S. HRG. 107–449

S. 1448, THE INTELLIGENCE TO PREVENT TERRORISM ACT OF 2001 AND OTHER LEGISLATIVE PROPOSALS IN THE WAKE OF THE SEPTEMBER 11, 2001 ATTACKS

HEARING

BEFORE THE

SELECT COMMITTEE ON INTELLIGENCE

OF THE

UNITED STATES SENATE

ONE HUNDRED SEVENTH CONGRESS

FIRST SESSION

ON

S. 1448 THE INTELLIGENCE TO PREVENT TERRORISM ACT OF 2001 AND OTHER LEGISLATIVE PROPOSALS IN THE WAKE OF THE SEPTEMBER 11, 2001 ATTACKS

MONDAY, SEPTEMBER 24, 2001

Printed for the use of the Select Committee on Intelligence

Available via the World Wide Web: http://www.access.gpo.gov/congress/senate

U.S. GOVERNMENT PRINTING OFFICE

79–625 PDF WASHINGTON : 2002

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

SELECT COMMITTEE ON INTELLIGENCE

ONE HUNDRED SEVENTH CONGRESS

BOB GRAHAM, Florida, *Chairman*
RICHARD C. SHELBY, Alabama, *Vice Chairman*

CARL LEVIN, Michigan
JOHN D. ROCKEFELLER IV, West Virginia
DIANNE FEINSTEIN, California
RON WYDEN, Oregon
RICHARD J. DURBIN, Illinois
EVAN BAYH, Indiana
JOHN EDWARDS, North Carolina
BARBARA A. MIKULSKI, *Maryland*

JON KYL, Arizona
JAMES M. INHOFE, Oklahoma
ORRIN G. HATCH, Utah
PAT ROBERTS, Kansas
MIKE DeWINE, Ohio
FRED THOMPSON, Tennessee
RICHARD G. LUGAR, Indiana

THOMAS A. DASCHLE, South Dakota, *Ex Officio*
TRENT LOTT, Mississippi, *Ex Officio*

ALFRED CUMMING, *Staff Director*
BILL DUHNKE, *Minority Staff Director*
KATHLEEN P. MCGHEE, *Chief Clerk*

C O N T E N T S

S. 1448, THE INTELLIGENCE TO PREVENT TERRORISM ACT OF 2001 AND OTHER LEGISLATIVE PROPOSALS IN THE WAKE OF THE SEPTEMBER 11, 2001 ATTACKS

MONDAY, SEPTEMBER 24, 2001

U.S. SENATE,
SELECT COMMITTEE ON INTELLIGENCE,
Washington, DC.

The committee met, pursuant to notice, at 3:05 p.m., in room SH–216, Hart Senate Office Building, the Honorable Bob Graham (Chairman of the Committee) presiding.

Committee Members Present: Senators Graham, Rockefeller, Feinstein, Wyden, Durbin, Bayh, Edwards, Mikulski, Shelby, Kyl, DeWine, Thompson, and Lugar.

OPENING STATEMENT OF HON. BOB GRAHAM, U.S. SENATOR FROM THE STATE OF FLORIDA

Chairman GRAHAM. I call the meeting to order.

This meeting of the Senate Select Committee on Intelligence is for the purpose of hearing testimony on legislation that was introduced on Friday relative to law changes as it relates to American intelligence and counterterrorism.

The horrific events of September 11 demonstrate America's vulnerability to international terrorism. But the warning signs of our vulnerability have been evident for some time—the bombing of the U.S. Embassy and the Marine Barracks in Beirut as long ago as 1983; the 1993 bombing of the World Trade Center; the 1996 bombing of Khobar Towers in Saudi Arabia; the 1998 bombing of the U.S. Embassies in Kenya and Tanzania; and last year's terrorist attack against the *U.S.S. COLE* in Yemen.

These and other terrorist incidents have made it increasingly important for the Senate Select Committee on Intelligence to focus on the adequacy of the Intelligence Community's response to the terrorist threat.

Our Committee has called this hearing today to discuss with government officials and outside experts and civil libertarians the provisions of S. 1448, The Intelligence to Prevent Terrorism Act of 2001, which Senator Feinstein and I introduced last Friday, along with co-sponsors Senators Rockefeller, Bayh and Nelson of Florida. We will also address today selected provisions of the proposal which was sent to the Congress by Attorney General John Ashcroft on Wednesday, September 19. The Attorney General provisions we

will address today are those that fall within the jurisdiction of the Intelligence Committee.

A number of panels and commissions in recent years all have made clear that any effort to improve the governmentwide approach to terrorism must take into account every facet of the issue—detection, prevention, consequence management, crisis management, and law enforcement, diplomatic and military responses. We, as a government, need to address these issues in a coordinated fashion so that priorities may be set, resources allocated, and government structures changed, if necessary, to serve that overall strategy. A counterterrorism intelligence program must be designed within that larger context of a government counterterrorism program. We must have a centralized authority for managing the intelligence components of that counterterrorism policy. The Director of Central Intelligence needs to perform that intelligence role for the U.S. Government.

In the wake of the September 11 incidents, we must begin to act on myriad aspects of this problem. Accordingly, last Friday, in addition to the legislation I have already referenced, I introduced another bill, S. 1449 which creates a National Office for Combating Terrorism within the White House. Senator Feinstein and I and others have been working on this proposal for several months. We believe, along with the other co-sponsors—Senators Rockefeller, Durbin, Mikulski, Bayh, and Nelson of Florida—that for a coordinator of the forty-plus Federal agencies that must play a role in counterterrorism that the office should be with the following characteristics.

It should be created in statute so as to support the Legislative and Executive branches. It should have a Senate-confirmed director so that he will have the stature appropriate for the position and should have budget authority over that portion of the various agencies' budgets which relate to counterterrorism so that the director can set priorities and allocate the resources appropriately against those priorities. And finally, the director should examine the overall structure of the U.S. Government to deal with terrorism prevention and response and, if necessary, recommend restructuring or merging of agencies and functions.

We believe that the President's Executive order was a significant step forward to achieve these objectives, and that the President's selection of Governor Tom Ridge is an excellent choice to coordinate this enormous and critical effort by the U.S. Government. We want to give him the authority and the tools he needs to be successful.

In this hearing today we will not be discussing the National Office for Combating Terrorism. The Committee will have hearings on that bill in the near future in conjunction with the other committees of jurisdiction, such as the Senate Committee on Governmental Affairs.

Today we want to focus on the issues that are most critical for immediate resolution by the Congress. The Attorney General has urged expedited attention to his series of proposals. Our action today and the Judiciary Committee's hearing tomorrow, which will focus on those matters in its jurisdiction, are indicative of the close collaboration between the Administration and the Congress on these critical issues.

The bill that we will discuss today includes a number of statutory provisions relating to clarifying the authorities of the Director of Central Intelligence to combat terrorism; updating the laws governing electronic surveillance to collect foreign intelligence so as to improve collection against international terrorist targets; and enhancing the ability of law enforcement and intelligence agencies to share critical information relating to the plans and intentions of terrorists.

This legislation represents the culmination of months of effort by many Members of this Committee and other Members of the Senate. I would like to particularly recognize Senator Feinstein and Senator Kyl for the effort that they have invested in this legislation.

My colleagues and I are committed to the substance of these provisions because we believe that they enhance intelligence collection without unreasonably diminishing our civil liberties. We welcome the comments from the witnesses today to help us ensure that the language of these provisions will accomplish both of those goals. We hope that the experts at the Justice Department, FBI and CIA will work with our staff to make certain that we have drafted these provisions in an effective manner.

In addressing these issues, we must be mindful that the terrorist threat to the United States is not a crisis; it is a cancerous condition which we will have to deal with over an extended period of time. Many people liken the war that we are now commencing against terrorism to the war that we have been waging over the past three-quarters of a century against organized crime. Much of the progress we have made in the war against organized crime is a direct result of changing laws to enhance our abilities to deal effectively with this long- term scourge. In a similar fashion, the legislation that we are considering today would allow us to more effectively deal with terrorism as a long-term threat.

Many of the proposals in our bill deal with electronic surveillance to collect foreign intelligence inside the United States, as authorized under the Foreign Intelligence Surveillance Act of 1978. This bill will bring those collection capabilities into the 21st century. Wiretapping laws relating to criminal collection, as contrasted to foreign intelligence collection, have already been updated in many respects. This bill applies the same Constitutional and civil liberties protections in the Foreign Intelligence Surveillance Act context that we are currently applying in the criminal context.

Vicki Divoll, our Committee's General Counsel, will walk through provisions of the bill in a moment.

Later we will be asking our witnesses for their views on both the provisions of S. 1448, as well as select provisions of Attorney General Ashcroft's proposed legislative program which are relevant to the Intelligence Community.

After Ms. Divoll has completed her outline of the provisions in S. 1448, we will turn to our first panel. But first Vice Chairman Shelby.

OPENING STATEMENT OF HON. RICHARD C. SHELBY, U.S. SENATOR FROM THE STATE OF ALABAMA

Vice Chairman SHELBY. Thank you. Thank you, Mr. Chairman. Thank you for calling this hearing. Mr. Chairman, Members of the Committee, I have a few observations.

For many years, this Committee has been emphatic regarding the critical importance of our intelligence apparatus. It is our first line of defense in the war against terrorism and it could be our first line of offense.

Granted, there are some things that we can do in the short term to improve our ability to address this threat and I believe we will do them. We have already provided additional funds and we will grant, I believe, the executive branch new legal authorities through legislation that we are discussing today.

There is a more fundamental problem, however, that cannot be fixed by quickly drafted legislation or emergency funding. Our current national security structure is a legacy of the cold war. The Department of Defense and the Intelligence Community were organized to counter the Soviet threat and they remain in essentially the same form today. The failure of our national security institutions to transform and adapt is a direct result of nearly a decade of inaction and neglect in light of a dramatically changing world situation.

Changing circumstances, as we all know, demand a change in strategy. If we fail to develop a comprehensive national strategy to achieve clear objectives, there is no chance of us organizing our Government to defeat successfully the terrorist threat.

Our Nation derives its guiding principles from the Declaration of Independence and the Constitution. Our Federal Government, in accordance with these guiding principles, develops its objectives and strategic plans in light of the current world situation.

After World War II, the United States faced an entirely new world situation. We went from a relatively isolated and disengaged player on the world stage to the central figure in a global clash between freedom and communist tyranny. Just as the growing Soviet menace and its developing nuclear capability gave rise to President Truman's reexamination of our national objectives and national security strategy, so must the attacks on New York and Washington give rise the to same type of examination.

The result of Truman's reexamination was a document—NSC–68—that formed the basis of our national security strategy and our plans to achieve it for nearly the next half century. The Soviet Union subsequently collapsed not only because it was fundamentally corrupt, but because the United States had a clear purpose and vision of its place in the world and a plan to achieve it.

I believe we now need that same type of vision and a plan. There have been many commissions, studies and reports on every aspect of our national security policies and structure. But, they all have operated in the same vacuum created by the lack of any clear statement of our national purpose in the post cold war world.

The President has already begun the reexamination and taken some very important steps. Now, I believe, he needs to memorialize his vision and assign responsibility and organize the Federal Government to achieve our national objectives.

Why is this important for the Intelligence Community? We all know very well the debilitating effects that turf battles and parochialism can have on our ability to organize and accomplish anything at all. These same maladies have often paralyzed the Intelligence Community. The Intelligence Community is still organized in tightly controlled "stove-piped" organizations that often refuse or are unable to share information with each other for any number of reasons.

The new threats that we face require an intelligence organization that is organized and managed in a manner that recognizes its fundamental purpose. That purpose is to collect, analyze and disseminate information. Our intelligence apparatus is first and foremost an information enterprise. Any effective information enterprise by definition must be networked, be interactive, agile, flexible and focused.

The agencies and elements of the Intelligence Community are anything but agile. They are often paralyzed by their bureaucratic structure. Perhaps the rigid structure was appropriate for monitoring the Soviet Union, but I believe it is antithetical to meeting today's threats. It is particularly ill suited for using modern information technology.

The classic bureaucracy is designed to limit interaction between its people. We will never be able to defeat the terrorist threat without the ability to share rapidly all sources of information on terrorist activities and then take decisive action.

As we saw in the bombing of the *U.S.S. COLE*, we may not get specific tactical warning. But, we may be able to formulate a clearer picture of the threat if our analysts have access to every available piece of information and are allowed to synthesize and disseminate this information. This type of interactive and dynamic community is possible if we have strong leadership guided by a clear vision. But, it will take time, and we don't have time.

I believe that we need to embrace an unconventional approach. The terrorists think unconventionally. We need new thinking and new people looking at this problem. We need our country's most talented and capable people leading the effort.

The old ways, I would submit, have failed us time and again in the new threat environment that we're in today. The examples continue to grow. We all know we've had some successes, but let's talk about the problems—the attack on Khobar Towers; the first attack on the World Trade Center; the attack on the *U.S.S. Cole*; the attacks on our embassies in Africa; and the attacks on September 11.

We have shed enough blood and squandered enough treasure. We need a rapid response. And, I'm afraid that the calcified bureaucracies of our national security institutions are not capable of rapid change. I believe we need to start over with a national commitment of talent and resources much like President's Kennedy's effort to take us to the moon. We need an action-oriented approach where success is measured in the amount of terrorist cells destroyed or disabled, not on how many reports are issued.

I don't know if this new approach will spawn a new organization, but we must begin to think, as we say, outside the box. The answers to this problem are out there and we need to bring them in, nurture and support them and let them flourish undeterred by the

stranglehold of government bureaucracies. Our Intelligence Community, as presently constituted, is virtually incapable of such an effort. As we learned on September 11, the threats are immediate as must be our response.

We can talk about legislative fixes and appropriating more money to feed our failed institutions. I've done some of both. What we cannot do is continue to ignore our limitations and our vulnerabilities. If we fail to marshal our Nation's collective talents and resources behind this effort, we are just waiting for the next attack.

Thank you, Mr. Chairman.

Chairman GRAHAM. Thank you, Mr. Vice Chairman.

[The prepared statement of Senator Rockefeller follows:]

PREPARED STATEMENT OF SENATOR JOHN D. ROCKEFELLER IV, U.S. SENATOR FROM WEST VIRGINIA

Thank you Mr. Chairman. I am grateful for the leadership you have shown over the past 2 weeks as the Congress and the American people have struggled to come to grips with the consequences of the September 11 attacks. The legislative package you and Senator Feinstein introduced on Friday is just one example of that leadership. You have also provided the kind of measured, temperate analysis of the situation that has helped reassure the American people that the Congress is not only aware of the problems we face, but is working expeditiously to implement meaningful and well thought out solutions.

Your legislation is an example of that forward looking, measured approach. This Bill, S. 1448, is the product of several months of work. I know you and your staff have reached out to other relevant Committees in the Senate and have shared language and held discussions with the Administration on all of these provisions. This effort, along with the priorities you have set for the Intelligence Committee and the funding included in the annual Intelligence Authorization Bill, provides the groundwork to have a meaningful impact on intelligence collection against terrorists.

The challenge we have now is to evaluate each of these proposed changes, not as a response to recent events, but for how they will help our intelligence and law enforcement communities deal with terrorism in the long term. As we bolster those efforts to protect America from terrorist attacks, we must make sure we do not sacrifice civil liberties for short term security. Changes we make in the next few weeks will be with us long after we have vanquished Osama bin Laden. Therefore, those changes must be consistent with our underlying values.

Chairman GRAHAM. Ms. Divoll.

STATEMENT OF VICKI DIVOLL, GENERAL COUNSEL, SENATE SELECT COMMITTEE ON INTELLIGENCE; ACCOMPANIED BY: STEVEN CASH, COUNSEL, SENATE SELECT COMMITTEE ON INTELLIGENCE

Ms. DIVOLL. Thank you, Mr. Chairman, Mr. Vice Chairman. I'd like to introduce Steve Cash, who is also a counsel on the Committee and works on counterterrorism issues for the Committee.

I'm just going to walk through briefly the provisions in the Graham-Feinstein bill, S. 1448. I'll start with title I, Clarification of Authorities of the Director of Central Intelligence.

Section 101. The purpose of that provision is to put the DCI in his Intelligence Community hat, not his hat as head of the CIA, this Intelligence Community role in a position to manage the information collected under the Foreign Intelligence Surveillance Act. Currently the DCI manages the strategies for collecting using every other tool available to him. The FISA tool is a critical tool used inside the United States, but it's a critical tool for collecting foreign intelligence.

The provision is designed to put the DCI at the very front end and the very back end of that process. Operational efforts would still be conducted by the FBI, because this is a domestic activity. The specific targeting would be done by the FBI. But the DCI would perform with respect to FISA the same function he performs in other areas, which is to set an overall strategy for how this valuable resource should be used, how it should be allocated, how it should be prioritized, and how it would fit in with the rest of the collection—would it be redundant, would it be in addition to the other types of collection that we have.

So he would be responsible for setting those priorities and providing a strategy to the FBI for them to use in implementing that strategy.

He would also find himself at the end of the process. As a Vice Chairman mentioned, all the information collected of foreign intelligence value has to get to the analysts and has to be analyzed as part of all the information coming in and has to then be processed and make it to the policymaker/consumer so they can act on it.

FISA needs to be part of that process, and this would put the DCI in charge of making sure that the information is tracked to the proper analysts, is analyzed and makes it into a disseminated product to the community. We feel that that's an important role for him to play.

The second provision is more of a technical change but also important in the sense that in looking at the definitions of the National Security Act of 1947 you see that the definition of counterintelligence includes international terrorism, but the definition of foreign intelligence does not. The purpose of this provision is to clarify that. The purpose is not to rearrange the responsibilities between the FBI and the CIA with respect to collection and activities. The purpose is to clarify in the law that of course the DCI has a role in international terrorism overseas.

As you play out the National Security Act through its provisions, we want to make sure that that is clarified in the law.

Section 103 is an attempt to deal with the much-publicized issue of recruitment of terrorists who have unsavory pasts, whether it be violent crimes or human rights abuse. Everyone seems to acknowledge that those are the types of people who would be most helpful in this effort to collect information, human source intelligence information. But there is a fear that the regulations at the Agency, the CIA, have a chilling effect on efforts in the field to recruit those types of people.

The effort here is to clarify in law, if the Congress accepts this provision, wants to send a message to the field that this is lawful, to recruit such people and establish relationships with them. This provision does not attempt to dictate to the DCI or the Executive branch what types of approval processes they need to have to make sure the officers do their work appropriately. It merely is designed to State in law that this is a lawful activity.

Section 104 is an attempt to give a break to the intelligence agencies who prepare so many reports for Congress on intelligence matters. Given that they are busy with other things now, we thought we would give them an extension until February 1 and they can have an extension beyond that if they certify to the Com-

mittee that the people who prepare those reports are working on counterterrorist matters.

Title II deals with several aspects of electronic surveillance. Section 201 is meant to deal with the definition of communications under FISA. The purpose of this provision is to carve out of that definition communications that aren't really content-based, that wasn't intended when the provision was enacted to be part of the FISA process.

These would be the types of communications where, for example, a hacker tells his computer to tell another computer to do something or not do something. One example we've given is if a hacker in a foreign country communicated with the computer of the Hoover Dam, for example, and told it to open the flood gates, that type of communication is not content based and really has no purpose in requiring a FISA order. So the FBI would be able to collect that type of communication without having to get a FISA order.

Sections 202 and 203 are both provisions that we've had in this bill for some time but that are also part of Attorney General Ashcroft's package. Section 202 speaks to the duration of surveillance and physical search orders under FISA against non-U.S. persons, including terrorists operating as agents of foreign powers inside the United States. The current law requires the Department of Justice to renew those applications every 90 days for electronic surveillance and every 45 days for physical searches. This provision would extend both of those to 1 year and would hopefully free up the lawyers at the Department of Justice and the FBI also to work on new FISAs rather than having to constantly go back and renew old FISAS.

Section 204 is a provision that clarifies in law that Foreign Intelligence Surveillance Act collections can occur simultaneously with title III collections in the criminal arena. This would say that there are two courts that deal with those. The prosecutors would have to make the showing required under title III for a criminal wiretap, and the FISA lawyers would have to make the showing to the FISA court that it meets the standards of FISA.

In some cases it makes sense, if the lawyers decide that it does, to do both, and as long as both standards are met, both courts approve it, we felt it was useful to clarify that in the law.

Title III is entitled——

Senator FEINSTEIN. Mr. Chairman, excuse me. She skipped section 203, which I think is an important section.

Ms. DIVOLL. Oh, thank you, Senator, yes.

That is a provision that is also in the Ashcroft proposal. This is a provision that tries to get FISA up to date with the criminal context. In criminal wiretap law there is something called a roving wiretap that's been accepted as an appropriate approach. This would allow that same type of targeting to be done under FISA. If it's a situation where a terrorist target is trying to defeat the collection against him by throwing away a phone and picking up a new phone or moving or whatever method he would use, this would allow that FISA to continue on to the other technology rather than having to be re-applied to the FISA court.

Thank you, Senator.

Section 301. In law currently there is a requirement that officers in the intelligence community agencies in the course of their duties, if they come across evidence of a crime, a U.S. crime, they are required by law to report that to the Attorney General. There's an elaborate process in the agencies to do that. This would be in a sense a reverse crimes reporting requirement.

This requires law enforcement officers in the course of their duties, if they come across foreign intelligence information, they would also have a duty to provide that to the DCI, again so that all-source reporting, all of the information available to the U.S. Government is used properly and effectively to counter this threat and other threats.

Section 302, the Foreign Terrorist Asset Tracking Center. This is a reporting requirement. It's not a mandatory requirement. It asks the DCI, the Director of Central Intelligence, and the Secretary of Treasury to work together and by February 1 come up with a proposal to implement in the Department of Treasury or wherever they see fit an operation that would track terrorist financial networks and transactions and provide that information to the Intelligence Community, which would hopefully provide valuable information about relationships within terrorist groups and the communications among them and the transfers of money. So that's required as a report by February 1.

Section 303 is the National Virtual Translation Center. One of the key problems that's been highlighted by many is the fact that we collect vast amounts of intelligence, both technically and with human sources, and that we don't have the capabilities to translate that quickly and efficiently get it to the analysts and the operators in the field who need it.

This provision would require the establishment of a center that really is not a bricks and mortar kind of thing. It's a virtual center that would link up, through a secure data base, the vast translation resources available in our country. People who live in different parts of the country and have unusual translation and language capabilities could be hooked up, the information could be put in a data base after it's collected, sent to them They would process it, put it back in the data base. It gets to the analysts and ultimately to the consumer in an efficient way.

Section 304 is a training provision that we think augments many of the other provisions that I've spoken about. It provides for training of Federal, State and local officials who may come across in their duties foreign intelligence information but wouldn't know how to recognize it. They would be trained to know what to look out for and who to call to get it into the Federal Government's hands.

It also would train them to be better consumers of intelligence so in the event of a crisis such as the one we just had, when the Federal Intelligence Community reaches out to State and local they will have a point of contact and a frame of reference and be speaking the same language. So that's the purpose of that provision.

Thank you.

Chairman GRAHAM. Are there any questions of Ms. Divoll?

Senator Shelby.

Vice Chairman SHELBY. Ms. Divoll, did you go into section 103? You mentioned that, did you not?

Ms. DIVOLL. Yes.

Vice Chairman SHELBY. This deals with the establishment and maintenance of intelligence relationships to acquire information on terrorists and terrorist organizations. With respect to section 103 of this legislation, under applicable law and current CIA guidelines who can our intelligence officers recruit?

Ms. DIVOLL. The intelligence officers recruit those that they feel are appropriate to meet the requirements they have been given, and then there's an elaborate process within the Agency to vet those recruitments and approve them up through the chain of the Agency.

Vice Chairman SHELBY. Does section 103 present any separation of powers issue? If so, how do you resolve them in favor of the legislative branch?

Ms. DIVOLL. Well, that's a good question.

