S. HRG. 103–1073

COUNTERINTELLIGENCE

HEARING

BEFORE THE

SELECT COMMITTEE ON INTELLIGENCE

OF THE

UNITED STATES SENATE

ONE HUNDRED THIRD CONGRESS

SECOND SESSION

ON

COUNTERINTELLIGENCE

TUESDAY, MAY 3, 1994

Printed for the use of the Select Committee on Intelligence

U.S. GOVERNMENT PRINTING OFFICE

20–678 CC WASHINGTON : 1995

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0-16-052172-6

SENATE SELECT COMMITTEE ON INTELLIGENCE

DENNIS DECONCINI, Arizona, *Chairman*
JOHN W. WARNER, Virginia, *Vice Chairman*

HOWARD M. METZENBAUM, Ohio
JOHN GLENN, Ohio
J. ROBERT KERREY, Nebraska
RICHARD H. BRYAN, Nevada
BOB GRAHAM, Florida
JOHN F. KERRY, Massachusetts
MAX BAUCUS, Montana
J. BENNETT JOHNSTON, Louisiana

ALFONSE M. D'AMATO, New York
JOHN C. DANFORTH, Missouri
SLADE GORTON, Washington
JOHN H. CHAFEE, Rhode Island
TED STEVENS, Alaska
RICHARD G. LUGAR, Indiana
MALCOLM WALLOP, Wyoming

GEORGE J. MITCHELL, Maine, *Ex Officio*
BOB DOLE, Kansas, *Ex Officio*

NORMAN K. BRADLEY, JR., *Staff Director*
JUDITH A. ANSLEY, *Minority Staff Director*
L. BRITT SNIDER, *General Counsel*
KATHLEEN P. MCGHEE, *Chief Clerk*

CONTENTS

COUNTERINTELLIGENCE

TUESDAY, MAY 3, 1994

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

The Select Committee met, pursuant to notice, at 10:06 a.m., in room SH–216, Hart Senate Office Building, the Honorable Dennis DeConcini (Chairman of the Committee) presiding.

Present: Senators DeConcini, Kerrey, Bryan, Graham, Warner, and Gorton.

Also Present: Norman Bradley, Staff Director; Judy Ansley, Minority Staff Director; Britt Snider, Chief Counsel; and Kathleen McGhee, Chief Clerk.

OPENING STATEMENT OF SENATOR DENNIS DECONCINI

Chairman DECONCINI. The Intelligence Committee will come to order.

This Committee, like the rest of the American people, was shocked and dismayed by the arrest last February of CIA employee Aldrich Ames and his wife Rosario on charges of spying, first for the Soviet Union, and then for the Russian Republic, from 1985 until the time of their arrest.

Last week, both pled guilty to crimes growing out of their espionage activities. Ames will spend the rest of his life in prison, his wife, a minimum of 5 years.

While there will be no trial, enough information has been made public to confirm that Ames, who had access to extraordinarily sensitive information, was able to carry out his espionage activities from 1985 until his arrest, without detection. All of this occurred in an agency which we thought had stringent security procedures—perhaps the most stringent in Government.

In the weeks following the arrest, this Committee has attempted to ascertain what went wrong. How could this kind of thing go on so long without detection. Why did it take the most sophisticated law enforcement agencies in the world 3 years to make a case against Ames, an individual described by one news magazine as "extraordinarily inept."

Our inquiry is far from complete. Indeed, it cannot be completed until the debriefing of Ames is complete. But it seems to me, based upon the inquiry to date, that several things are clear.

First, our security policy practices and attitudes have become so lax that people believe that they can beat the system, and they can.

Second, the system lacks sufficient checks to tip us off to security problems. The Government requires relatively little information

from employees who hold sensitive positions. At the same time, there is over reliance on the polygraph, which, as Mr. Ames related to the Washington Post, can be defeated with a simple mixture of confidence and friendliness toward the examiner.

Third, our investigative agencies are still limited in the sorts of information they can obtain about Federal employees, even where the employee has access to information whose loss could be devastating.

And finally, I regret to say, our investigative agencies seem to be more concerned with protecting their own bureaucratic turf than getting down to the business of catching spies.

The Nation cannot afford to let this situation continue. We don't need another quick fix. We have already had more than 10 of these, and all appear to have failed, the 1988 Memorandum of Understanding between the CIA and the FBI being the latest example. The cold war may be over, but as the Ames Case demonstrates, other countries will continue to conduct espionage against us when they see it is in their interest to do so.

