, Washington Post Outlook, December 25, 2005;

"Intelligence Reform", Chapter in Ideas for America's Future, by Jefferey Bialos, Suzanne E. Spaulding contributor, 2008;

"Building Checks and Balances for National Security Policy: The Role of Congress", Advance, American Constitution Society for Law and Policy, Vol.2, No.2, Fall 2008;

" Homeland Security Law", Chapter in National Security Law, 2nd ed., ed. John Norton Moore and Robert F. Turner;

"If it Ain't Broke, Don't Fix It", Patriot Debates: Experts Debate the USA PATRIOT Act, ed. S. Baker, J. Kavanagh;

Report of the Homeland Security and Freedom Working Group, New America Foundation Conference on Terrorism: Security and America's Purpose: Towards a More Comprehensive Strategy, September 6-7, 2005.

"Intelligence Restructuring: Just the First Step," National Strategy Forum Review, Winter 2004

"Civil Liberties in a Post 9/11 World", Forging America's New Normalcy: Securing Our Homeland, Protecting Our Liberty, 5th Report of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction ("Gilmore Commission"), December 2003;

"Legal Framework for Shielding, International Journal of Emergency Mental Health, Vol.4, Fall 2002

"The Deutch Commission Report: An Overview," Nonproliferation Review, CNS, Vol. 6.4 Fall 1999.