Vice Chairman SHELBY. I guess the first question is, do they present any separation of powers issues?

Ms. DIVOLL. I don't think so, Senator. One approach recommended by some to deal with these regulations within the Agency—these are classified regulations but essentially they're an approval process to make sure that those who would be recruited who have difficult pasts, that there's enough approval process up the chain to balance the risks of working with someone like that against the gains.

To just rescind those regulations by statute I think would present separation of powers problems because you are essentially telling the Executive branch what to do in their own internal approval processes.

Vice Chairman SHELBY. We would be telling the Executive branch what to do and how to do it.

Ms. DIVOLL. Yes, Senator. We thought that this didn't quite go that far and this just states in law that this type of recruitment is lawful and doesn't attempt to tell the Executive branch what types of approvals they would need to make sure that it's done properly.

Vice Chairman SHELBY. But the Executive branch on their own could change that as they changed it one time before.

Ms. DIVOLL. Yes, Senator.

Vice Chairman SHELBY. I'd like to ask, Mr. Chairman, Mr. Cash a question if I could on section 303, the National Virtual Translation Center. My question concerns the establishment of this center.

Mr. Cash, as a former intelligence officer, you know how important language skills are in the gathering, analysis and dissemination of intelligence. Could you elaborate on what this center would do? In other words, how would it assist us in preventing the next terrorist attack?

Mr. CASH. Mr. Vice Chairman, if I could answer that question with an example, if an intelligence officer sitting at Langley acquires, through whatever means, a document in a language like Urdu, the only Urdu translator who may be available right then, that day, may be living in Seattle. It's going to be very hard to fly him to Washington and it's going to be hard to take the document to Seattle.

The idea of the National Virtual Translation Center is that these resources would be linked through an internet-like mechanism, secure of course, which would allow the translation to take place in Seattle, the intelligence officer in Langley to read the results, perhaps share it with a colleague in London or France or some other country, and then maybe with an FBI agent in New York, all in near-real time, all without moving any human beings anywhere.

So instead of having to wait days to translate and read critical information, it could be minutes.

Vice Chairman SHELBY. I like the idea and I could see how it could work. Is there a projected cost for this center? As an appropriator, I wondered if you had talked to Senator Inouye or Senator Stevens about this.

Mr. CASH. The intention here is that, given the guidance that this statute would contain, that the DCI in his community role would take a look at this problem, with the general guidance we've given him, which is we would like you to establish such a center, and then would be able to come back to the Congress in a relatively short amount of time and say this is what it takes to get it done, this is how much money I will need to get it done, and this is how long it will take.

Vice Chairman SHELBY. What you'd be doing really, in a sense, is utilizing the latest technology to take advantage of any weapon deficiencies you might have.

Mr. CASH. That's exactly it—Napster for spies.

Vice Chairman SHELBY. Thank you, Mr. Chairman.

Chairman GRAHAM. Thank you.

Senator EDWARDS. Mr. Chairman.

Chairman GRAHAM. Senator Edwards.

Senator EDWARDS. Ms. Divoll, I wonder if you would, for all of our purposes, contrast the provisions in this legislation with respect to information-sharing between the FBI and the CIA with the Administration's proposals and comment on why your legislation is different.

Ms. DIVOLL. Certainly, Senator. There are some differences and there are some similarities. The Administration's package includes express changes in title III and rule 6(e) of the Federal Rules of Criminal Procedure to make certain that information collected in those ways can make it to the intelligence community. It's optional, but it would remove an impediment in law that now exists and open that up to possible sharing.

The Administration bill also has a provision that is a catch-all that catches everything else other than 6(e) and title III and says everything else also collected in the criminal context can be passed.

Our provision, section 301, goes a little further in one respect. In current form it says "in accord with other provisions of law" this information may be shared. If the title III and 6(e) provisions of the Ashcroft proposal are not enacted, then that type of sharing would not happen under section 301 because it would be otherwise prohibited by law.

If they are enacted, then this provision says that all such information, all such foreign intelligence information, 6(e), title III and all other—whether it be an FBI interview or collected in some other way—must be shared. It doesn't give them discretion.

Senator EDWARDS. One other question, Mr. Chairman.

Chairman GRAHAM. Let me just mention that the first witness on the first panel will be Mr. David Kris, Assistant Deputy Attorney General at the Department of Justice, who will provide us with the same analysis of the Attorney General's provisions as they relate to the jurisdiction of this Committee, as Ms. Divoll has just done for 1448.

Senator Edwards.

Senator EDWARDS. Thank you. This is another question for Ms. Divoll. Under current law FISA procedures can only be used when the primary purpose, "the" purpose, is foreign intelligence gathering. The Administration has proposed that "the" be changed to "a," as I understand it, which would mean that it has to be a purpose, not the primary purpose.

That provision is not in this legislation; is that correct?

Ms. DIVOLL. It's not.

Senator EDWARDS. I wonder if you could comment on why it is not included.

Ms. DIVOLL. Well, we've had the Ashcroft proposals just for a few days now, and these proposals we've worked on for some months. I think that it's fair to say that the Ashcroft proposals, coming after September 11, have sought to really go quite a bit further than we felt we would be able to go in this provision, and we haven't looked at that provision with the Chairman to determine whether it would be a good change or not. We're still working on that.

Senator EDWARDS. Have you done any work yet on the question of the constitutionality of making that change and broadening the FISA procedures? As I understand it, one of the reasons that they have withstood constitutional muster up until now is because of the limitation to foreign intelligence gathering.

Ms. DIVOLL. Yes, Senator. I don't pretend to be an expert in the courts that have reviewed FISA, but I think it is safe to say that if you make a fundamental change in FISA it is possible that the courts would feel they would need to take a second look and make sure that it meets constitutional muster.

Senator EDWARDS. My only comment would be I think many of us believe that the expansion of some of these authorities is a very good idea, but I think we need to make certain that we're doing it within the framework of what's constitutionally permitted.

Thank you, Mr. Chairman.

Chairman GRAHAM. Senator Durbin, then Senator Kyl, then Senator Bayh.

Senator DURBIN. Thank you very much. Thank you for the presentation.

A lot of attention has been directed toward section 103 and the so-called question of dirty assets and the regulations that were issued by the CIA in 1995, as I understand it requiring field officers to obtain prior CIA headquarters approval before establishing a relationship with an individual who has committed serious crimes, human rights abuses or other repugnant acts.

If I recall our earlier conversation, the situation that gave rise to this was in Guatemala, where some of the people whom we were working with turned out to have been involved in the assassination

and killing of Catholic priests and nuns, which gave rise to this new regulation requiring headquarters approval.

If you can answer this, can you tell me, since the enactment of these regulations in 1995, has the Agency ever turned down a field request to recruit an individual in a terrorist organization or in any way avoided contact with individuals, regardless of their past, who may have had information about terrorist activities?

Ms. DIVOLL. Senator, when the Bremer Commission on Terrorism came out with their recommendation a few months ago recommending rescinding of these internal CIA regulations, the Agency came forward publicly and answered that question and said that no proposal to recruit someone with human rights or other problems who had valuable information on terrorism and terrorist targets, none of those had been turned down.

The approval process can be very prompt and efficient, particularly if there is a sense of urgency, and I think people in the Agency believe that it has done a good job of balancing the need to work with such people against the risks of working with such people.

Senator DURBIN. I don't know if you can answer the second question, but it will be my last one. Is there a belief that these regulations have had a chilling effect on people in the field in terms of those that they seek to recruit for fear of these regulations or a negative response from headquarters?

Ms. DIVOLL. I think some believe that the people in the field feel that way. Some of the people in the field report that to Senators when they are on trips. Others of them, particularly those who work exclusively in the counterterrorist area I think say "no." I think they feel that this is their mission, this is their duty, and that it would be career-enhancing, if you will, to make such a recruitment. So there is controversy on that.

The purpose of this provision was to make sure that, to the extent anyone feared Congress's reaction to those types of recruitments that we said clearly in law that it's appropriate and desirable.

Senator DURBIN. Thank you. Thanks, Mr. Chairman.

Chairman GRAHAM. Senator Kyl.

Senator KYL. Thank you, Mr. Chairman. I needed to ask this question now. It may be appropriate for the next panel too, but I have a commitment from 4 o'clock to 5 o'clock that was made before this hearing was scheduled that I must honor.

So let me ask this panel first. This is really the reverse side of what Senator Edwards asked earlier. Under domestic law, law enforcement agencies can use pen registers and trap and trace devices to capture so-called peripheral data associated with a telephone call. The Supreme Court has ruled that that is fine, that there is no reasonable expectation of privacy in just the mere fact that one person called another. The actual communication is all that's protected. In other words, the telephone number or fact of the call is not.

My understanding under FISA is that the existence of the call or the data exchange is termed a communication that must be protected from electronic surveillance. Did you look at the possibility of altering that to conform it to domestic law and, if not, is there any reason that you know of why under FISA the digital or periph-

eral data associated with a call has to be considered as sensitive as the communication contained with the call.

Ms. DIVOLL. Senator, I understand. The provisions in the Graham-Feinstein bill, again as you know because you worked on it, were put together before September 11, and I think that the provision you're talking about, which is part of the Ashcroft proposal, will be one that this Committee will look very seriously at. We didn't include everything in this. We didn't feel that we could push too far because we weren't in the State we're in now. But I think people are going to look at that very carefully through the Ashcroft provisions.

Chairman GRAHAM. Thank you, Senator.

Senator Bayh.

Senator BAYH. Thank you, Ms. Divoll. Could you please expound in a little greater detail on the asset tracking center? It seems as if the provision focuses on the analysis and dissemination of foreign intelligence related to financial capabilities but doesn't really propose any additional action based upon the information, such as extending the suspicious activity reporting requirements or perhaps prohibiting a foreign entity that had been identified as a primary money-laundering concern from doing business in the United States.

Was there a reason for that?

Ms. DIVOLL. If it's all right, sir, I'll defer to Mr. Cash to answer that.

Mr. CASH. The intention here was to direct the creation of an entity that would allow the effective analysis of the vast amount of data from all different sources related to finance and financial transactions, analyze it, and make sure that it gets to the consumers. One of the very consumers that we were worried about are the kind of people in, for instance, the Department of the Treasury who make exactly the policy decisions or operational decisions you just referred to. So the intent was not to try to change the standards for, for instance, freezing assets or acting on a suspicious activity report, but rather to ensure that those policymakers are serviced as well as possible by the Intelligence Community.

It addresses the concern that that wasn't happening—a lot of financial data not going to a central place, not getting out to all of the right people.

Senator BAYH. The left hand not knowing what the right hand was doing.

Mr. CASH. Exactly.

Senator BAYH. Thank you, Mr. Cash.

Chairman GRAHAM. Thank you, Senator.

Senator Rockefeller.

Senator ROCKEFELLER. It's possible that Senator Durbin asked this question, but I didn't hear it. There's a follow-up to his question. If one says that no requests have been turned down from the field for approval at a higher level in so-called less-than-savory assets, and then you come back and you say "no," that's a very declarative answer. The other side I'm looking at, of course, is that not many requests are made because people don't want to be hung out to dry in case their asset turns in some way to be nastier than anticipated.

So my question would be, in fact, in view of the need for this kind of asset, have there been the numbers of requests for these folks that would warrant the statement "Oh, there really isn't a problem because nobody's been turned down."

Ms. DIVOLL. Senator, I think one way to answer that question is to speak to the difficulty of this type of recruitment in the first place. I think that people look at—people who are involved in the intelligence business look at this type of issue and they say we haven't succeeded, what's the problem, maybe it's these regulations, when in fact the target is a very difficult one and the officers are working hard to recruit that type of person, but that type of person often is not going to want to work for the U.S. Government.

So I think it's more a reflection of the difficulty of the target than the procedures themselves would be my answer.

Senator ROCKEFELLER. OK.

Chairman GRAHAM. Senator Wyden.

Senator WYDEN. Thank you, Mr. Chairman. I thank both of you for your presentations.

I think what Senators are reflecting is a desire for some balance. It's obvious that we want to have new tools out there to protect our citizens from the threat of terrorism without giving up the ages-old tradition of protection for freedom and civil liberties. It seems to me what both bills are trying to do—and maybe you can clarify this—is both them seem to give the judiciary a pretty significant role with respect to most of the areas where new power is authorized. Is that correct? Maybe I'm missing something. I think the hacking provision may be one that is different, but for the most part the judiciary is given pretty significant powers with respect to reviewing all this. Maybe you could comment on that with respect to both bills.

Ms. DIVOLL. Yes, Senator. The vast majority of the provisions in both bills are designed to expand the situations in which a court may order a FISA. It certainly doesn't require the court to order a FISA in those situations. It would, as you said, both in the criminal title III context and in the FISA context, judicial officials—the FISA court and the criminal courts—would be passing on these applications. They would just have a little bit more clear guidance from the Congress and a little bit more leeway on approving them, but they would still be reviewed.

Senator WYDEN. Thank you, Mr. Chairman.

Chairman GRAHAM. Are there any other questions? If not, thank you very much, Ms. Divoll and Mr. Cash.

I'd like to ask our first panel if they would please come forward. Mr. David Kris, Assistant Deputy Attorney General of the Department of Justice, Mr. Larry Parkinson, General Counsel of the Federal Bureau of Investigation, and Mr. Robert McNamara, General Counsel of the CIA.

As they are settling in, Senator Feinstein would like to make an introduction to the Committee.

Senator FEINSTEIN. If I might, there is a gentleman in the audience that I would like to introduce to the Committee. He is the brother of the pilot of the American Airlines Flight 77 that crashed into the Pentagon on September 11. Of course all 58 passengers and five crew members perished. The pilot, Charles Burlingame,

was a graduate of Anaheim High School in California. He attended and graduated from the U.S. Naval Academy. He served in the Navy from 1971 to 1978, where he flew F–4 Phantoms and retired with the rank of Commander. From 1979 to 1998 he served in the Naval Reserve, obtaining the rank of Captain. He has had a 22-year career as a pilot with American Airlines and he was a day short of his 52 birthday when this happened. He leaves a wife, Sherry, and a 26-year-old daughter, Wendy, as well as two brothers, Mark and Brad, and a sister, Deborah.

Brad Burlingame is here today. He is the president of the West Hollywood Convention and Visitors Bureau. Both Mr. Burlingame's father and mother are buried in Arlington Cemetery, and the family is very desirous that Mr. Burlingame be buried there as well. I would like to ask Brad Burlingame if he would stand so that the Committee might acknowledge his presence.

Senator MIKULSKI. Thank you very much, Senator Feinstein. His brother lived in Maryland, so we also wish to welcome you as well.

Senator FEINSTEIN. Thank you.

Chairman GRAHAM. Thank you very much, Senators Feinstein and Mikulski. We extend to you and through you to all of the families of the victims of this horrible tragedy our deepest sympathy.

As indicated, Mr. Kris is prepared to not only comment on the proposals that are included in the introduced legislation but also on those provisions within the Attorney General's recommendation which relate to the jurisdiction of the Intelligence Committee. Mr. Parkinson is not going to be making formal testimony but will be here as a colleague of Mr. Kris.

Mr. Kris.

STATEMENT OF DAVID KRIS, ASSOCIATE DEPUTY ATTORNEY GENERAL, DEPARTMENT OF JUSTICE; ACCOMPANIED BY: LARRY PARKINSON, GENERAL COUNSEL, FEDERAL BUREAU OF INVESTIGATION

Mr. KRIS. Thank you, Mr. Chairman, Mr. Vice Chairman and Members of the Committee. Thank you for the opportunity to discuss proposed legislative responses to the acts of terrorism inflicted on our country on September 11.

My name is David Kris and I am an Associate Deputy Attorney General at the Department of Justice. My portfolio there includes national security policy and FISA, the Foreign Intelligence Surveillance Act. This is my first appearance before this Committee—actually before any Committee—and I appreciate the opportunity to present the Department's views.

Chairman GRAHAM. We appreciate this opportunity to be your first exposure to the Congress and we will try to act with appropriate respect.

Mr. KRIS. Thank you.

The Attorney General and the Deputy Attorney General both wanted to be here today. Unfortunately, a conflicting prior commitment to testify before the House Judiciary Committee and their operational duties in connection with this investigation have made that impossible. But, Mr. Chairman and Mr. Vice Chairman, they send their apologies and they hope that you and other Members of

the Committee will accept their heartfelt appreciation for your extraordinary leadership at this critical time.

In particular, Mr. Chairman, I want to thank you and the Vice Chairman and the other Members for the Committee's expeditious consideration of our request for a hearing today. For that and for the collaborative spirit that you have shown throughout this process we are deeply grateful. The Department has long enjoyed a close working relationship with this Committee and we look forward to its continuation.

We're also grateful that you have invited our views on the bill that you and Senator Feinstein introduced 3 days ago. I know you share our goal of giving the law enforcement and intelligence communities the tools that they need to stop terrorists before they can strike again.

Mr. Parkinson and I are prepared to discuss in detail the specific provisions of the Administration's proposal that you previously identified for us based on the Committee's jurisdiction. That proposal obviously remains our top priority. Due to the short timeframe and the operational and policy duties that Mr. Parkinson and I must carry out, we have not had an opportunity to fully review all of the provisions in your bill, and while I believe we can endorse the substance of some of your bill's provisions and I know that we share common goals, we would like to reserve some of our comments on the particulars of the language as the bill is currently drafted. The Department looks forward to working with the Committee as necessary to ensure that we achieve the goals that all of us seek.

We are therefore prepared to answer general questions on provisions of the Graham-Feinstein bill to the extent that there is a cleared Administration position on them, and we pledge to work with you on all of the bill's provisions to achieve our common goals of finding those responsible for the recent attacks and preventing future attacks.

Again, let me thank you for your outstanding leadership and commitment in holding this hearing and for focusing the Nation on the needs of the intelligence and law enforcement communities to fight aggressively and consistent with the protection of civil liberties the threat that terrorism poses to us and to the world.

Thank you.

Mr. MCNAMARA. Mr. Chairman, may I make a few opening remarks, please?

Chairman GRAHAM. Yes. Then, Mr. Kris, are you going to walk us through the Attorney General's provisions?

Mr. KRIS. Yes, sir, I will do that.

Chairman GRAHAM. Mr. McNamara.

STATEMENT OF ROBERT MCNAMARA, JR., GENERAL COUNSEL, CENTRAL INTELLIGENCE AGENCY

Mr. MCNAMARA. Thank you, Mr. Chairman, Vice Chairman Shelby, Members of the Committee. I do not have a formal statement for the record, but with the Chair's permission I would like to make a few opening remarks.

Two weeks ago today the mood of the American people actually was fairly upbeat and optimistic. Summer was over, the fall looked

promising, markets appeared to be recovering and moving back to that 10,000 mark, unemployment figures were at low levels, as were interest rates, parents were concerned about the beginning of the school year and the students were getting concerned about the beginning of football and soccer season.

Less than 18 hours later, the world as we knew it changed forever for all of us. Terror was forever redefined, and September 11 became a date that none of us will ever forget. Not only will we never forget the pictures we saw or the cries that we heard or the devastation that took place. We will not forget the overwhelming emotions of the moment—the fear, the horror and the helplessness.

If we did not know it before, we learned how vicious terrorists are and how vulnerable an open society can be. But we also had occasion to see good among evil—extraordinary courage and exceptional kindness. We saw clearly, perhaps as never before, that we are neither black nor white, neither Asian nor Hispanic. We are neither Jew nor Muslim or Christian. We are Americans and we are proud of it.

In those first few horrible moments we may have been forced to our knees, but only to pray for those who had fallen. Our hearts may have been broken but not our spirit, and certainly not our resolve. As we stood together that day and as we stand together in the days ahead, we will take to heart the words of our President. Our grief has turned to anger and anger to resolution. Whether we bring our enemies to justice or justice to our enemies, justice will be done.

To that end, the men and women of the Central Intelligence Agency and of our entire Intelligence Community are working around the clock to assist our partners in law enforcement, the military and diplomacy to bring to justice the perpetrators of these atrocities and to thwart others who would harm the national security of the United States.

Mr. Chairman, I applaud your leadership and efforts to respond quickly and vigorously to the current and continuing threat of terrorism. I appreciate the opportunity to testify today regarding two separate legislative proposals that in many instances would provide needed enhancements to law enforcement and the Intelligence Community authorities. These enhancements have been carefully drafted to protect the civil liberties guaranteed United States citizens by the Constitution and at the same time to improve our ability to protect national security.

The Intelligence Community's mission at its core is the collection and dissemination of foreign intelligence and counterintelligence information to those who chart our country's course in the world. Without robust collection authorities, however, the Intelligence Community cannot provide the important information that our Nation's leaders need to make the difficult decisions they face in times of peace and in times of crisis. The statutes that control the manner in which the intelligence community conducts electronic surveillance are currently struggling to keep pace with the rapid expansion of communication technologies. The Foreign Intelligence Surveillance Act of 1978 was drafted well before communication devices such as cell phones and e-mail had so permeated our daily lives.

Both pieces of proposed legislation would make a number of sensible enhancements and clarifications to existing law enforcement and Intelligence Community authorities to deal effectively with the communication technology explosion. These enhancements and clarifications would also remove artificial barriers to information-sharing between law enforcement and the Intelligence Community.

The Intelligence Community supports in one form or another a number of the provisions found in both pieces of legislation. However, we also believe that these proposals provide an excellent starting point for the Administration and Congress to discuss other needed improvements to intelligence capabilities, carefully balancing the interest of national security with the privacy rights we all enjoy under the Constitution.

I welcome the opportunity to discuss these pieces of legislation or other important proposals that would further the ultimate goal of both Congress and the Administration, and that is the protection of our fellow citizens.

Thank you, Mr. Chairman.

Chairman GRAHAM. Thank you very much, Mr. McNamara. Mr. Kris, if you could walk us through the Attorney General's proposals, let me state a question which will relate to all of the provisions. The Attorney General, when he made his announcement, emphasized the sense of urgency. He talked about trying to get this accomplished within a 2-week period. As you discuss the specific provisions within your ability to do so, if you could give us some sense of why the urgency to move forward on these particular recommendations.

Mr. KRIS. Yes, sir. What I would like to do, with your permission, is actually begin with section 151 of the Administration's proposal. I think as I go through I will be able to come back to some of the earlier sections that you identified—sections 103, 104 and 105—but it will ensure, I think, a little more thematic coherence if I do it that way.

For each of these provisions I'll try to give a one-sentence overview of what the amendment would do, explain the current law, and then show what the amendment would do to current law, and try to give you then finally a sense of the reasons that we think these amendments are needed.

Section 151 would lengthen the period of court-authorized electronic surveillance and physical searches under FISA. In current law, electronic surveillance is authorized for 90-day periods, physical searches for 45-day periods for most FISA targets. However, for surveillance and searches of foreign powers themselves, as opposed to their agents, authorization periods for both physical search and electronic surveillance are 1 year.

The amendment would change those timing provisions in two ways. First, it would extend from 45 to 90 days the period of court authorization for a physical search of an ordinary target, a routine target. That would bring into accord the period for electronic surveillance, which is currently 90 days, and the period for a physical search.

The other thing that the amendment would do is it would expand the category of targets to whom the 1-year authorization periods apply. In particular, 1-year authorization periods would be avail-

able against officers or employees of a foreign power and foreign members of an international terrorist organization. I think the critical point to make with respect to that expansion of the 1-year provision is that none of the targets that would be subject to it under the Administration's proposal would be U.S. citizens or permanent resident aliens.

The reasons for these amendments are largely to deal with difficulties we have had implementing the authority we got from the court and to improve efficiency and streamline the process.

With respect to the 45- to 90-day expansion for physical searches, FISA searches are unlike ordinary criminal law searches in that they are conducted surreptitiously and it is often difficult actually to execute the authority we have from the court within a 45-day window. Enlarging the period to 90 days would double our chances of successfully implementing the authority.