We must have in place a legal and administrative framework which gives us the best chance to deter spying, which gives us the best chance to detect it, which gives us the best tool to investigate it, which gives us the best chance of prosecuting it successfully. We do not have that system in place today, in my judgment.

The purpose of today's hearings is to consider what changes are needed. Since the arrest of Mr. Ames, four bills have been introduced and referred to this Committee, to deal with the shortcomings of the current system: S. 1866, introduced by Senator Metzenbaum, a member of this Committee; S. 1869, introduced by Senator Cohen and Senator Boren, stemming from their work for many years as Chairman and Vice Chairman of this Committee, and we are pleased to have Senator Cohen here today to testify on what he thinks is necessary; S. 1891, introduced by Senator Heflin; and S. 1948, introduced by Senator Warner and myself.

This morning the administration will present to us its own legislative proposal, which contains elements of the bills already introduced. Although I have only been able to review the bill very quickly, it appears to me that there is something here very constructive that we can work with.

Our administration witnesses will also present their non-legislative fix on how to improve coordination and cooperation between the CIA and the FBI. I commend the administration for the progress it has made on these two matters.

It is my intent to have the Committee markup a counterintelligence legislation bill later this month if at all possible. And I know, because of time restraints of Senator Cohen, I am going to yield to Senator Warner for an opening statement. Before I yield to other Members, I am going to let Senator Cohen and Senator Boren give their statements. Then we will come back to Members.

Thank you, Senator Cohen and Senator Boren, but Senator Warner first.

OPENING STATEMENT OF SENATOR JOHN W. WARNER

Vice Chairman WARNER. Thank you, Mr. Chairman.

We welcome our colleagues and we wish to commend them for what they have done as predecessors to the Chairman and myself. And I am going to, in my remarks here this morning, pose a question to both of you. And that is, as we look at the controversy today between the Central Intelligence Agency and the FBI—and that is the focal point of what we have got to determine here legislatively—I do not find a record that the Jacobs Panel, which was under your auspices, really focused on that, nor did either of you two gentlemen in your work. And I am wondering, at least I don't see the emphasis, Senator Boren—you look quizzical at the moment—that we are placing today on this issue. I don't see that emphasis with your early work with the Jacobs Panel and your other work.

So as we look at the administration bill, I don't know, I put it in last night on behalf of the two of us, Mr. Chairman.

Chairman DECONCINI. Yes, I know.

Vice Chairman WARNER. I find the administration bill somewhat vague, and I have to tell you in all fairness, it falls short of the goals that I would hope to see the Congress achieve in this new piece of legislation. But we'll reserve judgment until such time as we have looked at it very carefully.

Mr. Chairman, you opened up with the comments, "shock and dismay." Indeed, I join you. But I think we have got to be very cautious in this state of shock and dismay that we do not swing the pendulum too far. We're looking at a balance between individual rights and the national security interests of this country. Just how far we will move remains to be seen. I think we have got to move that balance somewhat further toward our security interests and that would require a greater concession on the part of the employees of our many agencies and departments involved in national security work. So I hope we don't over react, but hit that proper balance, Mr. Chairman, and I welcome our witnesses this morning.

Chairman DECONCINI. Thank you, Senator Warner, and thank you for your cooperation and your real hands-on involvement with constructing what I hope will be a constructive change with whatever we do here.

It is a pleasure to begin our hearings with Senator David Boren and former Vice Chairman of this Committee, Senator Cohen. Senator Boren served for 6 years as Chairman of this Committee. Many things changed, including the nature of how this Committee handled different problems, the nature of security within the Committee.

And I notice we all saw the announcement that Senator Boren will resign at the end of this session to become president of the University of Oklahoma. You will be missed, David, I can assure you. Not only is your legacy still here on this Committee, but in many, many other areas.

Senator Cohen, we welcome you here, and your outstanding performance as Vice Chairman, working with Senator Boren and making the changes that this Committee, I think, is trying to live up to.

And we will hear from whoever cares to go first.

Senator BOREN. Mr. Chairman, I think Senator Cohen has to Chair another committee or is due to Chair one right now. So if I

could defer to him, and then I will make my opening comments immediately following his.

Vice Chairman WARNER. He has to look after my interests on the committee until I get there.