It would also help us in cases where we are seeking both electronic surveillance and physical search authority simultaneously because the similar period would keep the applications in sync as we go down the line and renew them as necessary.

The reason for the 1-year provision expansion is that the targets that we would add to that category are often here for long periods of time and it is difficult to continually renew applications to maintain coverage. I want to emphasize it is not a trivial thing to put together and file a FISA application. As the Committee is aware, a FISA application requires the personal certification of a high-ranking executive official such as the Director of the FBI or the Director of Central Intelligence. It also requires the personal approval before filing of the Attorney General or the Deputy Attorney General.

Finally, depending on where the search or surveillance may take place, it will require an affidavit from a field agent in the FBI, for example, and that will require transmission of highly-classified material over great distances within this country to ensure that what we file with the court is accurate.

It is a significant process and reducing the number of applications that we need to file on these non-U.S. person targets would aid us significantly.

Section 152 of the Administration's proposal is what is commonly now referred to as a multi-point authority or roving wiretap authority. Under current law, when we seek authority to conduct electronic surveillance from the FISA court, the court will issue an order of assistance to a particular telecommunications provider to allow us to implement the surveillance. The amendment would allow the court to issue broader orders that we could use with any provider, if the court found that the actions of the target may have the effect of thwarting the surveillance.

The reason for that amendment is effectively tradecraft and countermeasures that our adversaries can employ in this area. The adversary in a FISA situation is often a very sophisticated target—state-sponsored or otherwise. It is under current law possible for a spy or a terrorist, let's say, to simply switch cellphone providers just before a critical communication will occur. In the time it takes us to go back, spin up a new application, obtain the certification

and approval from the Attorney General and file the document with the court to get a new secondary order, it may be too late.

This authority, as the Committee is aware, exists already on the criminal side and we would like the same authority on the FISA side.

Sections 153 and 154 of the Administration's proposal are designed to foster and facilitate greater coordination between the law enforcement and the intelligence sides of the Government. Section 153 would amend the certification provision in FISA to which I previously referred. Under current law, the DCI or the Director of the FBI, as the case may be, will certify that the purpose of the search or surveillance is to collect foreign intelligence information. The amendment would change that requirement from "the" purpose to "a" purpose.

Let me also describe section 154 before I come back to the reasons for the amendments. Section 154 is designed to address the other side of the coin, and that is it will allow all foreign intelligence information developed in a criminal investigation, regardless of the method used to collect the information, to be passed over to intelligence and other appropriate authorities within the Executive branch. That would specifically deal with restrictions that are contained in title III, the domestic criminal wiretap law, and rule 6 of the Federal Rules of Criminal Procedure, which governs grand jury secrecy.

The provision would say that notwithstanding any other law, foreign intelligence information—and that is a defined term—may be passed to intelligence authorities regardless of other restrictions that exist. As I say, the basic animating purpose here is to ensure that the two sides of the Government are communicating well. I think this investigation is a paradigmatic example of the need for that greater cohesion.

It's been reported in the press there are 4,000 FBI agents out gathering information, and I have spent time in the FBI's command center, SIOC, seeing that information being pulled in by any lawful means that is available to us. It is less than ideal, I can say, to have information coming in through a title III wiretap, if there is one, and have it be the case that the criminal investigators who are running that wiretap are simply unable to pass the information over to the counterintelligence investigators who may be performing FISA surveillance or doing something else on the other side.

So the animating purpose here is to bring those two sides together, allow for a single unified, cohesive response, and avoid splintering and fragmentation.

Now there have been questions raised about the constitutionality of the "a purpose" test. Let me say a word about that. I do think that's a real issue.

We have had, as a procedural matter, our Office of Legal Counsel, which is the component within the Department of Justice whose job it is to evaluate the constitutionality of this kind of legislation, review the proposal here before we put it in our bill. They have approved its inclusion in the bill. Indeed, I am told that a letter is being prepared that will communicate the substance of our

analysis on this, but let me give you just the sort of short version of it now.

FISA articulates standards for electronic surveillance that are different from and in some ways more lenient than those that exist in ordinary criminal surveillance. The justification under the Constitution for using those different standards has historically in the case law been linked to the purpose of the surveillance, in particular that the purpose of the surveillance be to collect foreign intelligence information.

The question of exactly how much purpose and what degree of purpose is constitutionally necessary is open to question. There is not a vast amount of case law on this. Some cases have adopted a primary purpose standard but have left open the possibility that the floor may be lower.

What our amendment would do would be to eliminate any artificially high statutory barrier and allow the constitutional standard to be developed on a case-by-case basis. OLC has concluded that an amendment of that kind would not risk the statute being struck down on its face. What we would have to deal with is a case-by-case evaluation in each case of whether we have crossed the line. But that would allow development of the law at the constitutional level and eliminate the statutory barrier, and that is the gist of our thinking that underlies section 153.

I want to emphasize this is a serious problem, and I think the example I gave—that of being in the FBI SIOC—is one illustration of that. We hope that this can be dealt with.

Let me, having spoken about sections 153 and 154, talk about sections 103 and 104, two of the other provisions you asked about. Section 103 and actually section 354 as well are both sharing provisions that are designed to eliminate specific barriers to sharing information obtained from a criminal investigation. Section 103 deals with title III's limitations; section 354 deals rule 6. Both of those are covered by our section 154.

If you were to enact section 154, I think sections 103 and 354 would not be necessary because section 154 is the blanket approach to this problem.

Section 105 is another provision that you identified for us, and it would allow the use of wiretap information obtained abroad from foreign governments. Effectively it provides that if there is no U.S. law enforcement involvement or no U.S. involvement at all in that electronic surveillance conducted by a foreign government abroad, the information may be introduced in an American court.

If there is U.S. involvement, then the basic U.S. legal standards, such as the requirement of probable cause, would apply to the surveillance and that would determine its admissibility.

Let me go on to sections 155 through 157, which are the last three provisions that the Committee asked about. Section 155 would change the FISA pen/trap standard. There's been a discussion of pen registers and trap and trace devices. They are devices that record both digits dialed but not the content of a telephone communication or the routing and addressing information of an electronic mail message, but again not the content of the electronic mail.

What this provision would do, section 155, is make the FISA pen/trap statute roughly analogous to the corresponding criminal pen/trap statute. Under current law, to obtain a FISA pen/trap order we must show almost as much as we have to show in order to get a full content, a full-blown FISA order. The result of that is, frankly, that we hardly ever use the FISA pen/trap statute. Because if we're going to go to the lengths required under the current law, we will go the extra 5 percent and get the full content order.

Our basic position here is that it is at least ironic that information that is available in a routine drug investigation or some other routine criminal investigation is not available under the same standard in an anti-terrorist or espionage investigation. The requirement that we're proposing is a relevance standard, which is what applies on the criminal side. Here it would be relevance to a counterintelligence or intelligence investigation; whether there is relevance to a criminal investigation.

Section 156 of the Administration's bill would eliminate the requirement for prior FISA court approval and expand the scope of FISA subpoenas to make them roughly analogous again to various criminal administrative subpoena provisions that already exist. Under current law, we must go to a FISA court judge or a specially designated magistrate and obtain an order to issue a subpoena that would apply only to four categories of recipients—a common carrier, a public accommodation, a physical storage facility, or a vehicle rental facility.

The amendment would remove both the requirement of advance court approval and would expand the scope of the subpoena provision to include all records, not just those in the four categories that I mentioned. The reason that we are seeking that authority is effectively both speed and efficiency and breadth.

Eliminating the requirement of advance court approval means we can get what we need quickly, with less paperwork, and the breadth would allow us to reach targets like schools, gyms—you've seen some of the newspaper reporting—dry cleaners, information that may well be critical in one of these investigations. Again this would bring into parity with existing criminal administrative subpoena authorities the FISA subpoena provision. There is authority, for example, in a routine drug case for the Attorney General not only to compel the production of documents but to compel witness testimony without any prior court involvement. He may simply issue the subpoena. That statute is 21 USC 876.

Finally, section 157 changes the standards for issuing so-called national security letters, and it changes it in two basic ways. It would allow these letters to be issued by FBI field offices rather than by headquarters officials, and it would eliminate the nexus requirement to a foreign power to make the national security letter authority more analogous to corresponding criminal authorities.

Under current law national security letter authority—and a national security letter is just what it sounds like. It's a letter issued by the FBI to either a telephone or internet service provider, a financial company or a credit company to produce documents and to keep secret the fact that they have been asked to produce documents in a foreign intelligence or counterintelligence investigation.

What our amendment would do is allow special agents in charge—that is, the top-ranking FBI field agent in each of the FBI's 56 field offices—to issue one of these letters rather than requiring the letter to be sent out by an Assistant Director at headquarters. It would eliminate the requirement of a nexus to a foreign power, leaving in place only a relevance standard.

That is roughly analogous to the standard that applies in the criminal context in a grand jury. Obviously we can't and don't use grand juries in most foreign intelligence/counterintelligence investigations, both because it is a quintessentially criminal investigative tool and because it is not really part of the grand jury's historic mission to look into counterintelligence or intelligence issues. This would give us an authority that roughly corresponds to grand jury subpoena authority, although in a more narrow class of cases, and I think would be an important contribution to our efforts to gather information quickly, especially in a case like this one.

I think that is the last of the amendments the Committee specifically asked about, so I will stop.

Chairman GRAHAM. Thank you very much, Mr. Kris.

For the information of the Committee members, questioning will be on a first-arrival basis. After the Chairman and the Vice Chair, the next questioners will be Senator Feinstein, Senator Rockefeller, Senator Wyden, Senator DeWine, Senator Edwards.

You emphasized in several areas such as sections 155 and 156 of the Attorney General's recommendations that you were attempting to render more comparable the standards under the Foreign Intelligence Surveillance Act with those that are currently in place for criminal matters. Have the analogous sections to those that you are proposing for FISA been adjudicated in their criminal context and found to be constitutional?

Mr. KRIS. I think the answer to your question is yes, but let me be more specific. With respect to pen/trap orders, the Supreme Court has squarely held in a case called *Smith* v. *Maryland* that there is no fourth amendment privacy interest in the telephone numbers that you dial or the numbers from which you receive a call. I think the reasoning of that opinion would apply equally to other kinds of routing and addressing information.

So I think with respect to pen/trap orders there is no constitutional question and there would not need to be any showing made at all to satisfy the fourth amendment.

I think administrative subpoenas have also been upheld whenever challenged, and I don't think that there is any real question about the Attorney General's ability to do that. There are a number of such statutes on the books.

Chairman GRAHAM. Recognizing that the answer to this question may involve sensitive or classified information, are you at liberty to select any of the provisions in the Attorney General's recommendations and indicate why there is this special sense of urgency that the Attorney General alluded to when he presented these to the Congress last Wednesday?

Mr. KRIS. It is difficult to answer that question in an open hearing and, of course, we are all, I am sure, available for a closed hearing where we could go into much greater detail.

If I may, let me just say something generally. The current investigation is really a sort of all-hands-on-deck approach where we do have many, many agents out there and we are doing everything that we can do under law to get the information we need to protect the public from future attack, and to give the President the information he needs to make the kinds of foreign policy and other decisions that he will have to make.

As I say, having been in SIOC when information is just coming in, the embargoes that currently exist in various places in law make it very awkward for everybody to get together and share the information. When you have an investigation this size, you need to have coordination or things begin to fall apart.

So I will say that it would be very helpful in an investigation like this one to have the sharing provisions, and I think beyond that I would defer to a closed session, with the Committee's permission.

Chairman GRAHAM. In the legislation that has been introduced, 1448, one of the provisions clarifies that the intelligence agencies would be authorized to retain so-called dirty assets without specifically directing them to do so and being sensitive to the separation of powers doctrine. Mr. McNamara, would you have any comment on the way in which 1448 deals with the issue of the authority of the CIA to hire assets with suspect backgrounds?

Mr. MCNAMARA. I think Ms. Divoll has actually laid out quite carefully and candidly what the issue is here. As you heard earlier, the reason these guidelines are in place—and I must caution that the guidelines are still classified and I'm somewhat constrained about what I can say—the reason they were put into place is because of a genuine and a serious concern that Congress had in 1994 and 1995 about the way assets, CIA assets overseas both were being recruited and were being used, and whether or not there was, for lack of a better term, adult supervision in the entire process.

What we have attempted to do or what the Agency attempted to do 6 years ago was to put in place a structure whereby both the Agency and the Committee and the Congress could be assured that somebody had looked at this to see whether or not the gain that we might be able to get offset whatever the person may have done.

I'm a little concerned about the way the statute is drafted, Mr. Chairman, although I'm sure it's unintended. It appears in the first sentence to give a case officer, a first-tour case officer, in wherever immunity from anything that may happen as a result of taking on this action. I'm not sure the intention, but the second part is it's also limited to only acquiring information, which means the officer could not direct the dirty asset, for lack of a better term, to engage in covert action, which, although the President would have authorized it, could have authorized it, to engage in any kind of disruptive activity, although clearly that's one of the things that we do should we be able to accomplish this objective.

Third, I've been the General Counsel now for almost 4 years. Either I or my senior deputy see all of these before they go to the DDO and upward. The entire purpose is to make sure that somebody else has gotten eyes on this, that people who are responsible and accountable to Congress and the American people are making a decision that does two things. It weighs in the balance whether

or not this is someone in fact that we want to have our payroll, if that's what it is, or working as an asset.

For instance, if the individual had killed Americans or if the individual had been involved in an airline hijacking or if an individual had been involved in some type of other terrorist activity, somebody needs to think about that, and a first-tour officer shouldn't be the one.

The second advantage is that it really protects the first-tour officer, or the second- or third-tour officers. So there is somebody who is saying to him, "Yes, this can be done." You can go ahead and do this. I know there's been a lot of discussion. I know former Director Woolsey firmly believes that there has been a chilling effect that has had an adverse impact. I know the Vice Chairman has been to a number of our offices overseas, as have others, and talked to officers. I have as well. I take a chance to talk to all of our first-tour officers when I'm out of the country.

All I can say is our information is different. But the bottom line, I think, is we're going to do whatever we have to do and do it right to make sure that the American people are protected. But at the same time we have to make sure we do it smartly. I don't know whether or not this would have an unintended consequence, and I'm sure that's one of the things the Committee is concerned about.

Chairman GRAHAM. Thank you, Mr. McNamara. When I read the list of questioners, I apologize. I omitted Senator Mikulski, who will come immediately after Senator DeWine.

Senator MIKULSKI. Mr. Chairman, I don't have any questions. Those were answered in the discussion. Thank you.

Chairman GRAHAM. Senator Shelby.

Vice Chairman SHELBY. Mr. Kris, does the statutory authority to conduct simultaneous title III and FISA surveillances present the same questions that section 153 does in the Attorney General's bill? In other words, isn't there a question of purpose if we are conducting simultaneous taps?

Mr. KRIS. I think the answer to that question is yes. The question of whether there is a primary or other intelligence purpose underlying FISA is a case-by-case and highly fact-intensive determination. I think in many cases at least if we were doing simultaneous title III surveillance of the same target it might play into the primary purpose calculus, yes.

Vice Chairman SHELBY. Mr. Kris, could you just briefly address the separation of powers—we alluded to this earlier—issues raised by section 103 of the Chairman's bill?

Mr. KRIS. Yes. I will do so. However, I should say that we have asked OLC again to render a more formal opinion on that. What I will say that I think raises some separation of powers concerns in my mind is something that Mr. McNamara mentioned before, and that is the "notwithstanding any other law" provision.

That suggests that even if the DCI or the President were to say to the first-year case officer don't recruit that particular dirty asset, the case officer would be authorized to do so anyway. Now I don't think—and based on what I heard earlier, I'm more confident—that that is the intent. We may have an ability to work with the staff to deal with drafting issues that we have. But I think that is

an area in which there might be—and I don't want to say that there would be—separation of powers concerns.

Vice Chairman SHELBY. Mr. Kris, what specific provisions in the Graham-Feinstein proposed legislation do you need right now in the Justice Department in order to properly prosecute the ongoing war on terrorism, from your perspective?

Mr. KRIS. Well, we are very, very happy with sections 202 and 203. Indeed, those provisions may be an example of the principle that great minds think alike, since they are quite similar to provisions we have in sections 151 and 152 of our bill. I think those are probably the two leading provisions from our perspective.

Vice Chairman SHELBY. OK. Mr. Parkinson, under section 101 of the Graham-Feinstein proposal, the DCI, I believe, would "manage" employees within the Bureau and other agencies across the community. How would you envision this working in light of their existing chains of command that we have today?

Mr. PARKINSON. Well, let me say to begin with, Senator Shelby——

Vice Chairman SHELBY. "Manage the analysis and dissemination," it says.

Mr. PARKINSON [continuing]. We do have some concern over the language that appears on page 3 of that legislation, and we would like to engage the Committee and staff in a discussion about its intent. One appearance issue is that it appears that it may—and we don't know whether this is advertent or inadvertent—put the DCI and the Agency in the domestic security arena. I think that's an important issue that we have to focus on.

Assuming we work that out and the Congress makes the judgment that an expanded role for the DCI is appropriate here in terms of how it plays out I think I am quite confident that we would work very well with the Agency, as we have, in carrying out the authorities that are given.

Vice Chairman SHELBY. Let me just share the language with you as I see it on page 3.

Establish requirements and priorities for and manage the analysis and dissemination of all foreign intelligence collected under the Foreign Intelligence Surveillance Act of 1978,

quoting the U.S. Code,

including the provision of assistance to the Attorney General in order to ensure that information derived from surveillance or physical searches under that Act is used efficiently and effectively for foreign intelligence purposes, except that the Director shall have no authority to direct, manage or undertake electronic surveillance operations pursuant to that Act unless otherwise authorized by statute or Executive order.

That's what we're talking about here.

Mr. PARKINSON. That's correct.

Vice Chairman SHELBY. All right. Thank you, Mr. Chairman. My time is up.

Chairman GRAHAM. Thank you very much, Senator.

Senator Feinstein.

Senator FEINSTEIN. Thanks very much, Mr. Chairman.

Mr. Kris, I think your testimony was very helpful and I want to thank you. I also think it was very powerful in one way because it really is the first time the Department has officially admitted

that the communication issue is truly an issue and, as you just said, less than ideal.

One of the problems I think working in this area is people will say to you one thing formally and they'll say another thing informally, so how you really know becomes sometimes a difficult task. But I think you have clarified what we believe, based not on something people said, because it's always been denied—oh, there's no problem in intelligence-sharing—when in fact we believe there is. So I want to thank you for that.

I wanted to ask you a question on section 151, if I might. This is the period of orders of electronic surveillance of non-U.S. persons under foreign intelligence surveillance. Is that there largely just because of the jurisdiction of this Committee being that if you had U.S. citizens covered under this it would come under the jurisdiction of another Committee? Because I have a hard time knowing why. I mean, we know there are cells operating in this country. It may even be that the U.S. citizens are participating in those cells or people here legally. As a matter of fact, it's very likely.

So the question is why not give this authority across the board?

Mr. KRIS. OK. Before I answer that question, let me just respond to what you said earlier.

Senator FEINSTEIN. You're not going to take it back, are you?

Mr. KRIS. I don't want to give myself more credit than I'm due. If Senator Thompson were here he could tell you. He recently commissioned a GAO report which does discuss some of the long-term issues we've had with information-sharing, and we then wrote a letter in response to the report. So I don't want to give myself more than I deserve.

With respect to section 151, I don't think that—I mean, I can tell you that the thinking behind section 151 has nothing to do with which committee would evaluate it, and frankly that's well beyond my ken. The concern, though, or the reason for limiting the 1-year authorization period is part of our overall approach here, which is to try to be balanced, to push the envelope and give ourselves more authority where we really need it, but to be sensitive also to the civil liberties and privacy concerns that this kind of surveillance will go against.

We are really trying to get the authority where we need it most. This provision does not enlarge or change the targets that we can surveil. It only allows for longer periods. That, we have found, is a significant issue primarily for non-U.S. persons, especially—and I want to be careful in an open hearing of exactly what I say—for employees or agents of foreign powers who are often here for long periods of time. That's really the motivation here—respect for U.S. person civil liberties, which we think are especially important, and there is a difference between surveilling non-U.S. persons and surveilling U.S. persons, but also to focus on exactly what our need really is.

I think our need is greatest with respect to non-U.S. persons. For U.S. persons we can still get the surveillance, but we'll have to come back every 90 days and have a judge keep looking at it.

Senator FEINSTEIN. In this situation you want to do that.

Mr. KRIS. Yes.

Senator FEINSTEIN. OK. I would think about that. But, in any event, let me go on to section 153. This section clarifies that the certification of a FISA request is supportable where foreign intelligence-gathering is "a purpose" of the investigation. It would eliminate the need continually to evaluate the relative weight of criminal and intelligence purposes and would facilitate the information-sharing between agencies.

Now, I am told that the primary purpose test has often been cited as one of the reasons that FISA meets the constitutional requirements under the fourth amendment. Would elimination of this test place the entire FISA in danger of being struck down by a court?

Mr. KRIS. The answer to your question I think is no, and again I'm relying here on the analysis of our experts in the Office of Legal Counsel. Let me try to explain in particular with respect to the risk to the whole statute.

Courts will occasionally evaluate constitutional challenges on an as-applied basis, where you deal with only the particular case, or on a facial basis, where you evaluate the statute in general. What we would definitely not like to see is an amendment to FISA that led to a facial attack and a successful facial attack on the statute, which would throw the entire statute out on constitutional grounds.

We are confident that changing "the purpose" to "a purpose" will not permit a facial challenge to FISA. Because of the way courts evaluate these things, we are confident that under existing jurisprudence they will evaluate this on a case-by-case basis. There is a case, *United States* v. *Salerno,* that stands for the proposition that if a statute is valid in some applications, as the "a purpose" standard clearly would be, there is no justification for striking down the statute on its face. Instead, courts deal with the challenges on a case-by-case basis.

I think there is a possibility, if we go too far in a particular case, that we would end up being suppressed in a subsequent attempt to introduce the evidence in court. But we think that's a risk that's worth taking in order to solve this problem that we've discussed about information-sharing. But I emphasize our experts—and I agree—think that the statute is not in jeopardy on its face.

I've been reminded and I think I mentioned this before, we will be sending a letter to Congress that sort of details at great length our constitutional reasoning and the reason for the statement I've just made to you.

Senator FEINSTEIN. Thank you very much. Thanks, Mr. Chairman.

Chairman GRAHAM. Thank you, Senator.

Senator Rockefeller.

Senator ROCKEFELLER. Thank you, Mr. Chairman.

I just want to go back to the so-called less-than-desirable factor, the chilling effect, so to speak, of CIA and potential human rights violations. If this were carried forward and it were lifted, as I happen to favor, and there was not the high-level approval every single time, is that done in part—does that put in jeopardy in a way for the case officer, let's say, on the ground in a country for the possi-

bility of an asset committing an act of terrorism on the United States, in other words putting that person at risk?

I put that in this context. The answer that I got when I previously put this forward was, "Well, we really don't have that many requests." That strikes me as a little bit of a pre-September 11 type of answer and that if there's anything which has been on the public airwaves in the last several weeks it's been the need for a much greater body of human intelligence, not all of which, I guess, can be of the most attractive sort.

So in a sense I'd like to know is the idea of not doing this to protect the case officer, making the approval come from a higher level in case the person turns nasty toward the United States?

Mr. MCNAMARA. Senator, I think it actually has multiple purposes. One is to protect the officer. Especially a first-tour officer shouldn't be going out there and making a determination to bring on somebody and pay him and use him as an asset without ever even telling the chief of station. But, more importantly, many times the individual officers—and in fact just for the record, the way this is drafted it's not just a CIA case officer who actually knows tradecraft. It is anybody who is a member of the Intelligence Community, the way it's drafted now.

So somebody from NRO who has never done this could actually, according to the way it's drafted, be running assets that we wouldn't know anything about.