Senator BOREN. I think that's correct.

Chairman DECONCINI. Senator Cohen.

STATEMENT OF SENATOR WILLIAM S. COHEN

Senator COHEN. Well, thank you very much.

First of all, let me thank President Boren. I notice there has been a decided improvement in his arrival time since his appointment. He is at least 10 minutes earlier than he would have been when he Chaired the Committee. So we have seen some marked improvement since your decision to accept a new assignment.

[General laughter.]

Senator COHEN. But you are right, Mr. Chairman. This Committee, this Congress, the Senate, is going to miss David Boren for his outstanding contribution to the U.S. Senate, to the country. And I will have more to say about that at a later time.

But I would like to thank the Committee for inviting us to testify about ways in which we can improve the Nation's counterintelligence efforts.

When Boris Yeltsin gave his memorable speech to a joint session back in 1991, he bluntly declared, "no more lies." And perhaps because of the thunderous applause he received at the time, many Americans seemed to have misheard him to say, "no more spies." We now know better.

The point is, we should have known all along. Both the Chair and the Vice Chair have indicated they are shocked about the most recent case. I was not shocked at all. If anyone got the impression that the end of the cold war meant there would be no one left to come in from the cold, they didn't get that impression from Moscow. Because after the collapse of the Berlin Wall, the Warsaw Pact, the Soviet Union and later the Russian intelligence officials clearly stated they were going to be very much in the business of aggressively searching out and stealing business secrets, at the very least.

The CIA and the FBI and others warned that the end of the cold war would produce no decline in espionage against the United States, and indeed, it might even lead to an increase, and some Americans might be more comfortable selling secrets to countries that no longer appeared to threaten us.

During the 1980's, more spies were unmasked than during any other time in our history. They were clerks, analysts, military personnel, other low- to mid-level employees with access to our most important secrets, and a willingness to sell those secrets to the highest bidder. I point out, only one-tenth of them were recruited. Nine out of ten were volunteers, initiating contact with a foreign intelligence service.

Senator Boren and I, who were serving as the Chair and Vice Chair of the Committee, were familiar with these issues. We participated in the Committee's counterintelligence review following the arrest of the Walker spy ring, which resulted in our Committee's 1986 report, entitled, "Meeting the Espionage Challenge."

And we were determined to see that, in fact, we didn't just study the issue. We wanted to act upon it. So we convened a panel of wise men, so-called, who had significant experience in both Government, law, and industry, to try and identify ways in which we could improve the counterintelligence system without sacrificing the personal liberties that Senator Warner has referred to that our national security apparatus is meant to protect.

And this panel was led by Eli Jacobs and included such individuals as Warren Christopher, Lloyd Cutler, A.B. Culvahouse, Sol Linowitz, Admiral Inman, and others, and they worked closely with the both of us as well as with the entire intelligence community for a year, reviewing all of the espionage cases that had occurred in the history of our country, to try to, as the Chairman has pointed out, better deter, detect, and prosecute cases in the future.

And I think it is important to note, this was not just a response to a single case such as we have with the Ames case now. It involved a systematic review of a large number of cases that occurred over a period of decades.

It was based upon that panel's work and our Committee's work that we introduced legislation that was designed to accomplish what the Chair has indicated: To deter, to detect, and then to prosecute those who were not deterred.

Given the pecuniary motives of today's spies, we sought to improve the chance that warning lights would start flashing when Americans started handling highly-classified information and started to live beyond their means, as was noted in a 1990 statement that I think is particularly pertinent in light of the Ames case: If a guy goes from a Vega to a Jaguar in a year's time, something is wrong and should be detected.

Now there is a doctrine, of course, a legal doctrine, called *res ipsa loquitor*—the thing speaks for itself. And Thoreau was asked to give a definition of that. He said that is when you find a trout in your milk. I would say the same thing is probably true here, when you find a Jaguar in the garage on a Vega salary.

We concluded that the FBI should be given access to financial and foreign travel records of people who were cleared to have top secret information, and for 5 years following access to that information. And this, we felt, constituted a moderate loss of privacy for those who would handle highly-classified information, but we felt it would create an important deterrent to those who attempted to spy, and it would be a new tool to catch those who did so.