The purpose is multiple. No. 1, is to protect the case officer. No. 2, is to make sure we're doing the right thing. No. 3, is to bring it back and make sure we run it against our data bases and traces. Is there something else we know about him or her? Have they been involved in something we're looking for? Is there an outstanding U.S. warrant for this individual? There are a number of things where you just really need headquarters to be aware of.

I think, more importantly, this Committee should be insisting that we be accountable, the senior intelligence officers at the CIA be accountable before somebody does something like this. This is not slowing the process down, I don't think. As I said, I've only been there 4 years and these can be done very, very quickly.

PDD–35 comes out and lays out everything that we're targeting. The chiefs of station are pushing at their people to try and find people who can penetrate these. They are very, very hard to do. Not only do they not like us, in many cases they hate us and will not work with us. The opportunity to get somebody who will do something for us, even to the extent of giving us some information, would be a career-enhancing opportunity and not a career-limiting event.

Senator ROCKEFELLER. It's not a question of congressional second-guessing which worries you on this. It's simply what you spoke about?

Mr. MCNAMARA. No, sir. I don't have any problem with congressional oversight. In fact, I think in many cases this would enhance congressional oversight. We have come to the Committee to tell them what we are doing when we're bringing dirty assets in. We wouldn't be able to do that. I think this Committee should know what we're doing.

Senator ROCKEFELLER. OK. The whole concept of the virtual language capacity is a very, very interesting one to me and I think is a very strong part of the Graham-Feinstein amendment. Now as I think Senator Graham indicated in his press conference, it's aimed at Arabic, Farsi, Urdu or maybe not Farsi but Pashto. But it's for the whole panoply of languages.

That has been a concern of mine in any event in terms of the capability, and I've frequently referred to the fact that Mormons are doing many of our best language work. We are not teaching any longer in our schools. America is in a sense withdrawing from the world. Now that could have changed very dramatically, probably will have since September 11 in terms of things like teaching languages.

But it strikes me as a very, very powerful initiative and one that I think we ought to undertake.

Mr. MCNAMARA. Senator, I think you're right. What the Chairman and Senator Feinstein have put together is a very novel and intriguing idea. My only concern or our concern from the Intelligence Community is there are a number of counterintelligence issues this raises, No. 1. No. 2, there are a lot of security problems. The issues of connectivity in and of itself are something that we are trying to deal with within the community, that we've already tried to approach.

The cost could be absolutely prohibitive. I'm just wondering whether or not on a short-term basis we can actually look at this with the Committee and study its ramifications to see whether or not this is the framework you want to put into a statutory construction. The difficulty is that once it's etched in concrete as a statute and a requirement, we don't have the flexibility that I think you and Mr. Cash were talking about earlier on when he mentioned it in terms of what that capability is.

But our translators are different than FBI translators. Our requirements are different than the FBI translators. Protection of classified information is different. The difficulty is it should not be paralytic. On the other hand, what it should be is something that is done in a way that both is effective and efficient and quick and gets it turned around.

I don't know—and on behalf of the community—I don't know if this is exactly the right paradigm, but what we'd like to do is experiment and see what we can come up with and then maybe come back to you and say, "Here's some of the other options." Would this satisfy it?

Senator ROCKEFELLER. That's fair enough. But you wouldn't disagree that there has to be a sharp increase in our capacity.

Mr. MCNAMARA. Absolutely agree.

Senator ROCKEFELLER. Thank you, Mr. Chairman.

Chairman GRAHAM. Thank you, Senator.

Senator DeWine.

Senator DEWINE. Thank you, Mr. Chairman.

Mr. Kris, let me first say that I think the Attorney General has come forward with some very, very positive proposals. Some of these have been made in the past and Congress has not acted upon them. I hope that now, with this situation that we are in and the tragedy of September 11, we will. I think also that the Chairman's

proposal has many, many very positive things in there, and I would congratulate you, Mr. Chairman, on that as well.

I don't want to beat a horse that's going to be going around a few more times beyond today, but I want to come back, if I could, to section 153. I understand your explanation and if we do pass this I guess I hope you're right that you are lucky enough and we're all lucky enough to do it on a case-by-case basis. I'm not sure you're right.

I'm not even sure, though, if it's on a case-by-case basis that's what we want. It seems like to me that's going to be a real mess and there are going to be some real problems for us as a country.

As you know, the case that really is kind of the intellectual underpinning of the FISA statute was *United States* v. *U.S. District Court*, or the Keith case. When you read that, as I know you have and the counsel has, it's very, very clear that what the Supreme Court of the United States was saying is there are apples and oranges, and when you're dealing with a criminal it's one thing, and when you're dealing with national security it's something else and we're going to treat them differently and the standards are going to be different. The Court elaborates in four or five different ways what the differences are.

The statute today, as you know, talks about "the purpose." That I suppose, it seems to me, is pretty much interpreted as "the primary purpose." We might be able to get by with "a primary purpose," maybe. But I think when you get to "a purpose" I just think what does that mean—2 percent of what you're trying to do is national security and 98 percent is criminal? Where do you draw the line?

I just think we're getting into some real, real problems. I'm very sympathetic with what you're trying to do. I just wanted to make that statement.

I want you to explain to me, though, one more time what this gets you. What does it get us in national security? I'm missing it. I really understand the problem about sharing information. I understand about the artificial walls. I understand the reason we have to have more cooperation. A lot of what's in the Chairman's bill and a lot of what's in Attorney General Ashcroft's bill goes to that. I have a couple of provisions I want to add that I think will help in that area, and I won't get into them today.

Explain to me, though, what the change in the statute does to accomplish the breaking down of those walls and the sharing of that information, because it seems like it's going the wrong way to me on the information. But maybe I'm missing something.

Mr. KRIS. Well, with respect to the purpose inquiry that is conducted both by the FISA Court in the case of a U.S. person when it evaluates the certification of the purpose of the sought electronic surveillance or search and a District Court if under FISA it evaluates a motion to suppress, I think the analysis has focused concretely on two things—first the flow of information from the intelligence side to the criminal side and, second, the advice that goes back from the criminal side to the intelligence side.

Senator DEWINE. OK. I'm with you so far.

Mr. KRIS. So, to give you a hypothetical example, if prosecutors start telling counterintelligence investigators, "Hey, you're up on

Joe Jones", you should probably go up on his brother Fred because he's involved in money-laundering, it's not a crime that affects national security but we would really like to get some good surveillance on Fred, that advice-giving can alter the perceived purpose of the surveillance of Fred because it is being driven by or it is perceived to be being driven by criminal equities and a criminal purpose.

The concern that we have, therefore, is to allow just the right amount of information-sharing and advice-giving but not too much, so that we don't cross the line, the purpose line, and end up in a bad situation where we are either conducting or attempting to conduct unauthorized surveillance or, if the FISA Court agrees with us but a District Court later disagrees, we end up suppressed in a criminal case.

Senator DEWINE. OK. Give me another example, because I really didn't understand that one, or do it again—if the Chairman will indulge me just a minute—because I think this is very important. We have to understand the situation. You're going in to get a FISA and the factual case you have to create is a case where it's not "the purpose." It's much less than that, because that's why you're making the change. You're going from "the" purpose to "a" purpose.

So now we're down to you've got a lot of other reasons out there that you want a FISA, but one of them is, "a" purpose, national security.

Mr. KRIS. OK.

Senator DEWINE. Because that's the factual situation that your change in the statute leads me to. With me so far?

Mr. KRIS. I think I understand you.

Senator DEWINE. OK. Now create the case. Tell me the case where it's just a portion of really what I want to do.

Mr. KRIS. OK. I think that issue comes up in a number of both terrorism and espionage cases because terrorism and espionage are, by their nature, both counterintelligence concerns—we want to stop spies from stealing our secrets and passing them to foreign governments—and, because of the way the criminal law is today, they are Federal crimes. We see that in the prosecution of Robert Hanssen or Brian Regan or Ana Montes.

What you face inevitably in a case like that, both in espionage cases and in terrorism cases, is an inquiry that's being conducted by courts into sort of what is driving this surveillance or search. Is it the desire to gather evidence so that we can successfully prosecute this person and lock them up, or is it instead the non-law enforcement concern about stopping espionage and preventing further harm or what have you.

Now there is an argument that prosecution of spies and terrorists is just one more counterintelligence tool, one more protective measure. By surveilling them we can recruit them, double them, we can cut them off from access to classified information, we can PNG their handlers, or possibly prosecute them. But that argument would be, I think, new.

So the basic concern is that in these cases there is the possibility of criminal prosecution and the concern is that that not be the driving force behind the surveillance.

Senator DEWINE. Mr. Chairman, I've gone too long and I apologize. I thank the Chair for your indulgence.

Let me just say to our witnesses today I appreciate the testimony very much. I'm going to explore this a little more because I'm not, contrary maybe to what I said, I'm open. I'm willing to listen. If there's a compelling reason to do this, maybe we should do it. I guess I just don't get it yet. So I'm going to explore it a little more. I appreciate it.

Mr. KRIS. We're at your disposal.

Senator DEWINE. Thank you.

Chairman GRAHAM. Senator Wyden.

Senator WYDEN. Thank you, Mr. Chairman.

I'd like to ask you, Mr. Kris, if I could, about electronic surveillance and particularly how the Administration sees drawing the line between what constitutes lawful online activity and matters that we ought to be concerned about, such as criminal hacking from abroad.

Section 201 is trying to define criminal hacking, and clearly this is going to be an issue for the Congress. How would you define it?

Mr. KRIS. It's a difficult term to define. We take a run at it on the criminal side in section 106 of our bill and, if you'll permit me, I'll turn to that provision.

We define hacking in terms of trespass and if you are a trespasser into a computer then effectively that is the core of the hacking definition that we have in section 106. I want to say that this is—and I'm happy to respond—I want to say that this is not one of the sections identified and it is not really within my personal area of expertise. This is a criminal law provision here. But that is the gist of what we are doing in section 106.

I think the section 201 provision, as I understand it, is motivated by a similar concern. I think it's intriguing notion on the FISA side to take out hacking from the definition of FISA electronic surveillance. I think that's one that we would like to sit down with not only our interagency process in the Intelligence Community but also with the staff to sort of work to see if we can ensure that we're doing exactly what we want to do and nothing more.

Senator WYDEN. Let me, if I might, change the subject to the question of biological and chemical and radioactive materials. Your bill has a provision that makes it unlawful to possess a variety of materials—biological agents and a host of other areas that are essentially health-related. What do you think the major vulnerabilities are now in this area and how would your bill address it?

Mr. KRIS. Again I have to sort of apologize, Senator. That is not one of the provisions that was identified to us by the Chairman in advance of the hearing, and I am really very reluctant to set out into an explanation of something that I am not really prepared to discuss. We can certainly get back to you with the right people on that, but I don't think I am.

Chairman GRAHAM. Senator Wyden, I asked the General Counsel to screen the Attorney General's recommendations for purposes of identifying which of his recommendations were in the jurisdiction of our Committee, and it was only those that we submitted to Mr. Kris and asked him to be prepared to comment on today.

Senator WYDEN. So we can't get an answer out of any of the people at the table.

Suffice it to say this is what my constituents are asking about today, and this is in the Justice Department's bill. I certainly respect you, Senator Graham, if they are not prepared to talk about it, but clearly there are statutes and regulations that apply to the possession of chemical agents and toxins and biological agents, and I hope we'll talk about it down the road.

Mr. PARKINSON. Just quickly, Senator Wyden, I assume you're referring to section 305 of the Administration's bill, and while we didn't come necessarily prepared to talk about that, that section does enhance the number of offenses in the biological weapons arena. It adds subsections to existing statute 175 to include additional offenses of possessing biological agents and toxins, and then it has a section about select agents within the jurisdiction of the Health and Human Services Department.

The intent and the goal of those sections is to make sure that biological agents or toxins are only in the hands of authorized personnel, and it does two things. It establishes a new regulatory regime within the purview of HHS and it also adds a couple of new offenses to address it on the law enforcement side.

Senator WYDEN. Are there vulnerabilities that you can discuss this afternoon that make the need for those improvements necessary?

Mr. PARKINSON. There certainly are vulnerabilities. I can't comment about imminent vulnerabilities, but certainly at a larger level we and the Department and the Intelligence Community have been focused on biological and chemical weapons as a priority for several years now. I think that there's no question there are vulnerabilities, and this provision, section 305, is one attempt to deal with it both on the law enforcement side and the regulatory side.

Senator WYDEN. Mr. Chairman, obviously this is not a day to get into as much detail as we might in this area, but I hope we will turn to it, because this is something I am getting asked a great deal about, and it is in the Justice Department's bill and we're going to be anxious to talk to you.

Thank you.

Chairman GRAHAM. Senator Edwards and then Senator Kyl.

Senator EDWARDS. Thank you, Mr. Chairman.

Mr. Kris, you were probably here when I asked Ms. Divoll some questions about the differences between the Administration proposals and the provisions of the bill. Let me say first of all that I spent part of Saturday in Charlotte with our FBI officials in North Carolina, and their overwhelming message to me was we have to bring these FISA procedures up to being able to deal with what we're confronted with technologically today.

I understand the concern and I am with you. I want to make this work. But I also share some of the concerns that others have expressed and I expressed earlier. Let me just talk about it briefly and then get you to respond if I can.

If I understand it correctly, the fundamental premise on which FISA is based is that, unlike a title III wiretap, because it's a foreign intelligence-gathering operation, it's not required to meet some of the constitutional standards—for example, probable cause re-

quirements. At least that's not been required in the statute. You can comment on that if you would.

But that of underlying premise has been critical in the analysis of why this legislation has to date been constitutional. Now the change from "the" to "a" of course is a huge change in terms of the law. It may not sound like much, but in terms of the law it's an enormous change. That change means that the primary purpose of the investigation could in fact be criminal, as long as a purpose was foreign intelligence-gathering. So I have multiple concerns, one of which you've already addressed.

I was concerned about the possibility that somewhere down the road the U.S. Supreme Court may declare the statute facially unconstitutional. You've talked about that some. I'd like to hear more about that because I continue to have concerns about that. But I understand your reasoning about that.

Second, the possibility that a conviction may be overturned or also that information gathered as a result of a FISA application may not be allowed into evidence, suppressed by the court, and, I might add, I think it goes further than that. It seems to me that it creates the possibility that not only that particular FISA would be suppressed but that others within the same class would be found to be unconstitutional as applied. Therefore you have a problem not just in the individual case, which I know you've talked about some here today, but you could have a declaration by a Federal district court somewhere in the country that could have implications for ongoing FISAs, for FISAs that are similar and fall within the same class, and as a result would have much broader implications. So I'd be concerned about that.

I might add I know from having looked at the Supreme Court cases the Supreme Court has taken a particular interest, I think, in the last couple of years in this specific issue, not dealing with FISA but what the primary purpose of the search was. So that's a concern I have.

Then finally I know that the U.S. Supreme Court has historically—you've talked about the fact that we're going to have the courts deal with this on a case-by-case basis. The U.S. Supreme Court has traditionally, in issues of foreign intelligence-gathering, showed deference to Congress, and properly so. I agree with that. But they showed deference to Congress. I just wonder from your perspective whether it would not be some abdication of our responsibility to say, "Well, we're going to leave this issue to the courts on a case-by-case basis, where the courts are very likely to say or very possibly could say this is an area of foreign policy, this is an area of foreign intelligence-gathering, this is an area traditionally left to Congress."

That being the case, who has the responsibility for deciding whether in fact this is appropriate and constitutional?

Just one last notion. Instead of changing the statute, suppose we said—and this is nothing but an idea—you expressed concern about having to constantly evaluate whether the primary purpose was a criminal investigation or the primary purpose was foreign intelligence-gathering. That makes sense to me. I can see that.

But instead of changing the language of the statute, which might potentially create more problems than it cures, suppose we said that in your initial application you are required to show that the primary purpose was the FISA requirement that exists now—foreign intelligence-gathering—but at some point down the road if it changed, when you come up for renewal you wouldn't have to make that showing again. In other words, it only has to be shown in the initial application.

I'm sorry. I went on too long. But if you could respond I would appreciate it.

Mr. KRIS. It's a tall order to cover all of that. I'll do my best. First, with respect to the probable cause issue that you raised, as a technical matter FISA does require a showing of probable cause, but it is of a different thing. In the criminal context it's probable cause that a crime has been committed; here it is probable cause that the target is an agent of a foreign power. But I take your larger point about the difference in standards.

I guess, responding to the other point about how this would play out in a suppression situation, the first thing I guess I should say is I don't think that even under the current regime and under any possible regime we can avoid making case-by-case determinations. Whether it be a primary purpose inquiry, a purpose inquiry, or any other inquiry, we are and have to examine each one of these applications not only because I think they are going to be evaluated on a case-by-case basis but because the certification from the Director of the FBI and the approval of the Attorney General is made on a specific case-by-case basis. One of the safeguards of FISA is that it requires that high-level involvement.

Also, I don't know if this has been made clear, but I think the FISA Court, in evaluating FISA applications, would be entitled, and OLC is of this view as well, to evaluate the constitutionality of an application ex ante. So we would not just be in a situation where we're rolling the dice and taking our chances in district court.

Senator EDWARDS. The evaluation would take place on the front end, is what you're saying.

Mr. KRIS. Yes, exactly.

As to the sort of derivative suppression, that is a fairly complex body of fourth amendment law about when, assuming an initial constitutional violations, the fruits of that violation taint subsequent searches. That has got to be evaluated also on a case-by-case basis. But I acknowledge the issue.

With respect to the deference and the delegation issue, I would like to think that the courts have recognized Executive authority and have paid deference to Executive determinations in the area of foreign intelligence, and indeed I think that's reflected in FISA. When the DCI or the Director of the Bureau makes a certification as to purpose, the FISA Court by statute is required, even in the case of a U.S. person—and district courts I think would operate under the same standard—to review the certification only for clear error. So there is a built-in deference mechanism where if the DCI or the Director of the Bureau makes a certification, it is to be upheld unless it is clearly erroneous, which is a fairly generous standard of review.

I think that deference, even if not in that precise form, would continue to apply regardless of how the statute is amended and indeed even if there were no statute.

Finally, I guess with respect to the initial application idea I guess I think that if we are going to allow a lower standard than primary purpose in second and subsequent applications I'm not sure that will do the trick for us. I'm not sure it will solve the problem, I guess more importantly, because we will be up on multiple renewals and if after the second one we are dropping down I think we will face a lot of the same concerns that you have. That's sort of a idea that I would want to give a little more thought.

Senator EDWARDS. I've taken too much time already. Thank you for that response. Let me just make clear I want to work with you. I want to make this work. We appreciate the work you're doing. I know first-hand from my folks that what you're proposing is of critical importance. We just need to be sure that it's going to do what we want it to do.

Mr. KRIS. Yes, sir. Thank you.

Chairman GRAHAM. Thank you, Senator Edwards.

Senator Kyl.

Senator KYL. Thank you, Mr. Chairman. I have three specific questions, if I could.

The first is a situation in which at least it's my understanding that FISA actually presents a tougher standard than generally. This has to do with the—well, the best example is the trap and trace or the pen registers that the U.S. Supreme Court has held in the regular context do not present a constitutional expectation of privacy or constitutional issue, with respect to just the existence of the call or the numbers themselves and so on. Yet under FISA the mere existence of the call or the data exchange is termed a communication and must be protected from electronic surveillance.

Why is that so? Why isn't that being suggested for change? Question No. 1.

Question No. 2, is it the fact that FISA does only apply to non-U.S. citizens? Once somebody is identified as meeting the criteria agent of a foreign power or terrorist group and so on, then why should citizenship constitutionally make a difference here? Why should there be a higher standard?

Finally, I wasn't here when you answered Senator Shelby's question, Mr. Kris, but I understand from staff that you expressed a concern about section 204, and I just wondered whether you could go into greater detail on the problems associated with section 204 requiring the Government to meet both title III and FISA standards.

Mr. KRIS. Yes, sir. With respect to the first question concerning pen/trap authority, there is a proposal in the Administration's bill—section 155—that would lower the standard for FISA pen/trap orders to make them roughly analogous to the standard for criminal pen-trap orders. You are right. Under *Smith* v. *Maryland* there is no fourth amendment privacy interest in pen/trap information, and the standard in criminal cases is a certification from the applicant that the information sought is relevant to a criminal investigation.

We're seeking a standard in FISA that would require a similar certification that the information sought is relevant to a counterintelligence investigation. So that would be our section 155.

With respect to FISA and U.S. citizens, U.S. citizens may be FISA targets if they are agents of a foreign power as defined by statute, and the statute contains two definitions of agent of a foreign power. The first applies to any person other than a U.S. person, and the statute defines a U.S. person to be a citizen or a permanent resident alien. So that could apply either to U.S. citizens or foreign persons. Then a second provision that defines the term for U.S. persons. It has a slightly higher standard—I may have misspoken. I want to make sure I get it clearly.

There is a provision that applies to anyone other than a U.S. person, so only to foreigners, and then another provision that applies both to U.S. persons and foreigners. So a U.S. person, a U.S. citizen, can be an agent of a foreign power if they meet the statutory requirements.

Finally, with respect to——

Senator KYL. On that, I mentioned the terrorist group. Does a terrorist organization fit within the foreign power such as to include for our purposes here today that definition?

Mr. KRIS [continuing]. Yes. Under 1801(a) of title 50, subsection (4), a group engaged in international terrorism—and that is itself a defined term—is a foreign power, and a U.S. person can be an agent of an international terrorist group just as a non-U.S. person can under slightly different standards. So it does cover a U.S. citizen who is a member of a terrorist organization and acts to further the goals of that organization.

With respect to section 204, as I understand it, I think the gist of section 204 is to allow simultaneous title III and FISA surveillance of the same target. I guess the concerns I have about that provision—well, let me back up and just say this. I think it is a good idea to make clear—and we have a provision in here that does so—that FISA governs FISA, pen/trap governs pen/trap, title III governs title III.

Doing them simultaneously I think raises two concerns for us. The first is that under the purpose analysis that's been discussed quite a bit today I think when we start using criminal authorities to get surveillance on a FISA target we muddy the water. We raise an issue there. I think second, and this is maybe more pressing, title III does not contain the special secrecy provisions that FISA contains. In a FISA case if there is a motion to suppress it's handled ex parte and in camera so that the defendant doesn't get access to the application that led to the surveillance. That's critical to protect our sources and methods. The same is not true in title III.

So if we were to go up title III on some of these targets we would risk exposing our sources and methods. That's why we actually use FISA for most of these targets.

Senator KYL. Thank you very much.

Chairman GRAHAM. Senator Shelby.

Vice Chairman SHELBY. Mr. Chairman, I'll try to follow up on what Senator Kyl's talking about in a sense.

Mr. Kris, section 105 of the Ashcroft proposals, as I understand it, would allow U.S. prosecutors to use against U.S. persons, information obtained by foreign government wiretaps overseas as long as U.S. intelligence or law enforcement personnel were not involved in the surveillance. Is that right?

Mr. KRIS. Yes, sir, that is correct.

Vice Chairman SHELBY. How do you envision the government establishing at trial that no employee of the U.S. Government was involved in the foreign surveillance? That might be tough. It might not be. I don't know.

Mr. KRIS. I think it might depend on the case. I can, just sitting here, sort—it's been a while since I was a trial lawyer, but I can think of a couple ways. One is we might be able to call or obtain evidence from the foreign official who conducted the wire and have the appropriate official over there, wherever it may be, make a certification, or I think there are authorities for depositions of foreign witnesses. I don't want to overstate it because I'm not intimately familiar with those. But I think there is a mechanism for obtaining evidence from a foreign government official.

The other way I guess would be to do it from the U.S. side. The difficulty I guess I see there is it could be anybody.

Vice Chairman SHELBY. Certification would be hearsay, wouldn't it, in a sense, unless there's an exception to it.

Mr. KRIS. I think—and Larry you may have more detail on it—there is a method of getting information from foreign government officials into evidence in an American court.

Vice Chairman SHELBY. Could you furnish that for the Committee?

Mr. KRIS. I would be happy to do that.

Mr. PARKINSON. I would say, Senator Shelby, an analogous situation arose in the African bombing prosecutions in New York. It was not electronic surveillance but the circumstances surrounding a statement given by one of the defendants while in foreign custody was a significant issue. At the end of the day in pretrial suppression hearings the prosecutor, who was the primary prosecutor on the case, actually testified about all the circumstances and what kinds of contact we had with the foreign government. So it was fully explored during pretrial proceedings. It actually worked reasonably well.

Vice Chairman SHELBY. And it came in?

Mr. PARKINSON. Well, yes, eventually the statement came in. The judge ruled that under the circumstances it was admissible.

Vice Chairman SHELBY. I'm just raising the question. I think it should be raised.

Thank you, Mr. Chairman.

Chairman GRAHAM. Thank you very much, Senator. I wish to extend my appreciation to this panel for an excellent and I imagine not the last time that we'll be discussing these matters with you. I appreciate the comments that I believe all three of you have made that it would probably be an appropriate next step for your offices and our staff to continue to pursue some of the issues raised here.

My goal is to achieve a blending of what the Attorney General has recommended and what we had been developing prior to Sep-

tember 11 so that we can present as the intelligence component of what is likely to be a larger piece of legislation a piece of legislation, multiple sections, that had as high a degree of consensus as possible.

I think the question that Senator Wyden raised underscores that we aren't the only place that this issue is going on. As you mentioned, Mr. Kris, the reason that maybe you're here instead of the Attorney General is that he's testifying before a Judiciary Committee, which has jurisdiction over a number of other of the Attorney General's proposals, particularly those that are more of a criminal rather than an intelligence orientation.

So we've got a lot of work to do, with a sense of urgency to get on with it. I appreciate your contributions to our progress in understanding and appreciating the Attorney General's proposals as well as your comments on those that we have made.

Mr. MCNAMARA. Thank you again for your leadership, Mr. Chairman.

Mr. KRIS. Thank you, Mr. Chairman.

Chairman GRAHAM. The second panel—and I appreciate your patience and perseverance—is comprised of Mr. Jeff Smith, former General Counsel to the Senate Armed Services Committee and former General Counsel to the CIA, and now a partner of the law firm of Arnold and Porter; Ms. Kate Martin, director of the Center for National Security Studies; and Mr. Jerry Berman, executive director, Center for Democracy and Technology.

Thank you very much to all three of you. Again, I appreciate your willingness to testify on short notice and about this important and complex set of legislative proposals.

Mr. Smith.

[The prepared statement of Mr. Smith follows:]

PREPARED STATEMENT OF JEFFREY H. SMITH

Mr. Chairman, it is an honor to appear before you this afternoon to discuss these issues of great national importance.

You have asked me to discuss my views on how the United States should respond to this attack, particularly from an intelligence and law enforcement perspective. You have also asked for my views on the legislation pending before the Senate, particularly on those issues for which this Committee has jurisdiction.

It is a special privilege for me to appear before this Committee, because I was honored to be a member of its staff for nearly 5 years. Mr. Chairman, Mr. Vice Chairman, I commend you for your leadership over the years, particularly in this extraordinarily difficult and demand time. I am sure this Committee and the Congress will play a great role in leading this Nation to victory.

Let me also add, Mr. Chairman, a note of commendation to the truly extraordinary efforts being made by the men and women of the U.S. Intelligence Community. They are working around the clock in an unprecedented effort of dedication and determination to find out who attacked us, prevent future attacks, and support the U.S. diplomatic, military, law enforcement and intelligence response that is forthcoming. In particular, I know that George Tenet has put his heart and soul in this effort, and he deserves the nation's thanks.

OVERVIEW

Not long ago, there was much talk that we were headed toward a borderless world. Many believed that such factors as the revolution in information technology would render borders meaningless. Some even questioned the future of State sovereignty, although others asserted that the State would survive and remain the principal actor in international politics.

The increased flow of capital, goods, people, technology, and ideas across borders has brought much to many of the world community. However, as the President has

stated, those who stand to lose from such trends have lashed out in irrational fear at the freedom, progress and prosperity the rest of the world enjoys. These forces of fear have woven a network across many borders of like-minded individuals, organizations and governments to declare war on us and our allies.

The very nature of this international network presents us with unique challenges for which we must find new and innovative responses. This threat comes at us from many directions and in many guises, and we must be prepared to respond on an equally broad front.

The terrorists have created their own borderless world, and it is therefore ironic—and most appropriate—that President Bush has called upon all states to enforce the most basic rules of international law: namely, that states must exercise governmental authority within their defined borders. President Bush has rightly demanded that every State abide by the rule of law by rooting out terrorists on its territory or cooperating with us in doing so. Indeed, all states have a common interest in defeating these forces of terror and fear because these forces can turn on other states as surely as they have turned on us.

How then, should the United States respond? In my opinion, five principles should govern our response.

First, because this is a seamless, borderless attack we cannot have artificial seams or borders in our responses. In the past, we have approached terrorists acts by asking whether a particular act is a law enforcement, intelligence, or national security matter. That question must no longer be the first question. We must be able to collect and analyze *information*; then sort out later whether it's "evidence" or "intelligence."

We must see this as an integrated threat for which we must have a single, integrated response. There should be no artificial "stove pipes" in our responses. By that I mean we must have, as the armed services do, a "joint" response. For many years now, the Department of Defense has worked very hard to create joint organizations that will fight jointly. The same must be true not just within our military but across the government.

This is easier said than done, but the President took a major step in this direction by appointing Governor Ridge as the cabinet-level coordinator for homeland security. The contours of his responsibility are not entirely clear at this point, but consideration should be given to a "civilian CINC" who would be responsible for coordinating the U.S. war on terrorists. Much as the Goldwater-Nichols Defense Reorganization Act of l986 gave increased authority to our CINCs overseas, a civilian CINC for counter-terrorism could pull together all of the various elements to respond to the war. Perhaps, like a military CINC, the various agencies should assign "forces" to him for the fight. President Bush may have intended that Governor Ridge function in this manner. In any event, I believe we need to continue to work very hard to resolve the organizational issues.

Second, our laws and regulations must be reviewed to assure that they do not foster the stovepipes that have caused so many problems in the past. For example, we know that government agencies do not share information as efficiently or as quickly as they should. In some instances, current law prevents such information-sharing. Those laws should be reviewed and changed as appropriate to foster effective information-sharing. I am pleased to see that many of the specific proposals before Congress make those changes.

In addition to legal requirements, attitudes and traditional rivalries continue to impair information-sharing. Nevertheless, it has been my experience that when U.S. officials are given a particular mission, they roll up their sleeves, share the information and get the job done. I am sure that is what has happened after this attack. It is now up to Congress to eliminate unnecessary impediments in the law that clog the machinery of government. The executive branch, too, must reduce or eliminate unnecessary constraints on the sharing of information.

At the same time, we must recognize that many of these rules, such as grand jury secrecy, were enacted to protect the rights of our citizens. We must find a way to accommodate the Intelligence Community's needs without impairing the rights of U.S. citizens.

Third, we must be as aggressive as our Constitution will permit. For example, we should examine whether the standards for conducting electronic surveillance of non-U.S. citizens within the United States to acquire foreign intelligence should be changed. Yesterday's *Washington Post* reports (p. A18) that the FBI wanted to initiate electronic surveillance against some of Osama Bin Laden's non-U.S. person associates in the United States prior to the attack but the Justice Department did not believe there was adequate authority under FISA to obtain a wiretap. If that's true, we should change the law.

The basic concept underlying FISA is that a warrant is required to approve electronic surveillance to collect foreign intelligence in the United States—but that a somewhat lower standard is appropriate than for criminal purposes. FISA also distinguishes between U.S. persons and non-U.S. persons and it is, in theory, easier to obtain a warrant to collect against non-U.S. persons than U.S. persons.

I have not had time to review the recent case law on surveillance of non-U.S. persons. But I am generally aware that courts have, over time, extended more Fourth Amendment protections to non-U.S. persons. I suspect, however, that most if not all of those cases are criminal cases. I believe, therefore, that Congress should take a hard look at the standards in FISA for conducting surveillance of non-U.S. persons and consider easing the standards for obtaining warrants for electronic surveillance against non-U.S. persons for foreign intelligence purposes.

As Justice Arthur Goldberg said, the Constitution is not a suicide pact.

Consideration should also be given to changing the rules on "minimization" of information about U.S. citizens obtained in the course of electronic surveillance under FISA. It is my impression that intelligence analysts believe that valuable intelligence frequently is lost because of an overly cautious interpretation of the minimization rules.

Fourth, we will win this war—but how we win it matters. We must not abuse the rule of law at home in seeking to enforce it overseas. We must be determined, and when necessary prepared to use lethal force. But that does not mean that we should, as some people have said, "throw out all the rules." The world has developed a body of law, the Law of War, governing the conduct of armed conflict. These rules are designed not only to reduce the horrors of war and to protect noncombatants, but also out of a recognition that the manner in which the war is fought should not cause future conflict by sowing the seeds of hatred.

In that respect, we need to examine each of our proposed actions with respect to the rule of law and how it will be seen by others. For example, we should not rescind the ban on assassinations. Americans are not assassins. Repealing the ban crosses a line that most Americans are uncomfortable crossing. In any event, we have been able to conduct military and intelligence activities, including some using lethal force, to accomplish our objectives in the past. Moreover, it is not an effective deterrent to terror. It often creates martyrs and heroes among the terrorists and exposes our own leaders to increased threats of assassination. Finally, when this war is over, I do not believe we want a world in which our actions have established the assassination of foreign leaders as an acceptable norm of international behavior.

Fifth, the U.S. response should mobilize all resources of the nation. In particular, the President should call upon American industry to put its genius to work to meet and defeat this threat. The President should support innovative, public/private cooperative efforts to ensure that the best minds in industry, academia and other elements of the private sector are marshaled against this national threat.

However, concerning the specific legislation currently under consideration, I believe that the Congress should make clear that with respect to increased electronic surveillance, the government will not adopt technical mandates requiring the information technology industry to build their systems in such a way as to facilitate interception, to enhance security or to control the dissemination of encryption. Instead, the government should reach out to industry and harness market forces to achieve the necessary results.

A national objective must be to assure that U.S. industry remains the world leader in these fields. Our security is much better enhanced by having American industry continue to lead rather than to face information technology and encryption produced overseas, which would happen if the United States exerts an overly heavy hand and interferes in the marketplace in the development of technology.

I also believe, Mr. Chairman, that this committee should carefully review the Administration's bill from the perspective of whether it takes into account all of the concerns raised by the Intelligence Community. I appreciate that the bill was very quickly pulled together and I value the need for speed. But we must be careful not only on the civil liberties side, but also on the government's side. For example, I know there are concerns as to whether there has been adequate sharing of information from the law enforcement agencies to the Intelligence Community. There may also need to be minor adjustments to FISA to address recent or anticipated developments in technology.

For all of these reasons, it seems prudent to me to enact those provisions for which there is wide support and proceed more deliberately on other provisions.

PROPOSED LEGISLATION

Now let me turn to the specifics of the legislation.

You have asked me to consider those provisions of the bill as introduced on behalf of the Administration that are within the jurisdiction of this Committee. You have also asked me to comment on the bill introduced by the Chairman of this Committee. I have not had a great deal of time to study either bill, but I am happy to provide the following preliminary comments.

ADMINISTRATION'S BILL

Turning first to the bill as introduced on behalf of the Administration, I note that Section 103 amends 18 U.S.C. 2510(7) to permit sharing of Title III wiretaps with any officer or employee of the executive branch of the Federal Government.

The proposed change in the statute includes no limitation as to whom it may be given. It seems prudent to limit the purposes for which such information may be disseminated within the executive branch, for example by limiting it to national security matters.

The analysis also says that it will harmonize Title III standards with those of FISA. However, intelligence officers have complained that too frequently the Department of Justice either refuses to share information collected under FISA or is very slow in providing it. I believe this is a more fundamental question and ought to be addressed along the lines I suggest above. I can see no reason why information collected by the Department of Justice under a FISA wiretap is not immediately made available to a relevant agency of the Intelligence Community. If it concerns a U.S. person, it seems to me that the Attorney General could require common minimization standards to be followed by all intelligence agencies.

Section 104 is characterized as a "savings provision," and the explanation says that it provides that collection of foreign intelligence is governed by foreign intelligence authorities rather than by criminal procedural statutes. That is a noteworthy objective, as I discuss above. However, it is not clear to me what this proposed change would accomplish. I believe more detailed explanation of the proposed changes and its consequences are needed.

Section 105 appears to codify the so-called "silver platter" doctrine; namely that when a foreign government provides information to the U.S. Government for which the U.S. Government has not asked nor had any role in collecting, the U.S. Government may use that information. However, I am troubled by the proposed language of the new section 2514(1)(b). It would require that when a U.S. official participated in the electronic surveillance, the information collected may only be used when it "would have been lawful if executed within the United States." That may be entirely appropriate in the case of a criminal prosecution, but I do not believe such limitation should apply in a case of collection of foreign intelligence. There may also be reason to distinguish between information collected on a U.S. person—for which a higher standard might be appropriate—and a non-U.S. person.

Section 151 extends the duration of the time—to 1 year—that the FISA court may authorize search and surveillance in the United States of officers and employees of foreign powers and foreign members of international terrorist groups. This is the same provision as section 202 of Senator Graham's bill and seems to be a sensible provision.

Section 152 expands the obligations of third parties to furnish assistance to the government under FISA, particularly when the target moves frequently to avoid detection. This is substantially the same as section 203 of Senator Graham's bill and enhances the ability to monitor individuals who move rapidly to change the mode of their communication to avoid detection. It also seems sensible and should be adopted.

Section 153 would change the language of FISA so that it may be used where foreign intelligence is "a" purpose of the investigation, as opposed to current law which limits it to instances in which it is the sole or primary purpose of the investigation. Consistent with my views as outlined above, I believe this is an appropriate change. I believe the government should have flexibility in deciding whether to initiate a FISA collection, particularly when foreign nationals are involved, as opposed to being forced into a Title III collection with its higher standards. However, the Committee should ask the Administration whether current law has limited its ability to conduct FISA in instances in which the Administration thinks it would have been appropriate. The Committee should be careful in endorsing this change because it holds out the potential that the government would seek FISA surveillance warrants—when it didn't have enough information to get a Title III order—but in which the foreign intelligence information to be obtained was remote or highly speculative.

Section 154 calls for greater sharing of foreign intelligence information held in the hands of the Department of Justice, whether in a grand jury proceeding or obtained under Title III. I believe this is an extremely important provision but note that it

does not appear to be codified. I believe it should be. I also note that it is similar to section 354 of the Administration's bill and section 301 of Senator Graham's bill. My first impression is that this provision in the Administration's bill is the most clear. In particular, the Administration's proposal mentions Rule 6E of the Federal Rules of Criminal Procedure, which has been a significant bar to providing relevant information from Grand Jury investigations to the Intelligence Community.

Section 155 would eliminate the requirement that the government establish that a communications device has been used to contact "an agent of a foreign power" in order to obtain a FISA order for a pen register/trap and trace order. I believe this makes sense and should be adopted.

Section 156 would give the Attorney General the authority to seek information with an "Administrative Subpoena" for documents and records similar to the authority that he has in drug investigations. This seems to be a sensible provision.

Section 157 expands the authority of the FBI to issue National Security Letters to request certain information. Current law requires both a showing of relevance and a showing of links to "an agent of a foreign power." The elimination of this latter requirement would permit the FBI to seek information in the same fashion as with criminal subpoenas. It seems to me sensible and should be adopted?

Section 354 makes specific changes to the Federal Rules of Criminal Procedure, and in combination with section 154 seems a sensible approach.

Although the Committee does not have jurisdiction over section 110 of the Administration's bill, I have one comment that I believe the Committee should consider and perhaps recommend to the Judiciary Committee. That section amends Title 18 so that a provider of telecommunications and services, including ISPs, could provide information to a governmental entity, including the contents of the communication, if the company "reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information." Companies ought to be encouraged to provide such information to the government in such circumstances. However, I note that there is no immunity for a company that makes such a disclosure. There is such proposed statutory immunity in Section 158, which provides for disclosure of educational records. That section provides "no person furnishing records or information pursuant to this subsection shall be liable to any other person for furnishing such information." I suggest that a similar provision be considered to protect those companies who voluntarily provide information on individuals to the government as provided under Section 110.

CHAIRMAN GRAHAM'S PROPOSAL

Turning to the bill suggested by the Chairman, I have the following comments.

Section 101 would add a new provision to the responsibilities of the DCI to "establish requirements and priorities for and manage the analysis and dissemination of all foreign intelligence collected under FISA." My inclination is that this is a good idea in that it would authorize the DCI to take a greater role in the use of FISA to collect and analyze foreign intelligence. However, I believe that the views of the DCI should be sought and carefully considered. It is important that the authority of the DCI be sufficient to assure that FISA collection is done in an efficient manner to support the collection of foreign intelligence but without giving the DCI excessive authority to direct the use of electronic surveillance in the United States.

Section 102 revises the National Security Act to make it clear that the DCI has particular responsibilities for international terrorism. Again, I believe this is a good change, as there has been considerable debate within the executive branch as to primacy for the collection, analysis and dissemination of information on international terrorism. This is a welcome change.

Section 103 would add a provision to the National Security Act stating that an officer of the Intelligence Community "may establish and maintain an intelligence relationship with any person for purposes of acquiring information" on a variety of terrorist targets. This is clearly aimed at assuring that case officers in the field will be encouraged to take the necessary risks associated with recruiting a human source in a terrorist organization, even when that individual may have committed murder or engaged in other serious human rights abuses or criminal activities.

The current guidelines were adopted by the CIA in 1995 because of concerns expressed widely in the press and the Congress that the Agency had dealt with such individuals. The guidelines adopted a simple test: Does the value of the intelligence that the individual could provide outweigh the risks to the United States that would be associated with dealing with this individual? The guidelines have two purposes. First, to assure that Headquarters make an informed decision to authorize the recruitment of such an individual. The view was that the balancing test should be done at Headquarters, not in the field. The second purpose is to protect the officer

involved. Once approval had been granted from Headquarters, the officer has a "hunting license" and is free to proceed, knowing that he or she had the full backing of Headquarters. This latter point was particularly important because in the mid-90's several officers were under investigation by congressional committees, the PFIAB, the CIA/IG, and, in some instances, criminal grand juries. Many officers, as this Committee well knows, felt it necessary to purchase personal liability insurance on their own to cover the costs of hiring outside counsel to defend themselves from the various investigations. I thought then, and think now, that no CIA case officer should ever have to purchase such insurance out of his or her own pocket.

I understand that many officers in the field believe that these guidelines are a hindrance to recruiting sources in terrorist organizations. I also understand that CIA Headquarters maintains that the guidelines do not hinder the recruiting of sources who could provide valuable intelligence in these organizations. It is therefore difficult to know where the truth is. However, it is clear that there is a perception in the field that these guidelines inhibit recruiting. CIA case officers must know that they are encouraged to take risks and that when they do so, they will be backed up by CIA Headquarters, the rest of the National Security establishment, and the Congress.

Therefore, these guidelines should be carefully reviewed by the DCI and his top leadership team, and if they are in fact inhibiting recruiting in the field, they should be changed.

I do have reservations about Section 103 of this bill. First, it provides that an officer may maintain a relationship only "for purposes of acquiring information." Thus, if an officer had a relationship with a source inside a terrorist organization, this language would limit our ability to direct that officer to use that relationship to disrupt a terrorist organization, for example by feeding misinformation to his source or by using his source to support a covert operation that would be designed to disrupt or destroy the terrorist organization. Second, it raises questions about CIA case officers dealing with persons in other groups, such as international organized crime or international narcotics organizations, that enjoy no similar provision.

On reflection, I think the Congress could usefully order the Director of Central Intelligence, perhaps in conjunction with PFIAB or some other outside organization, to conduct a careful review of these guidelines and, if they are in fact hindering the recruiting efforts in the field, they should be changed accordingly.

Section 104 defers submittal to Congress of certain reports and will surely be most welcome.

Section 201 amends FISA to exclude from the definition of interception an instruction or signal that is given to operate an electronic device. That seems a sensible provision and should be adopted.

Sections 202 and 203 are analogous to Sections 151 and 152 in the Administration's bill and, as noted above, should be adopted.

Section 204 seeks to clarify the relationship between Title III and FISA wiretaps. The consequences of this provision are not immediately clear but it does not seem sensible to me to have a situation in which two collections efforts are being mounted in parallel.

Section 301, as discussed above, is designed to assure that the Intelligence Community is given access to information held by the Department of Justice. This is a commendable objective but my inclination is to favor the provisions in the Administration's bill, as they seem more clear.

Sections 302, 303 and 304 also make reasonable and thoughtful changes to existing law and should be adopted.

Mr. Chairman, in conclusion let me repeat how honored I am to address these issues, and I look forward to answering the Committee's questions.

STATEMENT OF JEFFREY H. SMITH, PARTNER, ARNOLD AND PORTER

Mr. SMITH. Thank you, Mr. Chairman. I will be brief. The hour is late. I have submitted a statement which I will try to summarize here in just two or three moments.

It's clearly an honor to be here and to be back in front of this Committee. I was Senator Nunn's designee to this Committee for many years, and it's an honor to be back.

Also, on behalf of my former colleagues at CIA and in the Intelligence Community, they are putting forward an unprecedented

level of dedication as we speak, and I think we all owe them a vote of thanks. George Tenet, also a former alumni of this great Committee, has put his heart and soul into this effort and he deserves the Nation's thanks.

As I think about the issues you've asked me to address, it seems to me there are five principles that we ought to approach. I have taken a somewhat broader approach than just some of the specific questions you've asked me. This is a seamless attack on the United States across international borders, and in our response we need to have a seamless response as well. We need to, as you are trying to do, Mr. Chairman, try to create an integrated response to an integrated threat. There should be no stovepipes in the U.S. Intelligence Community that would impair our ability to respond.

Senator Shelby mentioned that in his opening statement. We don't want any stovepipes. We need to get rid of those.

Much as the Goldwater-Nichols Defense Reorganization Act of 1986 gave increased authority to our CINCS overseas—commanders-in-chief overseas—I'm rather attracted to the idea of a civilian CINC to attack counterterrorism, perhaps even adopting the model where forces from various U.S. agencies are assigned to this individual much as they are assigned an overseas CINC so that he or she can accomplish his mission.

Second, our laws and regulations must be reviewed to make sure that they do not foster the stovepipes that have caused so many problems in the past, and I am pleased to see that many of the proposals you've put forward address those changes.

Clearly we have to recognize that many of these rules—such as grand jury secrecy and so on—were enacted to protect the rights of our citizens, but we have to find a way to make our government work more effectively.

Third, I think we should be as aggressive as our Constitution will permit, particularly with respect to non-U.S. persons. Yesterday's Washington Post reports on page A18 that the FBI wanted to initiate electronic surveillance against Osama bin Ladin's non-U.S. person associates in the United States prior to the attack, but the Justice Department did not believe that there was adequate authority, given the information available to them, to get a FISA tap. If that's the case, I think we ought to look at the law and see whether it's working adequately. As Mr. Justice Goldberg said, the Constitution is not a suicide pact.

Fourth, we will win this war against terrorism, but how we win it matters. We must not abuse the rule of law at home in seeking to enforce it overseas. We need to examine each of our proposal actions with respect to the rule of law and see how it would be seen by others. It's beyond the scope of what you've asked me to think about, but, Mr. Chairman, I don't think it's a good idea to rescind the ban on assassinations. Americans are not assassins. We've been able to do everything we need to do without crossing that line. When this war is over, I do not believe we want a world in which the actions of the United States have established that the assassination of foreign leaders is an acceptable norm of international behavior.