A second significant change we proposed was to establish uniform requirements for access to highly-classified information, which can vary widely from one agency to another. According to a recent report by a panel appointed by the CIA and the Pentagon, information on a certain technology was subject to, "discretionary controls by the Department of Energy, but protected by deadly force by one of the military services." I think we can find similar disparities in terms of how different agencies handle highly-classified information.

This not only creates wasteful duplication, but it also allows what we call in legal terms, "forum shopping." You have a situation in which people can shop around for the weakest standards to meet. Jonathan Pollard, for example, the famous case, a gentleman

who pleaded guilty back in 1986 for spying on behalf of Israel, was denied employment by the CIA in 1977 because of security concerns, only to be hired 2 years later as a civilian naval intelligence analyst.

Other measures that we identified included improving protection of cryptographic information, which can be the magic key to read volumes of sensitive communications; closing gaps in our espionage laws; better enabling the Government to confiscate ill-gotten gains on the part of spies; establishing jurisdiction in U.S. courts for espionage acts committed abroad; and allowing monetary rewards for information leading to the arrest or conviction of spies or the prevention of espionage.

I think it is quite possible, had this legislation been approved when we first introduced it in 1990, Aldrich Ames would have been caught much sooner. It is equally important that unknown persons who might now be spying or considering doing so could be caught and deterred before causing great damage.

Unfortunately, what happened was the perception that the cold war had thawed, the resulting flood of good will rendered our legislation to be seen as, or misperceived, I should say, as the remnants of anachronistic cold war agenda, and it simply languished in the 101st and 102d Congresses.

Now, at that time we asked whether it would take another security disaster such as that involving Felix Bloch before Congress would be spurred to take action. I think the Ames case has pointed out the answer is yes. And now that Mr. Ames has reminded us that spying is going to continue as long as dollars are offered to those who are fallible human beings, we have an obligation to act quickly and to reform our counterintelligence system.

Now I will just take a couple of minutes, Mr. Chairman, and just present a synopsis of the key points and the key differences between your legislation and that which Senator Boren and I introduced.

Your bill would cover only employees of the intelligence agencies, in contrast to the broader sweep of our legislation. We would cover all people who have top secret clearances. And I think while the desire to narrow the scope of coverage is understandable, I would simply point out that many, perhaps even most, of the espionage cases involve people who are not intelligence employees.

You pick up the financial disclosure provisions from our bill and you expand them to include the Federal income tax returns, which I think is a positive improvement.

And you also use a different forfeiture mechanism to enable the Government to seize the spy's ill-gotten gains. I really haven't decided whether one mechanism is better than the other, but we have to have some mechanism in any event.

You drop the provision requiring Foreign Intelligence Surveillance Act, the FISA procedures for physical searches, due to the concerns about the prosecution of the Ames case. Now that the Ames case has been concluded, I would hope that you would consider putting that back in.

You also drop our provision on improving protection of cryptographic information due to the concerns about the validity of polygraphs as a result of the Ames case. In my view, the Ames case

merely affirms what we already knew. Polygraphs are not infallible. They are far from perfect. They shouldn't be over-relied upon. But employed with care as one of many tools, I think they still can be useful.

And finally, section 807 of your bill makes a major change that we are going to—I assume you are going to take a great deal of time to discuss this morning—and that is the responsibilities among the respective agencies.

As you have noted, the President, thanks to the two of you, introduced legislation—but the President last evening or this morning I am told, signed a Presidential Directive which tries to deal with this particular issue. I am not qualified at this point to know whether it goes far enough or whether it needs flexibility that's not granted in your proposal, but clearly something has to be done to break down the walls that for many, many years have separated the FBI and the CIA. Without pointing the finger of accusation at either agency—both can be found at fault over the years in different cases.

I make one final comment. Mr. Ames last week stated that he felt that too many people were employed in our intelligence service and were engaged in activity which certainly was highly questionable from an ethical point of view. I think the Intelligence Community is caught in a cross ruff. Whenever there is a failure, if there is a case of not enough national technical means—in the case where we had Libya, I recall when we were serving on the Committee, they said why didn't the Intelligence Community know that the Libyans were building one of the most massive chemical weapons plants in the world. Well, we didn't have enough overhead coverage at the time. We were quite preoccupied with the Soviet Union. We simply didn't have the assets.

Then the question was raised, well, why didn't we know that Saddam Hussein was going to invade Kuwait. And the answer was, we don't have enough human intelligence. Now along comes Mr. Ames and he says we've got too many people involved in a profession or endeavor which calls into question their ethical standards. It may be. And that is something that the Committee should always be willing to look at.