Fifth, I think we should mobilize all resources of the Nation. In particular, I think the Government ought to reach out to industry

and harness some of the genius of our industry to assist in the war on terrorism. The national objective must be to assure that our industry remains the world leader in all of the fields at play here, from aviation to information technology.

Finally, Mr. Chairman, I know you asked the Administration witnesses this, but I think particularly from this Committee's point of view as you move forward I urge you to consult closely with the Intelligence Community. To be perfectly candid about it, the Administration's bill was put together in a great rush, and I think we want to make certain that the issues that concern the Intelligence Community are adequately reflected in the Administration's bill or clearly in any bill that the Congress passes.

I've given the Committee extended comments on details of the legislation. I'm pretty rusty in many of the ins and outs of how these laws work, so please forgive my conclusions if they are inadequate. I won't go through them at any length. Two or three things I want to mention very briefly.

The first is again beyond the scope of this Committee but section 110 of the Administration's bill says that companies are encouraged to provide information to the Government even including the content of U.S. person communications when in an emergency it would risk life and limb. I think that's an honorable provision, but I notice that there's no immunity for the companies should they do that.

The Administration has also made a proposal that educational universities have to turn over educational records of individuals, and in that instance they are proposing to give the educational institutions immunity. I think a similar grant of immunity should be considered in the case of U.S. companies who give to the Government information on U.S. persons voluntarily.

I'm happy to talk about section 103 of your bill, Mr. Chairman, that would deal with the question of dirty assets. I do want to commend you for section 102, which gives the DCI increased authority over counterterrorism. When I was general counsel of the CIA we spent an unconscionable amount of time arguing with the FBI over who was going to issue the report prior to the 1996 Atlanta Olympics, whether that was the FBI's responsibility or our responsibility. Those sorts of arguments ought not take place.

Mr. Chairman, I'm happy to answer your questions.

Chairman GRAHAM. Good. Thank you very much, Mr. Smith. I'm going to call in your two brethren on this panel and then we will ask questions to all of you together.

Mr. BERMAN. We talked and tried to say could we split the baby in half.

Chairman GRAHAM. I will call on both of you collectively and you can allocate the time as you wish.

[The prepared statement of Mr. Berman follows:]

JERRY BERMAN, EXECUTIVE DIRECTOR, CENTER FOR DEMOCRACY & TECHNOLOGY

Mr. Chairman, Mr. Vice-Chairman, members of the Committee, thank you for the opportunity to testify at this hearing on the momentous question of improving our nation's defenses against terrorism in a manner consistent with our fundamental Constitutional liberties.

The Center for Democracy and Technology is a non-profit, public interest organization dedicated to promoting civil liberties and democratic values for the new dig-

ital communications media. Our core goals include enhancing privacy protections and preserving the open architecture of the Internet. Among other activities, CDT coordinates the Digital Privacy and Security Working Group (DPSWG), a forum for more than 50 computer, communications, and public interest organizations, companies and associations working on information privacy and security issues.

CDT joins the Nation in grief and anger over the devastating loss of life resulting from the September 11 terrorist hijackings and attacks against the World Trade Center and the Pentagon. Like many, our relatively small staff had friends and acquaintances killed in those heinous acts. We fervently support the efforts of our Government to hold accountable those who direct and support such atrocities.

It is clear that improvements need to be made in America's counter-terrorism procedures, and it appears there are many things that can be done without harming civil liberties. But we know from history that measures hastily undertaken in times of peril—particularly measures that weaken controls on government exercise of coercive or intrusive powers—often infringe civil liberties without enhancing security. In the current climate, it is all the more important to act deliberately and ensure that our response is balanced and properly targeted. If we give up the constitutional freedoms fundamental to our democratic way of life, then the terrorists will have won.

In that regard, Mr. Chairman, we commend you and the Committee for holding this hearing, and taking the time to consider the legislative proposals put forth by the Administration and those you have developed. Only through the hearing process can you and the American public understand what is being proposed, how it would change current law, and whether the changes are responsive to any deficiencies that the September 11 attack may have revealed. Just as President Bush and his military advisers are taking their time in planning their response, to ensure that they hit the terrorist targets with a minimum of collateral damage, so it is incumbent upon this Congress to avoid collateral damage to the Constitution.

COMMENTS ON CHAIRMAN GRAHAM'S "INTELLIGENCE TO PREVENT TERRORISM ACT"

My testimony will focus on the electronic surveillance provisions in both Chairman Graham's "Intelligence to Prevent Terrorism Act" and the Administration's proposed "Anti-Terrorism Act of 2001." My colleague Kate Martin will focus on several other provisions in the bills that need clarification. Many provisions of the Chairman's bill appear narrowly and approximately crafted to carefully provide desired intelligence capabilities; however I will also highlight at least one provision of the bill—Section 201—that may have broad implications for the Internet.

As you well know, this Committee—and the current legal structure of the Intelligence Community—were established after Watergate both to improve intelligence and to ensure that the rights of Americans were not eroded by the vast and sometimes vague intelligence authorities that had previously existed. The legal and oversight system for intelligence sprang not just from a concern about civil liberties, but also from a concern about improving the efficacy of intelligence gathering. As such, the Committee mission demands a careful vetting of any new proposed intelligence authorities and we applaud the committee for holding these public hearings to do so.

A number of the provisions of both the Chairman's bill and the Attorney General's bill would change provision of the Foreign Intelligence Surveillance Act of 1978 (FISA). As the Committee is also well aware, FISA gave extensive authority to the Intelligence Community. Under it the FBI and CIA have considerable capability to conduct electronic surveillance without the high standards (such as a showing of probable cause of criminal conduct, notice, and eventual adversarial scrutiny) demanded under our domestic criminal law for wiretapping. In exchange for these significantly lowered standards allowing much greater intelligence surveillance, FISA demanded a clear separation—a wall—between electronic surveillance conducted for intelligence purposes and electronic surveillance conducted for criminal law purposes. FISA was based on a clear understanding that it would not become a back door for use of foreign intelligence surveillance in domestic criminal investigations. FISA information that was incidentally collected regarding criminal matters could be shared across this wall but the purpose of a FISA surveillance had to be intelligence. This was intended to avoid a major erosion of our constitutional rights through the lower standards of FISA surveillance.

As we read the Chairman's bill, we applaud what appears to be the committee's intent to maintain that distinction between intelligence authorities and domestic law enforcement provisions. We are particularly pleased to see that the Chairman's bill does not appear to intended a rewriting of the FISA authorities. As described below, however, we believe that the Attorney General's bill does not reflect this deeper understanding and would eviscerate the FISA principles, allowing foreign in-

telligence surveillance standards to be used in criminal investigations. (See, e.g., Administration bill, Sections 151–157) Thus, while we have concerns about some specific provisions, we believe the Chairman's bill is far more narrowly crafted, and more appropriately targeted to the situation at hand.

First and foremost, we note with approval Section 204's attempt to make it clear that the FBI could conduct both a Title III criminal wiretap and a FISA wiretap, intercepting the same communications for different purposes. If done properly, this is a more direct and appropriate approach to allow criminal investigations and intelligence investigations to go forward side-by-side. We need to explore with the committee the specific language of the section, but if it tracks the intent expressed in the section-by-section analysis, we believe it is an appropriate approach.

Section 202, regarding the duration of certain FISA surveillance authorities, raises some concerns. FISA electronic surveillances of persons are already granted for periods three times longer than Title III surveillances. Under 202, the duration of surveillance before any judicial oversight would be extended from 90 days to 1 year. In the case of physical searches, the period would be extended from 45 days to 1 year. Courts have only turned down one FISA application in the 22-year history of the statute's use. Judicial review, after 45 or 90 days, hardly seems overly burdensome; if surveillance should continue a judge will surely—given the history of discretion in these matters—renew the order. The risk of this provision is that unproductive surveillance could continue for long periods of time without any judicial oversight.

Section 203, the assistance section, may also merit more careful drafting. To the extent, as indicated in the section-by-section analysis, it is only requiring additional assistance from service providers that cannot be identified in advance, we believe it is a measured response. However, we believe the language should be reviewed with staff to ensure that it is not granting new surveillance authorities.

Section 201 raises concerns and is one area where we should not legislate quickly in this complex field of electronic surveillance law. Frankly, we find the language to be very ambiguous and potentially very broad. It must undergo further discussion and more careful drafting.

As drafted, the provision would exclude from the definition of "electronic surveillance" any "instruction or signal" sent to a computer—if it was not a communication to another person, or was not for lawful information retrieval—thereby exempting such information from the reduced standards of FISA. As we read the interaction of Title III and FISA, this would allow the interception of such signals with no judicial oversight.

While apparently intended to allow interception of communications "from a hacker, located abroad" the provision also sweeps in a broad class of otherwise protected communications. It would appear to include, for example:

- commands sent remotely to a home security system;
- reminders being sent to an online calendar or alarm clock system;
- stock trade commands sent to an electronic trading system;
- programs or files being sent (not retrieved) to a computer system;

or any other commands one sends to one's own computer, Palm Pilot, or wireless phone. All of these sensitive communications, in which there is both a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, could now be obtained under FISA and without judicial oversight.

It is also unclear how the provision could be applied in practice. In a packet-switched data interception environment like the Internet, it is difficult if not impossible to know in many cases which packets to be intercepted contain an "instruction or signal" for a computer and are not for information retrieval, and which contain information that should require a judicial order. In many, if not in most, cases it will only be possible to see whether this provision applied after the communication is intercepted, read, and analyzed. Thus, if this provision is to be used it would appear to create a license for interception of numerous communications that would ultimately be discarded after they are read and analyzed.

Section 201 would appear to create a giant hole in the FISA electronic surveillance requirements and would allow the interception of numerous personal communication without judicial oversight. It is in serious need of redrafting at the very least; if its goal is to allow interception of hackers attacking a computer, it seems better addressed by provisions that would allow target computer owners to consent to the interception of attacks on their computers.

We recommend that this section be deleted or substantially clarified.

COMMENTS ON ADMINISTRATION PROPOSALS

The Administration's Anti-Terrorism Act of 2001 goes far beyond the measured response of this committee. It would expand Federal Government authorities, including the authorities of the intelligence agencies, to conduct electronic surveillance and otherwise collect information on U.S. citizens. Some of the changes are quite fundamental. The bill includes numerous, complex provisions extending the surveillance laws (while raising many questions about how they will be implemented) and altering the long-standing distinction between criminal investigations and foreign intelligence investigations. Many of the changes are not related to security concerns raised by the September 11 terrorist attacks. Many are not limited to terrorism cases, but relate to criminal investigations. Some have been proposed by the Justice Department before, and some have even been rejected by Congressional committees.

In terms of the issues within the jurisdiction of this Committee, these are our top concerns:

• Section 153. Foreign Intelligence Information. Allows the FBI to collect evidence for criminal cases under the looser standards of foreign intelligence investigations—an end-run around the relatively stringent requirements for wiretaps in criminal cases and a breach of the understanding that led to enactment of FISA.

• Section 155. Pen Register and Trap and Trace Authority. Eliminates the only meaningful statutory control that exists on use of pen registers ant trap and trace devices in intelligence cases.

• Section 156. Business records. Allows access to any business records upon the demand of an FBI agent, with no judicial review or oversight.

• Sec. 157. Miscellaneous national-security authorities—Amends several key privacy laws, allowing much greater access to banking, credit, and other consumer records in counter-intelligence investigations, with no judicial review at all.

A more detailed analysis of the Administration's bill follows below. Once again, we appreciate and commend this Committee's efforts to gather public input and to hold this hearing today. We hope the Committee will move forward with those provisions of its bill and the Administration's bill that are non-controversial and responsive to the tragic attacks of September 11, but will defer on the other more complex and divisive provisions that we have identified. We look forward to working with the Committee and staff to craft an appropriate response at this perilous moment in our country's history, and to avoid a rush to judgment on legislation that could ultimately imperil both freedom and security.

EXTENDED ANALYSIS OF THE ADMINISTRATION BILL

The Administration's bill has two kinds of provisions that give rise to concerns: those that would lower the standards for government surveillance and those that address the difficult question of information sharing.

In terms of collection standards, our law enforcement and intelligence agencies already have broad authority to monitor all kinds of communications, including e-mail. Both the criminal wiretap statute and the Foreign Intelligence Surveillance Act already cover terrorism. For some time, it has been recognized that those standards need to strengthen the standards for government surveillance. We see no justification for the changes proposed in the Administration bill that weaken those standards. We are particularly opposed to changes that would eliminate the judicial review that can be the most important protection against abuse.

The Foreign Intelligence Surveillance Act allows the FBI to conduct electronic surveillance and secret physical searches in the United States, including surveillance of U.S. citizens, in international terrorism investigations. FISA also authorizes court orders for access to certain business records. As you know, the standards under FISA are much lower than the standards for criminal wiretaps, and in return, the surveillance is supposed to be focused on the collection of intelligence, not criminal evidence. The FISA court, which last year approved more than 1000 surveillance requests, has denied only one request in its 22 year history.

Distinct from the Administration's unsupportable desire to avoid judicial controls on its authority, perhaps the central and most important problem facing the Congress is the question of information sharing. For many years, this has been recognized as a very difficult question; it is one that will be especially difficult to resolve satisfactorily given the pressure-cooker atmosphere of this time. We want to work out a balanced solution. But it cannot be done by wiping away all rules and barriers. Any solution needs to preserve the fundamental proposition that the CIA and other intelligence agencies should not collect information on U.S. citizens in the United States.

Sec. 103. Authorized Disclosure

Allows disclosure of information obtained from wiretaps with any executive branch official.—This is clearly too broad, especially in light of the vague language in 18 USC 2517 that allows sharing when appropriate to the proper performance of the duties of the official making or receiving the disclosure. The issue of greatest concern to us is that the CIA and other intelligence agencies would begin compiling files on U.S. persons. This provision should be narrowed, so that it authorizes disclosures to personnel with intelligence, protective, public health or safety, or immigration duties, to the extent that such disclosure is related to proper performance of the official duties of the officer receiving the disclosure, and with the proviso that nothing therein authorizes any change in the existing authorities of any intelligence agency. (Rather than amending the definition section of Title III, it might be better to build these concepts directly into section 2517.)

Sec. 105. Use of Wiretap Information from Foreign Governments

Allows use of surveillance information from foreign governments, even if it was seized in a manner that would have violated the fourth amendment.—Section 105 makes surveillance information collected about Americans by foreign governments (so long as U.S. officials did not participate in the interception) admissible in U.S. courts even if such interceptions would have been illegal in the United States. Such a provision is ripe for abuse and provides unhealthy incentives for more widespread foreign surveillance of U.S. individuals.

Sec. 151. Period of Orders of Electronic Surveillance of Non-United States Persons Under Foreign Intelligence Surveillance

Allows secret searches and electronic surveillance for up to 1 year without judicial supervision.—Under current law, the FISA Court can order a wiretap of a "non-U.S. person" for a period of 90 days, after which the Government must report to the court on the progress of the surveillance and justify the need for further surveillance. The court can authorize physical searches for up to 45 days. The amendment would extend both timeframes to 1 year, meaning that after the Government's initial *ex parte* showing there would be no judicial review for 1 year. We think this is too long. We recommend that the current timeframes be retained for the initial approval. (After all, they are already far longer than the 30 days for which criminal wiretaps, including criminal wiretaps in terrorism cases, can be approved.) If, after 90-days of electronic surveillance or 45 days of physical searches, the Government can show a continuing justification for the surveillance or search authority, then we would agree that the court could authorize a longer surveillance. We would recommend 1 year for electronic surveillance, 180 days for physical searches (thus preserving the current law's recognition that physical searches are more problematic than electronic searches and need to be authorized for shorter periods of time).

Section 152 Multi-Point Authority

Allows roving taps, including against U.S. citizens, in foreign intelligence cases with no limits—ignoring the Constitution's requirement that the place to be searched must be "particularly described."—This section purports to afford the FBI "roving tap" authority for intelligence investigations similar to what already exists for criminal investigations. See 18 USC 2518(11). A roving tap allows the Government to intercept whatever phone or e-mail account a suspect uses, even if the Government cannot specify it in advance. Roving tap authority is constitutionally suspect, at best, since it runs counter to the Fourth Amendment's requirement that any search order "particularly describe the place to be searched." However, the proposed language places no limitation on the exercise of the roving tap authority and offers the FBI no guidance for its exercise. The proposed change merely authorizes the court to issue to any "person" an order commanding them to cooperate with a surveillance request by the Government. If roving tap authority is supposed to focus on the targeted person, not on the telephone instrument, then the intercept authority should be limited to the target—it should only allow interception of communications to which the target of the surveillance is a party. Such limitations are absent from this proposal.

Section 153. Foreign Intelligence Information

Allows the FBI to collect evidence for criminal cases under the looser standards of foreign intelligence investigations—an end-run around the relatively stringent requirements for wiretaps in Title III.—This section, which merely changes the word "the" to "a," would actually make a fundamental change in the structure of the wiretap laws. It would permit the Government to use the more lenient FISA procedures in criminal investigations which have any counter-intelligence purposes and would destroy the distinctions which justified granting different standards under FISA in

the first place. Under existing law, FISA can be used only if foreign intelligence gathering is "the" purpose of the surveillance. The proposed provision would permit FISA's use if this is "a" purpose, even if the primary purpose was to gather evidence for a criminal prosecution. This is an extraordinary change in the law which has no justification.

Section 154. Foreign Intelligence Information Sharing

With no standards, permits the sharing of grand jury information, Title III wiretap information, and any other "foreign intelligence information" acquired in a criminal case with many different Federal officials not involved in law enforcement.—This is a sweeping change in the law. "Foreign intelligence information" is not defined. The provision places no limits on the purpose for which the information may be shared, and no limit on its reuse or redisclosure. It requires no showing of need and includes no standard of supervisory review or approval. As written, a criminal investigator could share with White House staff information collected about foreign policy critics of the Administration. The provision, at the very least, should be drastically curtailed.

Section 155. Pen Register and Trap and Trace Authority

Eliminates the only meaningful statutory control that exists on use of pen register and trap and trace devices in intelligence cases.—The law currently requires a showing that the person being surveilled is a foreign power, an agent of a foreign power or an individual engaged in international terrorism or clandestine intelligence activities. This amendment would eliminate that standard and permit the use of FISA for pen registers whenever the Government claimed that it was relevant to an ongoing intelligence investigation. Contrary to the DOJ's assertion in its section-by-section, this is not the same as the standard for pen registers in criminal cases. There, the surveillance must be relevant to an ongoing criminal investigation, which is moored to the criminal law. There is no similar constraint on foreign intelligence investigations, since they can be opened in the absence of any suspicion of criminal conduct. This provision ignores the fact that the Government was granted the special rules of FISA only for situations that involved intelligence gathering about foreign powers.

Section 156. Business Records

Allows access to any business records upon the demand of an FBI agent, with no judicial review or oversight. Traditionally, the FBI had no ability to compel disclosure of information in intelligence investigations. The compulsory authorities were limited to criminal cases, where the open, adversarial nature of the system offered protections against abuse. For example, in criminal cases, including international terrorism cases, the FBI can obtain grand jury subpoenas, under the supervision of the prosecutor and the court, where the information is relevant to a criminal investigation. The FBI has no ability to invoke the power of the grand jury in intelligence investigations, since those investigations are conducted without regard to any suspicion of criminal activity. In 1998, in an expansion of intelligence powers, FISA was amended to give the FBI a new means to compel disclosure of records from airlines, bus companies, car rental companies and hotels: Congress created a procedure allowing the FBI to go to any FISA judge or to a magistrate. The FBI had only to specify that the records sought were for a foreign intelligence or international terrorism investigation and that there were specific and articulable facts giving reason to believe that the person to whom the records pertain is an agent of a foreign power. This is not a burdensome procedure, but it brought the compulsory process under some judicial control. The Administration's bill would repeal the 1998 changes and permit the use of "administrative subpoenas" rather than an application to a court to get any business records under FISA. An administrative subpoena is a piece of paper signed by an FBI agent. There is no judicial review, no standard of justification, no oversight. Particularly in intelligence investigations, which are not even limited by the scope of the criminal law and in which there is no involvement of the U.S. Attorney's Office, FBI agents should not have such unreviewable discretion to compel disclosure of personal information.

See. 157. Miscellaneous National-Security Authorities

Allows much greater access to banking, credit, and other consumer records in counter-intelligence investigations.—Current provisions of law allow the Federal Government to obtain sensitive banking, credit, and other consumer records under the relaxed and secretive oversight of FISA—but only when there are "specific and articulable" facts showing that the target consumer is "a foreign power or the agent of a foreign power." Section 157 would eliminate these essential requirement, mandating disclosure of this sensitive consumer data simply if an FBI official certifies

that they are needed for a counterintelligence investigation (and with an ex parte court order for access to credit reports). Section 157 would eliminate the "agent of a foreign power" standard in:

- The Fair Credit Reporting Act, allowing access to records from consumer reporting agencies (including the names of all financial institutions where accounts are held, all past addresses and employers, and credit reports);
- The Financial Right to Privacy Act, broadly allowing access to financial records; and
- The Electronic Communications Privacy Act, allowing access to telephone and toll billing records, and, newly added, all "electronic communication transactional records."

As such, the Section would greatly increase access to the personal information of consumers or groups who are not agents of foreign powers. And in each case access the institutions granting access to consumer information would be prohibited from disclosing that information or records had been obtained.

Section 158. Disclosure of Educational Records

Amends the law protecting education records to permit access to them.—While this might be justified in terrorism cases, the provision covers all cases involving "national security" and is far too sweeping.

Section 159. Presidential Authority

Does not appear to permit judicial challenge to seizure of property. At the very least, there must be such opportunity. A second provision allows the use of secret evidence. Use of such evidence, if ever permitted, must be on a much higher standard than that the information is properly classified, as provided here. The Government must be required to persuade a court that the disclosure to the party would result in imminent and serious harm and the court must require the Government to provide sanitized information to the party.

STATEMENT OF JERRY BERMAN, EXECUTIVE DIRECTOR, CENTER FOR DEMOCRACY AND TECHNOLOGY

Mr. BERMAN. I am the executive director of the Center for Democracy and Technology, which specializes in communications and internet privacy and freedom issues. But I've been around a long time, and in prior incarnations I was part of the lobbying effort to create this Committee in 1976 and also to pass and help draft the Foreign Intelligence Surveillance Act of 1978 and the Electronic Communications Privacy Act of 1986, working closely as a civil libertarian with Administration and Hill people to try and strike a careful balance between national security and civil liberties. I think the effort proved successful.

We have to go back and remember that this Committee was set up after Watergate for two purposes—first, to improve our intelligence capabilities and monitor that and keep track of that; and second to make sure that the CIA and FBI and other intelligence agencies do not go off the rails again, as they had done during the Watergate era, where they were investigating domestic dissent and Martin Luther King.

So we must be careful, and what we learned in that period is that emergency powers passed very quickly during World War II eventually spread out and eventually, instead of going after our foreign foes, which we need to do in this critical crisis, began to go after domestic dissent and it was not a happy period.

So, learning from that lesson, I think the Chairman asked the right question. Why are we in a race for a multi-multi-section bill covering the waterfront, which has provisions on law enforcement, intelligence and so forth? What needs to pass now and what needs to pass later?

The key issue that's been discussed here deals with the wall that was built on electronic surveillance—let me focus on that—the wall between electronic surveillance for intelligence purposes and electronic surveillance for law enforcement. The standards for intelligence are lower, and we're not just talking about electronic surveillance; we're talking about black bag jobs. We're talking about secret searches which never get turned over to the target of the investigation. The standards are important to give national security a leg up, but they need to be carefully reviewed, they need judicial supervision, and they need to be carefully thought out.

We applaud the Committee in your statute proposal. That wall is preserved, or at least the intent appears to preserve that wall by requiring that if you're conducting an intelligence investigation conduct it there, under FISA. If you also have a criminal investigation or information that leads to a criminal investigation, open a title III warrant. That dual authority maintains that wall.

If there is a problem between our intelligence agencies, it is not by eliminating the primary purpose test, which may be unconstitutional—Mr. DeWine raised that question and a number of the Committee—but surgically dealing with information-sharing that may be barred in criminal cases where you find out information that's of intelligence—and I would say investigation related to terrorism and international terrorism, which in a criminal wiretap ought to be turned over to appropriate agencies under proper circumstances.

That's a sharing issue, not a standard issue. That's why the unwillingness to share and clarifying that is an important thing we can work on. It requires some surgery. So you preserve that standard.

There are issues. You try to extend the length of a surveillance to a year, where foreign persons are concerned, and 90 days for physical surveillance. The issue there is that we're talking about secret searches again which never get disclosed. The judicial supervision is to ensure that there are not fishing expeditions, and the question is, since no FISA wiretap or extension except one has been turned down in the 22-year history of the statute, what is the bureaucratic problem of continuing that supervision?

I did not hear an explanation of why that's necessary. That's one section we have a concern.

I do have a concern in your bill with the gathering of machine instructions to a computer. I don't know how you pick those bits and bytes out of the air. Dealing with the computer, bits are bits, and instructions that may look like maybe a non-human communication to a computer also may contain packets which are communications. We need to figure out how to sort that out. That takes a little time.

But still, you're on the track of trying to maintain the demarcation. You need to look carefully at the Justice Department bill because it has vast implications for your mission, both intelligence and protecting our civil liberties. It breaks down that purpose, the primary purpose test. It allows roving wiretap authority, which is available in law enforcement, but under much broader discretion. It's not tied to any device. You're not just following telephones, you're following a person. Does that mean that you can follow the person to any computer they are using, or can you follow them to

a park and use electronic surveillance with a spike mike on whoever they are talking to?

These need to be examined. So there are expansions that need. Again, in terms of maintaining your intelligence mission, turning over grand jury information to the White House for intelligence purposes and not just to intelligence agencies is a very serious question. Maybe it should occur in an intelligence investigation, but you need to look at compromising sources and methods, the implications of having that information turned over. A grand jury investigation, from law enforcement investigation, wiretaps, not only to the intelligence but the other people in the Administration, what is the implications of those standards being taken down.

I want to emphasize that they are not only breaching the wall on the intelligence side but on the law enforcement side lowering authorities in the name of going after international terrorism which apply across all criminal investigations, not just terrorism investigations and then not just using information-sharing from the criminal side for terrorism investigations but in a wide range for any intelligence purpose. That is a very broad, sweeping change in our law.

I could go on to business records and privacy issues that it raises. There is a lot to examine, and since I cannot on the public record find any of the sweeping authority that they already have having interfered with this investigation in any way, that it was an intelligence failure and not a restrictions failure, why can't we take the time and go through this in a careful way, maybe a couple months, but to try and have a statute on the President's desk in 2 weeks without floor action is not the appropriate way to strike the balance between national security and civil liberties.

Thank you.

Chairman GRAHAM. Ms. Martin.

[The prepared statement of Ms. Martin follows:]

STATEMENT OF MORTON H. HALPERIN, CHAIR, ADVISORY BOARD, AND KATE MARTIN, DIRECTOR, ON BEHALF OF THE CENTER FOR NATIONAL SECURITY STUDIES

Thank you Mr. Chairman and Vice Chairman for the opportunity to testify today on behalf of the Center for National Security Studies. The Center is a civil liberties organization, which for 30 years has worked to ensure that civil liberties and human rights are not eroded in the name of national security. The Center is guided by the conviction that our national security must and can be protected without undermining the fundamental rights of individuals guaranteed by the Bill of Rights. In its work over the years on legislation from the Foreign Intelligence Surveillance Act to the Intelligence Oversight Act, the Center has begun with the premise that both national security interests and civil liberties protections must be taken seriously and that by doing so, solutions to apparent conflicts can often be found without compromising either.

We appear before you today at a time of great mourning, when it is difficult to turn our thoughts and attention from anything but our grief and trouble. And we appreciate the enormous efforts of those individuals who have put their own grief aside to concentrate on searching for survivors, comforting those who have suffered most directly and finding and holding accountable the perpetrators of these crimes.

It is not too soon to begin thinking about how we can improve our ability to prevent such unspeakable events from occurring again. However, as we do so we must resolve to act in a way that protects our liberties as well as our security and which recalls the lessons of the past from times when we permitted our concerns for security to accept erosions of our liberty that we now regret. The Alien and Sedition Acts, the Internment of Japanese Americans, McCarthyism, and the efforts of intelligence agencies and the FBI to disrupt the civil rights and anti-war movements

were not our proudest moments. We must not repeat them or lay the seeds for future abuses.

We owe it to all those innocent people who were murdered to reflect upon those basic principles and values which should inform our discussion today. What distinguishes us as a people from our fellow human beings who committed these terrible acts is our commitment to law and to individual freedom. It is a commitment to law made deliberately, with calm reflection and an opportunity for public debate. The genius of democracy is the understanding that in the noisy and seemingly inefficient marketplace of ideas, the wisest decisions will be made. And certainly there is no more important subject than how to protect both our liberty and security most especially at a time like this when both may be so at risk. The American people look to the Members of this Committee to make law as the founders of the Constitution envisaged when they set up this legislative body, after a full public debate informed by facts, analysis and the chance for reflection. We owe nothing less to those who have been killed and to our children born and to be born.

We commend the Chair and the Vice Chair for their hard work and quick action to outline proposals intended to help prevent such horrific acts in the future and to focus on needed structural reforms in the Intelligence Community. We are grateful to this committee for holding public hearings and for inviting the Center for National Security Studies to testify. At the same time, we call upon this committee not to precipitously make changes to long-standing rules on some of the most technically complicated and difficult issues before the Congress.

In urging you to proceed calmly and deliberately we speak on behalf of a coalition of more than 140 organizations from all ends of the political spectrum who last week all agreed on a Statement, which reads in part:

IN DEFENSE OF FREEDOM

> This tragedy requires all Americans to examine carefully the steps our country may now take to reduce the risk of future terrorist attacks. We need to consider proposals calmly and deliberately with a determination not to erode the liberties and freedoms that are at the core of the American way of life. We need to ensure that actions by our government uphold the principles of a democratic society, accountable government and international law, and that all decisions are taken in a manner consistent with the Constitution. We can, as we have in the past, in times of war and of peace, reconcile the requirements of security with the demands of liberty. We should resist the temptation to enact proposals in the mistaken belief that anything that may be called anti-terrorist will necessarily provide greater security. We must have faith in our democratic system and our Constitution, and in our ability to protect at the same time both the freedom and the security of all Americans.

I ask permission, Mr. Chairman to submit for the record as an attachment to my statement the full statement of the In Defense of Freedom coalition and a list of the organizational and individual signers of the statement. The danger of haste is not just to our civil liberties but equally to our security. We face an equal danger that in the understandable rush to do something, what is done will not be effective in making us any safer, that it will substitute for the difficult analysis and work that is needed to figure out just how to prevent such attacks in the future. This is particularly true with regard to widening surveillance of Americans, where extending the net of surveillance, rather than doing the difficult work of trying to figure out who should be targeted, may well lead to information overload, where it will not be possible for the government to distinguish the important from the insignificant.

We have had the Chairman's bill since Saturday morning and the administration's proposals being considered by this committee for 2 days more than that. We have done our best to provide the Committee with our preliminary analysis of the proposals.

But most significantly, we urge you before acting, to hold additional hearings, to obtain in writing the careful analyses needed of what the current authorities are and what changes would be effected by these proposals, why such changes would be useful and what the risks will be. These are very technical and complicated issues, with enormous implications for both civil liberties and our security and we need to act carefully.

If there are specific authorities immediately needed by the current investigators into last week's acts, those authorities could be separated from the rest of the proposals and considered as quickly as possible. But those proposals designed to prevent such intelligence failures in the future, can only be done wisely and effectively

after more is known about the cause of the failure and a public discussion about how to fix them.

On the subject of haste, we welcome the provision that would undo the hasty action of the Senate 10 days ago in repealing the DCI guidelines on recruitment of assets involved in terrorism or other human rights violations. That provision (sec. 815 in the September 13 amendment to H.R. 2500) was apparently based on the misunderstanding that the existing guidelines had prevented the CIA from recruiting terrorist informants, when the guidelines in fact simply required procedures intended to insure that the appropriate high level officials at the agency approved the use of any such informants. They were adopted in response to the report by the President's Intelligence Oversight Board that the CIA had not kept this committee informed as required by law of serious human rights violations. We understand that Section 103 of S. 1448, the Graham-Feinstein bill is intended to override section 815 passed September 13 by specifically authorizing what is already the case, that the CIA may use terrorist informants. We would suggest that the section 103 simply be amended to add that agency officers may do so "pursuant to guidelines or directives issued by the agency."

We have organized our discussion of the proposals before the Committee into three categories:

- Changes to the Foreign Intelligence Surveillance Act.
- Proposal to allow wiretap evidence obtained overseas in violation of Fourth Amendment standards to be introduced against Americans in U.S. courts; and
- Changes to the current authorities of the Director of Central Intelligence and rules regarding sharing of information gathered on Americans with the Intelligence Community.

I. PROPOSED CHANGE TO THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

We have attempted to coordinate our testimony with that being presented by the Center for Democracy and Technology. Mr. Berman will provide you with detailed comments on the specific provisions, but since one of us was intimately involved in the lengthy negotiations which led to the enactment of FISA, we wanted to provide you with some general remarks relating to the structures and purposes of FISA and of the efforts to protect civil liberties while giving the government the authority it needed to conduct electronic surveillance to gather foreign intelligence.

It is important to remember that FISA was a grant of authority to the government to conduct surveillance, which the Supreme Court had held was clearly within the ambit covered by the Fourth Amendment. The Court had suggested that the warrant requirements of the Fourth Amendment might be different in national security matters and Congress and the Administration worked together, with the active involvement of outside groups and scholars, over a period of several years to craft the careful compromise incorporated in FISA.

At the heart of FISA was this trade. Congress would authorize electronic surveillance of foreign powers and their agents within the United States under a standard different and less stringent than required for national security wiretaps and it would authorize the government never to tell the targets that their conversations were intercepted. In return the government accepted greater judicial involvement and oversight of the process (carried out in an ex parte rather than adversarial manner however) and a wall to insure that it did not use these procedures to gather information for criminal prosecutions.

Proposals to alter FISA need to be understood in this context. It is not an anomaly that the government has to go back to court more often than under Title III to get authority to continue surveillance of a private person lawfully resident in the United States. Since the person will never be told of the surveillance nor have an opportunity to move to have the surveillance records purged, it is important that a judge check regularly, at least as a surveillance begins, to be sure that the government's suspicion that the person was acting as the agent of a foreign power was correct and that the surveillance was producing foreign intelligence information while minimizing the collection of other information.

We urge you to keep this basic structure in mind as you consider objections to specific provisions. We urge also that you remember the care with which FISA was enacted and maintain the same spirit of skepticism and openness as this committee considers the proposed amendments.

In this connection, it is also important to remember that investigations of terrorism pose particularly difficult problems because of the intersection of First Amendment, Fourth Amendment and national security concerns. Unlike international narcotics investigations, it is important to distinguish between those engaged in criminal terrorist activity and those who may share in the religious or po-

litical beliefs of the terrorists, or even their ethnic background, without engaging in any unlawful acts.

Regarding specific proposals on both FISA and changes to other statues permitting national security investigations of financial records and other information, we refer you to Mr. Berman's testimony in addition to our comments below.

Elimination of the Primary Purpose Requirement, Administration Bill Sec. 153

We want to stress our concern, as spelled out by Mr. Berman, about the administration's proposal to eviscerate the original premise of the FISA, that its procedures would only be employed when the primary purpose of the surveillance was to gather foreign intelligence. The administration's proposal in section 153 would turn the statutory scheme on its head by allowing the use of FISA surveillance when the government's primary purpose is to bring criminal charges against an individual, a change which we believe would violate basic Fourth Amendment guarantees.

Duration of Authority to Conduct Surveillance and Searches of Non-U.S. Persons Under FISA. Graham-Feinstein Bill, Sec. 202, Administration Bill, Sec. 151

These sections would extend the period allowed for the conduct of FISA surveillance and searches of non-U.S. persons from 90 days and 45 days respectively, to 1 year for both surveillance and searches. For the reasons outlined above, the current limitations are an integral part of the balance intended to provide judicial supervision of the use of secret wiretaps and secret searches targeted against individuals, who, while not permanent residents or U.S. citizens may well be long-time legal residents and are protected by the Fourth Amendment. The statute currently provides 1-year authorization for surveillance and searches of embassies and similar establishments, because the Fourth Amendment does not apply to foreign embassies. If there is some necessity, other than to avoid inconvenience, for longer authorizations for individuals, we would suggest considering an amendment that would allow extended authorizations on a second application if the government made a showing that the initial surveillance or search did in fact obtain foreign government information. In such a case, the second order could authorize electronic surveillance for an additional 6 months, rather than the current 90 days, and authorize physical searches for 90 days rather than the currently allowed 45 days.

II. PROPOSAL TO ALLOW WIRETAP EVIDENCE OBTAINED OVERSEAS IN VIOLATION OF FOURTH AMENDMENT STANDARDS TO BE USED AGAINST AMERICANS IN U.S. COURTS, ADMINISTRATION BILL, SECTION 105

As described by the administration, section 105 of its bill would provide that United States prosecutors may use against American citizens information collected by a foreign government even if the collection would have violated the Fourth Amendment. As the administration points out, as criminal law enforcement becomes more of a global effort, such information will come to play a larger role in Federal prosecutions and indeed other provisions of the administration bill would extend the extraterritorial reach of U.S. criminal law to even more crimes than are currently covered today.

Section 105 would for the first time codify the extraordinary view that as the United States works to promote the rule of law throughout the world and to extend the reach of U.S. criminal law, it should leave the Bill of Rights behind. Implicit in this approach is the view that the Constitution is merely an inconvenience to law enforcement rather than acknowledging it as the best instrument yet written to govern the relations of a government to the governed.

Certainly, it is not obvious how to implement the protections of the Fourth Amendment against unreasonable searches and seizures in a new era of global law enforcement. It is an issue that has just begun to be examined by the courts. While a bare majority of the Supreme Court has held that the Fourth Amendment does not apply to the search and seizure of property owned by a nonresident alien and located in a foreign country, (*United States* v. *Verdugo-Urquidez*, 494 U.S. 259) it has affirmed that the Fifth and Sixth Amendments do protect Americans overseas. *Reid* v. *Covert*, 354 U.S. 1 (1957). The question must also be considered under international human rights law, as it is quite likely that unreasonable searches and seizures that don't meet Fourth Amendment standards also violate existing human rights treaties signed by the United States. The question of how to implement Fourth Amendment protections for overseas searches will probably at some point require congressional action, but it is a difficult and complicated issue that cannot be adequately addressed in the context of an emergency response to last week's terror attack.

III. CHANGES TO CURRENT LAW CONCERNING SHARING OF INFORMATION ON AMERICANS WITH THE INTELLIGENCE COMMUNITY

Several provisions of both bills would significantly change current statutory authorities and responsibilities for conducting terrorism investigations involving Americans or other U.S. persons inside the United States. The problem of effective coordination between such investigations and overseas intelligence activities is certainly one of the most important ones before this Committee. It is also one of the most difficult, both in terms of actually insuring effective investigations and making sure that the unintended consequences are not to repeal crucial protections for individual rights.

Since the creation of the CIA in the 1947 National Security Act, there has been an attempt to distinguish between law enforcement, the collection of information on Americans and others to be used in criminal prosecutions of individuals, and foreign intelligence, the collection of information about the plans, intentions and capabilities of foreign governments and organizations. When the CIA was created, its charter specifically prohibited the agency from any "law enforcement or internal security functions" 50 U.S.C. 403–3(d)(1). As was documented in the Church committee report, it was the blurring of the distinction between law enforcement and foreign intelligence national security investigations that led to the abuses by the intelligence agencies outlined in that report. Many of the reforms intended to prevent such abuses from happening again, were explicitly predicated upon recognizing the differences between law enforcement and intelligence, they have different objectives and require different means and different rules should apply in order to protect individual liberties. The most obvious examples are the different rules for criminal wiretaps set out in Title III and for foreign intelligence wiretaps in the Foreign Intelligence Surveillance Act, as well as the two sets of Attorney General guidelines governing FBI investigations, one for General Crimes, including domestic terrorism, and a different set for Foreign Counter-Intelligence investigations.

At the same time, it has always been recognized that some matters, most particularly internationally-sponsored terrorism and espionage on behalf of foreign powers implicate both law enforcement and foreign intelligence concerns. In the past few years, there has been an increasing number of situations where intelligence and law enforcement interests coincide and there are a substantial number of executive branch regulations, directives, working groups and practices that have been developed to address the myriad specific issues that are involved; for example reconciling the need for intelligence agencies to keep the identities of their human sources a secret with due process requirements that a criminal defendant be informed of the evidence against him and allowed to cross-examine his accusers.

The threat of terrorism obviously requires effective and close coordination between the Intelligence Community and law enforcement. We welcome these proposals as the first step toward examining whether statutory changes are now needed. However, we urge the Committee to take the time to examine the issue in depth beginning with an analysis of existing rules and practices. Nothing is more central to the protection of the liberties of Americans from the abuses of the past than the distinction between law enforcement and intelligence. The current proposals would be a sea change in laws that have been on the books for 30 years. Before that is done, we urge the Committee to act slowly and deliberately. We would welcome the opportunity to sit down with you and the Judiciary Committee together to work on solutions that will ensure an effective anti-terrorism effort without sacrificing individual liberties.

The specific provisions at issue include the following sections in the Department of Justice draft:

Section 103, repealing the present prohibition on disclosing Title III intercepts of Americans' conversations to the Intelligence Community, other than the FBI.

Sections 154 and 354, repealing the present prohibitions on sharing grand jury information and other criminal investigation information with the Intelligence Community, other than the F1BI.

The provisions in the Graham-Feinstein bill on this subject, are much narrower. However, they would also effect an important shift in current responsibilities that needs much more extensive discussion and analysis, before being acted upon. Specifically, Section 101 would shift from the Attorney General to the Director of Central Intelligence the responsibility for determining which Americans should be targeted for FISA surveillance.

Section 102 of the Graham-Feinstein bill would also change the foreign intelligence definitions in the National Security Act of 1947.

This provision would change the definitions in the National Security Act of 1947 so that "international terrorism" is included in the definition of "foreign intelligence"

rather than "counterintelligence." While, this may be a wise idea, it requires an extensive reading of the many and various laws and regulations which incorporate the current definitions in the Act to determine what the effect of the change would be, which we have not had an opportunity to do.

MISCELLANEOUS. SEC. 104 TEMPORARY AUTHORITY TO DEFER REPORTS TO CONGRESS

This seems like a good way to insure that adequate resources may be directed to the September 11 attack while also insuring that the Congress continue to receive the information required by the Intelligence Oversight Act on all intelligence activities. In this connection, we note that paragraph (c) entitled "Exception for Certain Reports" should refer to section 501 of the National Security Act (50 U.S.C. 413) as well as to sections 502 and 503 (50 U.S.C. secs 413a and 413b).

IN DEFENSE OF FREEDOM AT A TIME OF CRISIS

1. On September 11, 2001 thousands of people lost their lives in a brutal assault on the American people and the American form of government. We mourn the loss of these innocent lives and insist that those who perpetrated these acts be held accountable.

2. This tragedy requires all Americans to examine carefully the steps our country may now take to reduce the risk of future terrorist attacks.

3. We need to consider proposals calmly and deliberately with a determination not to erode the liberties and freedoms that are at the core of the American way of life.

4. We need to ensure that actions by our government uphold the principles of a democratic society, accountable government and international law, and that all decisions are taken in a manner consistent with the Constitution.

5. We can, as we have in the past, in times of war and of peace, reconcile the requirements of security with the demands of liberty.

6. We should resist the temptation to enact proposals in the mistaken belief that anything that may be called anti-terrorist will necessarily provide greater security.

7. We should resist efforts to target people because of their race, religion, ethnic background or appearance, including immigrants in general, Arab Americans and Muslims.

8. We affirm the right of peaceful dissent, protected by the First Amendment, now, when it is most at risk.

9. We should applaud our political leaders in the days ahead who have the courage to say that our freedoms should not be limited.

10. We must have faith in our democratic system and our Constitution, and in our ability to protect at the same time both the freedom and the security of all Americans.

Endorsed by:

Al-Fatiha Foundation, *Washington, DC*
Alliance for Justice, *Washington, DC*
American-Arab Anti-Discrimination Committee, *Washington, DC*
American Association of Law Libraries, *Washington, DC*
American Association of University Women, *Washington, DC*
American Civil Liberties Union, *Washington, DC*
American Conservative Union, *Alexandria, VA*
American Federation of State, County and Municipal Employees, *Washington, DC*
American Friends Service Committee—Washington Office, *Washington, DC*
American Humanist Association, *Washington, DC*
American Immigration Lawyers Association, *Washington, DC*
American Liberty Foundation, *Alexandria, VA*
American Muslim Alliance, *Newark, CA*
American Muslim Council, *Washington, DC*
American Policy Center, *Warrenton, VA*
Americans for Democratic Action, *Washington, DC*
Americans for Religious Liberty, *Silver Spring, MD*
Americans for Tax Reform, *Washington, DC*
Amnesty International—USA, *Washington, DC*
Arab American Institute, *Washington, DC*
Asian American Legal Defense and Education Fund, *New York, NY*
Asian Pacific American Labor Alliance, *Washington, DC*
Association for Competitive Technology, *Washington, DC*
Association of American Physicians and Surgeons, *Tucson, AZ*
Baptist Joint Committee on Public Affairs, *Washington, DC*
Benton Foundation, *Washington, DC*

California First Amendment Coalition, *Sacramento, CA*
Campaign for America, *Washington, DC*
Catholic Vote.org, *Washington, DC*
Center for Democracy and Technology, *Washington, DC*
Center for Digital Democracy, *Washington, DC*
Center for Economic and Social Rights, *Brooklyn, NY*
Center for Media Education, *Washington, DC*
Center for National Security Studies, *Washington, DC*
Chinese for Affirmative Action, *San Francisco, CA*
Citizens and Immigrants for Equal Justice, *Mesquite, TX*
Citizens Committee for the Right to Keep and Bear Arms, *Bellevue, WA*
Citizens' Commission on Civil Rights, *Washington, DC*
Civil Rights Forum on Communications Policy, *Washington, DC*
Common Cause, *Washington, DC*
Common Sense for Drug Policy Legislative Group, *Washington, DC*
Competitive Enterprise Institute, *Washington, DC*
Consumer Action, *San Francisco, CA*
Council on American Islamic Relations, *Washington, DC*
Criminal Justice Policy Foundation, *Washington, DC*
Democracy Foundation, *Ballwin, MO*
Doctors for Disaster Preparedness, *Tucson, AZ*
Drug Reform Coordination Network, *Washington, DC*
Eagle Forum *Washington, DC*
Eagle Forum of Alabama, *Birmingham, AL*
Electronic Privacy Information Center (EPIC), *Washington, DC*
Ethics & Religious Liberty Commission of the Southern Baptist Convention, *Nashville, TN*
Families Against Mandatory Minimums Foundation, *Washington, DC*
Family Violence Clinic, *Columbia, MO*
Federation of American Scientists, *Washington, DC*
First Amendment Foundation, *Washington, DC*
Free Congress Foundation, *Washington, DC*
Free the Eagle, *Fairfax, VA*
Freedom of Information Center, *Columbia, MO*
Friends Committee on National Legislation, *Washington, DC*
Fund for New Priorities in America, *New York, NY*
Fund for the Fourth Amendment, *Washington, DC*
Global Strategic Management, *Annapolis, MD*
God Bless America, http://myweb.ecomplanet.com/GOBA1953/defauft.htm
Government Accountability Project, *Washington, DC*
Gun Owners of America, *Springfield, VA*
Harvard Information Infrastructure Project at Harvard University, *Cambridge, MA*
Health Privacy Project, Georgetown University, *Washington, DC*
Human Rights Watch, *Washington, DC*
International Religious Liberty Association, www.irla.org
Independent Institute, *Oakland, CA*
Islamic Institute, *Washington, DC*
James Madison Project, *Washington, DC*
Japanese American Citizens League, *San Francisco, CA*
Latina and Latino Critical Legal Theory, Inc., *Coral Gables, FL*
Lawyers Committee for Human Rights, *Washington, DC*
Leadership Conference on Civil Rights, *Washington, DC*
Lindesmith Center—Drug Policy Foundation, *New York, NY*
MoveOn.org, *Washington, DC*
Multiracial Activist & Abolitionist Examiner, *Alexandria, VA*
Muslim Public Affairs Council, *Washington, DC*
National Asian Pacific American Bar Association, *Washington, DC*
National Asian Pacific American Legal Consortium, *Washington, DC*
National Association for the Advancement of Colored People, Board of Directors, *Washington, DC*
National Association of Criminal Defense Lawyers, *Washington, DC*
National Black Police Association, *Washington, DC*
National Coalition to Protect Political Freedom, *Washington, DC*
National Committee Against Repressive Legislation, *Washington, DC*
National Consumers League, *Washington, DC*
National Council of Churches of Christ, *Washington, DC*
National Council of La Raza, *Washington, DC*
National Gay and Lesbian Task Force, *Washington, DC*

National Lawyers Guild, *New York, NY*
National Legal Aid and Defender Association, *Washington, DC*
National Native American Bar Association, *Birmingham, AL*
National Youth Advocacy Coalition, *Washington, DC*
Net Action, *San Francisco, CA*
Network: A National Catholic Social Justice Lobby, *Washington, DC*
Nuremberg Legacy Project, *Washington, DC*
North American Council for Muslim Women, *Great Falls, VA*
OMB Watch, *Washington, DC*
Patrick Henry Center for Individual Liberty, *Fairfax, VA*
People for the American Way, *Washington, DC*
Philadelphia II, *Washington, DC*
Physicians for Human Rights, *Washington, DC*
Privacilla.org, http://www.privacilla.org
Privacyactivism.org, *Bellevue, WA*
Privacy International, *Washington, DC*
Privacy Rights Clearinghouse, *San Diego, CA*
Privacy Times, *Washington, DC*
Project On Government Oversight, *Washington, DC*
Research & Policy Reform Center, *Washington, DC*
Rutherford Institute, *Charlottesville, VA*
Second Amendment Foundation, *Bellevue, WA*
Sentencing Project, *Washington, DC*
Seventh-Day Adventist Church, World Headquarters, *Silver Spring, MD*
Sixty Plus Association, *Arlington, VA*
Society of American Law Teachers, *Minneapolis, MN*
Sovereign Society, Ltd., *Baltimore, MD*
Square One Media Network, *Seattle, WA*
Strategic Issues Research Institute, *Arlington, VA*
Unitarian Universalist Association of Congregations, *Washington, DC*
United Church of Christ, Justice & Witness Ministries
United States Committee for Refugees & Immigration and Refugee Services, *Washington, DC*
USAction, *Washington, DC*
Washington Lawyers' Committee for Civil Rights and Urban Affairs, *Washington, DC*
WILD for Human Rights, *San Francisco, CA*
Women's International League for Peace and Freedom, U.S. Section, *Washington, DC*

STATEMENT OF KATE MARTIN, DIRECTOR, CENTER FOR NATIONAL SECURITY STUDIES

Ms. MARTIN. Thank you, Mr. Chairman and Mr. Vice Chairman, for the opportunity to testify here today on behalf of the Center for National Security Studies, an organization which has for 30 years worked to protect civil liberties from being eroded in the name of national security.

We appear today before you at a time of deep mourning, when it is in fact quite difficult to turn our attention to this kind of issue and to anything other than our grief and sorrow at the losses that we all suffered. At the same time, we recognize that it is not too soon to begin thinking about how we can improve our ability to prevent such unspeakable events from occurring again. However, as we do so we must resolve to act in a way that protects our liberties as well as our security and which recalls the lessons of the past from times when we were permitting our concerns for security to accept erosions of our liberties that we now regret.

What distinguishes us as a people from our fellow human beings who committed these terrible acts is our commitment to law and individual freedom. It is a commitment to law made deliberately, with calm reflection and with opportunity for public debate. Cer-

tainly there is no more important subject than how to protect both our liberty and our security. The American people look to the Members of this Committee to make law as the founders of the Constitution envisioned when they set up this legislative body, after a full public debate informed by facts, analysis and the chance for reflection.

We commend the Committee for its hard work and quick action to outline proposals intended to help prevent such horrific acts in the future and to focus on needed structural reforms in the Intelligence Community. We are grateful to the Committee for holding these public hearings and for inviting representatives of our community to testify.

At the same time, we call upon this Committee not to precipitously make changes to longstanding rules on some of the most technically complicated and difficult issues before the Congress, with enormous implications for civil liberties. In urging reflection and time for calm deliberation, we speak on behalf of a coalition of more than 140 organizations from all ends of the political spectrum who last week agreed upon a joint statement to the Congress urging such calmness. That statement I have attached to my prepared remarks.

I want to mention that the danger of haste of course is not just to civil liberties but equally to our security. We face an equal danger that in the understandable rush to do something what is done will not be effective in making us any safer, that it will substitute for the difficult analysis and work that is needed to figure out just how to prevent such attacks in the future. This is particularly true with regard to widening surveillance of Americans where extending the net of surveillance rather than doing the difficult work of trying to figure out who should be targeted may well lead to information overload where it will not be possible for the Government to distinguish the important from the insignificant.

We have had the Chairman's bill since Saturday morning and the Administration's proposals being considered by this Committee for 2 days longer than that. We have done our best to provide the Committee with our preliminary analysis of the proposals and it is attached in our written statement. But most significantly, we urge you before acting to hold additional hearings to obtain in writing the careful analyses needed of what the current authorities are and what changes would be effected by these proposals, why such changes would be useful, and what the risks will be.

If there are specific authorities immediately needed by the current investigators into last week's acts, those authorities could be separated from the rest of the proposals and considered as quickly as possible. But those proposals designed to prevent such intelligence failures in the future, as Senator Shelby mentioned, can only be done wisely and effectively after more is known about the cause of the failure and we have a public discussion about how to fix them.

I just wanted to mention on the subject of haste we applaud the Chairman's bill in undoing what the Senate did on September 13 when it overruled the DCI guidelines on the recruitment of assets and we suggest that the provision about the recruitment of assets that's contained in the Chairman's bill is the appropriate way to

deal with that issue, and we would only suggest that, in line with some of the comments made by earlier witnesses, that the section could be amended to add that Agency officers may recruit terrorist informants "pursuant to guidelines or directives issued by the Agency."

I want to basically, I think, second Mr. Berman's remarks about particular changes to the Foreign Intelligence Surveillance Act and to the information-sharing authorities and just make a couple of brief comments about those.

I think it's important to keep in mind that what the Foreign Intelligence Surveillance Act does is authorizes secret surveillance and secret searches of the houses of Americans, and it does so in the context of a carefully drafted statute which many individuals in this room spent some number of months and years working out. We urge you to keep this in mind as you consider amending the statute and that you remember the care with which FISA was enacted. We especially urge you to remember that investigations of terrorism, while perhaps the most important undertaking for the Intelligence Community in the near or perhaps long-term future, at the same time pose the most difficult constitutional problems with regard to collection of information and investigations of Americans.

That is because of the unique intersection of first amendment, fourth amendment, and national security concerns involved in the investigation of Americans for terrorist activity. Unlike international narcotics investigations, for example, it is important to distinguish between those engaged in criminal terrorist activity and those who may share in the religious or political beliefs of the terrorists and even their ethnic background without, however, engaging in any unlawful acts. For 30 years we have had on the books a set of statutes and an even more extensive set of Agency guidelines, some classified and some public, all of which are designed to address the problem of effective investigation of terrorist activity while not infringing on first amendment rights and not targeting individuals based on their ethnic background.

Before those provisions are changed, we urge the Committee to take the time to sit down and look at what the perhaps unintended consequences might be of basic statutory changes.

I think I won't talk at the moment about the primary purpose requirement. I do believe, however, that this Committee has a constitutional responsibility itself to determine whether or not in your view the lower standards of FISA authorizing secret searches and secret surveillance would be constitutional if the primary purpose requirement were to be eliminated. I do not think it is an answer to say that the court will not address that question except on a case-by-case basis. I think this Committee and this body has a constitutional obligation to make that determination, not only in terms of its national security responsibilities but even more so in terms of its responsibility to protect individual liberties.

I want to just mention that we have serious concerns about the proposal that would allow wiretap evidence obtained overseas in violation of fourth amendment standards to be used against Americans in the U.S. courts. This is also a new and very difficult legal issue that comes about as part of the ever-increasing globalization of U.S. law enforcement. Without, I believe, adequate thought or

adequate development of the law in the court, the Administration proposal would for the first time codify the extraordinary view that as the United States works to promote the rule of law throughout the world and to extend the reach of our criminal law it should leave the Bill of Rights behind.

Implicit in this approach is the view that the Constitution is merely an inconvenience to law enforcement rather than an acknowledgment of it as the best instrument yet written by human beings to govern the relations of a government to the governed. Certainly it is not an easy question as to how to apply fourth amendment standards to searches and seizures of evidence gathered overseas to be used in the U.S. court. We suggest that it is an issue that at some time will most likely require congressional action and congressional determination. We suggest that in the terrible days following last week's tragedy is not the time to address that problem.

Finally, there is the question of the changes to the authorities and the responsibilities for information-sharing between the Intelligence Community and the law enforcement community about terrorism. This is, I believe, one of the most serious and difficult problems facing this Committee and this country at this moment. There is no doubt about it that the threat of terrorism requires effective and close coordination between the Intelligence Community and law enforcement. It is also true, though, that since the creation of CIA, when the National Security Act provided explicitly that the CIA would have no law enforcement or internal security functions, that we have recognized that the division and the distinction between law enforcement and intelligence is very important in protecting civil liberties.

At the same time, of course, we have recognized that there are areas like terrorism and espionage which overlap both intelligence and law enforcement. Nevertheless, we have a whole series of both statutes and present guidelines and directives on the books that recognize the distinction and in fact are premised on that distinction—for example, the FISA and Title III or the Attorney General guidelines for the conduct of FBI investigations, one of which is classified and covers foreign intelligence matters and one of which covers general crimes.

Before we change the authorities set forth in the National Security Act we believe it's important to have a careful and cautious examination of what the effect would be of changing those longstanding authorities, with an eye again, let me stress, to improving the needed coordination between the two communities to provide the most effective kind of both law enforcement and intelligence against terrorist organizations, but to do that in a way that is respectful and protects the liberties in this country.

Thank you.

Chairman GRAHAM. Thank you very much, Ms. Martin, and thank you to each of the panelists.

In your three comments the importance of our appreciation of the wall, as you described it, Mr. Berman, between using intrusive surveillance for foreign intelligence purposes and using intrusive surveillance for criminal purposes is a caution that is well placed and that we do need to keep very much in the forefront.

One of the areas in which this is raised with particular stark impact would be if we were to amend the law to say that you could get a FISA wiretap with something less than foreign intelligence being the primary purpose. As I gather, the recommendation of the Attorney General is that we eliminate that standard and then leave it up to the FISA court on a case-by-case basis to make judgments of if it's not the primary purposes, if it's 50/50 or if it's 40/60, where do you reach the point where you do lose the constitutional basis for a FISA tap.

To put that into its context, and if you feel, Mr. Smith, based on your previous background and current understanding, especially your role at the CIA, what is the problem that is raised by using the primary purpose standard as the basis of getting a FISA wiretap? What are the kind of cases that are compromised or threats to our security that are tolerated because we use this high standard for getting a FISA wiretap?

Mr. SMITH. In my experience, Mr. Chairman, what happens is that oftentimes it's not clear at the outset of an investigation whether this should be pursued as a law enforcement matter and ultimately possibly prosecution or simply to collect foreign intelligence and take action later on. Oftentimes you'll start down one road and find that you have to shift to another.

The question as I understand it with respect to "a" versus "the" is whether or not, particularly in the case of a U.S. person, the courts would ultimately hold that the test had been met under the fourth amendment to engage in this intrusive surveillance.

I'm not sure I know what the right answer is. My guess is that the folks in OLC at the Justice Department are right, namely that, depending on the facts of the cases as they come along, the courts would be willing to give a considerable deference if, for example, the first criminal cases that go to court are foreign nationals who presumably have fewer fourth amendment rights than Americans. They might not be so troubled if it's just "a" purpose and it then turns into a prosecution. In the case of a U.S. person, it may come out quite differently.

I think my colleagues on the panel are right. This is a hard issue and needs a lot of careful thought, and I think the Administration ought to be asked quite directly why do you need this. Why can you not proceed under the current procedures? I don't know the answer to that one.

Mr. BERMAN. I think the record is they haven't had difficulty here, and if you turn up in your intelligence investigation that you've got a money-laundering case, your bill says go get a title III warrant. Again I come back and say that if there is a wall between a criminal investigation with wiretapping, sharing relevant information in the middle of an investigation of money laundering it turns out that someone's laundering money for bin Ladin and that comes up in a criminal wiretap, there's the grounds for a FISA tap, which I think is probably already on, but there ought to be some way to turn that information over to an intelligence agency.

There's an information-sharing issue which may be a restriction in both statutes that could be worked on. But it's not the standard; it's the sharing of the data.

I also think that if you went on a fast-track/slow-track that you could take the most troubling issues of when you might get information about a terrorist investigation in a grand jury. I think that the Justice Department and the CIA will make strong cases that there are circumstances when use of illegal wiretap information may be critical in such a case. But rather than amending the criminal statutes across the board to provide that kind of information for any intelligence purpose, why don't we try and craft a terrorism section that deals with this crisis and the special circumstances of a new kind of enemy, one that we've got to be careful. Kate's absolutely right that this is an intersection between national security, law enforcement and civil liberties.

The new terrorist target is someone who drinks Bud, has a college education, goes to work at some company that Jeff may be representing, and lives in Laurel. How do we do that kind of targeting and not be over broad and at the same time, while we're worrying about collateral damage in Afghanistan, so we don't prevent our ability to penetrate those organizations by making everyone hate us across the whole Islamic world, you don't want the same thing to happen here.

Over-surveillance, the sense that there is an agent behind every bush, will make innocent people of that community stop talking to our agents. That's what happened in Watergate and you don't want it to happen here. It will be counterproductive not just to civil liberties but to your intelligence mission.

Vice Chairman SHELBY. Mr. Chairman.

Chairman GRAHAM. Yes, Senator.

Vice Chairman SHELBY. I appreciate all of your testimony, and, Jeff, we welcome you back here.

As I understand it—and I'll direct this to all of you, my observation first and then a question—under the criminal investigations you have today do the statutes afford the FBI roving tap authority for intelligence investigations? In other words, they would like what they now have for criminal investigations; is that right, Mr. Berman?

Mr. BERMAN. They have it for criminal investigations. It's always with a shudder. I'm not saying we like it, because you particularize things. I think that following telephones under FISA may make sense, but the way that it's drafted it's not clear that it's tied to devices any more; it's tied to the person and wherever that person is. We need some explanation of what they mean by that.

Vice Chairman SHELBY. As we discuss this matter, we're mindful of the Constitution, which grants us our rights. But we are also mindful here today of a heck of a challenge to our way of life, and what we want to do is have some balance. We do not want to destroy our constitutional rights for our citizens, but at the same time we want to give, if we can, under the auspices of the Constitution, the tools to the Justice Department and the FBI to fight this and win this without doing damage to the rest of us. Isn't this what we're trying to achieve?

Mr. BERMAN. I think we can do that. It doesn't require meeting the content standard. It can be a lower standard. But it needs to be more carefully drafted.

Vice Chairman SHELBY. The precision of language is very important, as we all know, and words have meanings, and whatever we do we ought to do carefully. But I believe we've got to do something to help the FBI, to help the Justice Department, because we cannot sit back and do nothing. None of us would want to do that. But we can be wise in what we do, if we're careful in what we do, can't we, Jeff? Isn't that your basic message here today?

Ms. MARTIN. Definitely.

Vice Chairman SHELBY. Thank you, Mr. Chairman.

Chairman GRAHAM. To follow on with what Senator Shelby was just saying, it seems to me prior to September 11 we had been aware of the fact that many of our previous laws had been developed with a certain expectation of what the technology was going to be. It was that telephone that sat on your desk or your night table, and that was how you communicated. Now, if we could step back and say what was the philosophical context, rationale, and constitutionally acceptable basis for allowing that telephone sitting on your desk to be wiretapped, then ask the question, now, in the new technology, where the same act, communication from human being to human being, is being carried out but the technology is substantially different, how do we adapt the laws to be consistent with the philosophy that allowed the static telephone to be wiretapped to now allow the computer or the cellular phone or the other forms of communication to be similarly accessed under the same circumstances that we tolerated before.

Mr. BERMAN. As I work a lot on the internet I've been talking to a lot of staffs about on a pen register all you're saying is, "Well, all we want from the internet is the same information from a computer that we get from a telephone, the pen register," which is the dialed digits. There is no equivalent on the internet. The transactional information that follows an e-mail has a name, it has a subject line, often with the subject line having the whole content of the message in it, which is, "Hey, Joe, join the meeting," and several messages like that tell you as much as what's in the content of the message.

I'm not saying that you don't provide pen register authority for advanced technologies and give the computers a pass, but you have to look at what's the equivalent. You've got a very low standard because you think you're only getting telephone numbers. If you're getting the content of the communications in many cases, shouldn't we be more circumspect and have a higher review. So that's the kind of technology issue we're prepared to address, but we need some dialog.

Chairman GRAHAM. I'm going to recognize Senator Shelby, but maybe I'm expressing a personal frustration. I thank you for your comments about having this open hearing and I look forward to having more as we focus on these issues. On the other hand, sometimes the factual predicate for needing these changes is stated to be classified. So we then have to go behind closed doors to hear what it is that is making it necessary to propose these changes.

Then we come back in a public hearing and we can't be as candid as we are being today in terms of a discourse between different points of view.

Mr. BERMAN. Just back on the process of FISA, this dialog between public and private, there was all classified information that we were dealing with in trying to craft the warrant requirement for FISA. It was done with dialog between the Justice Department and industry and civil liberties. All they did was they would present us, instead of classified documents, hypotheticals that were not related to and would not blow a source and method, and we would try and wrestle with what they thought were problems and see whether we could fit them into statutes. And you can do that. You have to do that because not everyone's going to be under a clearance.

But there is a lot that can be discussed in an open session or not in a classified room, where people can be brought together to explore these issues and work toward solutions.

Ms. MARTIN. I just want to second that. I think that this Committee has over the years many examples of crafting very complicated law in a public manner, with lots of public hearings, and that it's important to do so for another reason that hasn't really been talked about at great length, which is the public confidence in the process.

I think that while on the one hand the American public is very eager for you to do what's necessary to protect it, I think that we have to not forget that the suspicion of the secret intelligence agencies is just below the surface and that, as Jerry mentioned, it is important that that not become a cancer, especially in our minority communities in the United States and that if you're talking about expanding intelligence authorities that that be done in a way that people come to understand why it's necessary and what built-in protections are in there against abuses. That is very important.

That's the role I think this Committee has played over the years with us in having these dialogs.

Mr. BERMAN. I also point out that there are many authorities in the Justice Department bill where the authority is being delegated down, to a magistrate in any town. They are making decisions about nationwide searches involving terrorist activity. That is a prescription for real mischief because it ought to go to people who have some understanding. That's the same argument the Intelligence Community would make if we said why don't we just let any District Court judge approve these FISA taps. There's a special court sitting there.

Maybe it ought to have more appointees than just made by the Chief Justice of the United States, but there is expertise that ought to be involved and you've got to worry about how that process is played out. I don't think the bill that's on a fast track has been drafted carefully.

Vice Chairman SHELBY. Mr. Chairman, just a few observations. I think we all believe—I hope we do—that the security of our people, our Nation is very, very important. That's one of our highest priorities. We also believe strongly in the Bill of Rights, as well as in our constitutional rights apart from the Bill of Rights.

Now, I think one of the problems is going to be to make sure that we move but that we move wisely and that whatever we craft and whatever we pass and the President signs into law, one, will give the tools to the Justice Department to do its job. I think that's paramount. Also, we should be careful in our language because if

we pass something that's constitutionally questionable or suspect, it will be challenged. If we use all of this and develop great cases and prosecute the terrorists, if we find them—and I hope we will—and then ultimately the courts throw out some of this because of some laws that we haven't thought out, we're back to square one, if not in a hole, aren't we?

Mr. BERMAN. Yes.

Vice Chairman SHELBY. Jeff, you've been the General Counsel.

Mr. SMITH. You are absolutely right, Senator. You're very wise to do this.

I want to pick up on something that Jerry said that fits right here. We need to be very careful about this. Drafting FISA, I was involved on the Government side at the time. It was, I think, a very good exercise where we all sat down at the staff level in what seemed endless meetings to hammer this out. Jerry mentioned the role of industry. Let me encourage you and others to bring in industry, particularly the high tech industry whose equipment and technology is involved here. They were very much involved in 1978 when we were working on FISA, and I think they can bring a lot to the table because they understand precisely in ways that I certainly don't as to how the technology works, No. 1, and No. 2, perhaps equally important, they can tell you where it's headed.

Because a year from now we may be facing new technology and new challenges that we cannot now anticipate, and this is an opportunity to legislate and get it right. The old carpenter's adage of measure twice and cut once seems to be appropriate here.

Vice Chairman SHELBY. Thank you.

Mr. BERMAN. We did receive a letter from Senator Leahy to CDT's Digital Privacy and Security Working Group, in which Jeff has participated many times. It has civil liberties organizations, but it has a very broad cross-section of communications industry—telephone companies, Microsoft, AOL—working and asked to give advice on the communications infrastructure impacts of these proposals. I think that's worth having. We'd be glad to provide it to this Committee also.

Vice Chairman SHELBY. Well, let's win this war against terrorism.

Mr. BERMAN. Absolutely.

Vice Chairman SHELBY. Protect our liberties too.

Chairman GRAHAM. If I could close with a reference to American history, I have almost finished the biography of John Adams, and clearly the low point in John Adams' personal and political life was his signing the alien and sedition laws, which were a response early in our Nation's history to what was perceived to be a serious security attack.

Those laws proved to be not only unacceptable legally but they turned out to be unacceptable politically, as John Adams became the first incumbent President in our Nation's history to be defeated, in large part because of his role in the alien and sedition laws. Then they were subsequently repealed by his successor, Thomas Jefferson.

So the American people also have a history of concern about precipitous actions and there is a potential political price to be paid as well as the other concerns that you've discussed. So I would

hope that we would be cognizant of all of those warning signals. Yes, we want to give to our security agencies the powers that they need to protect our citizens. We also want to do it in a way that does not cause the United States to become like those very people that we are trying to protect our citizens against. It would be the ultimate victory of the terrorists if they were to force us to become like them by our surrendering of our individual freedoms and liberties, which so distinguish us as Americans.

So, with those thoughts, I want to extend again my thanks and appreciation. Please be receptive if and, I expect, as we call upon you over the next few days and weeks for your further counsel on these issues.

Mr. BERMAN. We applaud you for holding this hearing.

Chairman GRAHAM. Thank you.

[Whereupon, at 6:17 p.m., the Committee adjourned.]