But I must say that the honorable thing for Mr. Ames would have been to have quit the service and gone public. Instead, he chose to remain in the public service and betrayed his country. So I would not give much weight, if any, to his comments.

That's all I have at this time.

And Senator Warner, you asked me whether or not we addressed the issue of the relationship between the FBI and the CIA—we did not spend a good deal of time on that, and I think as a result of your efforts, your legislative efforts, you now see the administration moving, on an administrative basis at least, to try and deal with that issue. So I think without that it would not have happened.

Vice Chairman WARNER. Senator Cohen, I don't know whether you had a chance to read this very good article in the Post this morning.

Senator COHEN. I have not.

Vice Chairman WARNER. But it traces the history of this CIA–FBI controversy. And it observes, 16 years later, this is after Bill

Webster and Stan Turner tried to get it worked out, 16 years later, high ranking national security officials are still trying to figure out ways to promote cooperation between the two organizations.

Have you got any opinion now as to whether or not this should be done legislatively or left to this administration and its successors to do it simply by Executive order and administratively?

Senator COHEN. Well, my own view at this time would be to see whether or not the Executive proposal goes far enough. If you feel that it is too weak and it won't really deal with the problem, then you can always go forward legislatively. You've got new personnel. I think a new spirit of cooperation. Ordinarily when you pass something legislatively it is very restrictive and inflexible and perhaps one should defer at least temporarily to the administration to see whether or not——

Vice Chairman WARNER. But then it comes back to your relying on personalities currently in office, and it hasn't worked for all of these years.

Senator COHEN. That is true and that's something you have to take into account. But I would also point out that this is something that's endemic to human institutions. We go through the same process with the Appropriations Committee and the authorization committee. How many times have we gone to the Floor and watched some of our senior Members virtually engaged in fist fights over who has the authority and responsibility to authorize certain programs or to appropriate them. So it's not something that is unique to the CIA and the FBI.

I think in this particular case, if the administration lays down a proposal which is very far reaching, is not as flexible as perhaps they would like, but nonetheless gives some flexibility to working their problems out, having a system of rotation on the part of the FBI, of the CIA, and DOD, and also having a new Counterintelligence Center with the FBI situated at the head of that, that may be sufficient. But I think it would not have happened frankly, without your initiative.

So you'll have to decide, or we'll have to decide, whether or not the legislation has to be broadened to give the administration more flexibility, or whether you should defer legislatively and let it be implemented administratively. My own view is you probably have a combination of it to broaden the legislation, allow the administration sufficient flexibility, but have some strict guidelines there as well.

Chairman DECONCINI. Senator——

Vice Chairman WARNER. If I could just follow-up.

You and I have sat side by side on the Armed Services Committee for 16 years and we just passed the Goldwater-Nichols legislation which established within the military those principles, who is in charge, who is accountable when a mistake occurs. And now you have basically two co-equal agencies, the FBI and the CIA. And as long as you have this duality of who's in charge and dual accountability, you know from our experience in the military, problems happen.

Senator COHEN. And I might point out when the Goldwater-Nichols bill was being debated, it was heavily opposed by the administration and years later they have thanked us for going forward.

Vice Chairman WARNER. That is correct.

Chairman DECONCINI. Well, Senator Warner, thank you for asking those questions, because they deal exactly in what I am interested in focusing on and that is what Senator Cohen—and I am going to ask Senator Boren the same thing—if we decide, and I do compliment the administration for addressing this head on from the National Security Council on down and getting the directors of the two agencies and the Justice Department really to focus on it, because they have devoted some time and some thought and been realistic realizing, expressing the problem, and coming up with a solution.

What troubles me is there's no enforcement. There's no ultimate, says this is the way it is going to be if these two personalities, these two directors, or these two individuals, whoever they may be, current or to come, don't function in the way.

Now, I realize human beings can subvert legislation as well, but it seems to me that when you're sworn to uphold the law, you are more apt to do it than if it is just an Executive order and you disagree with someone. Do you have a comment? On the enforcement side?

Senator COHEN. Well, I haven't really studied the Executive order——

Chairman DECONCINI. Perhaps you would do that for us and give us whatever analysis you'd have. I'd welcome that.

Senator COHEN. I'd like an opportunity to look at it. I'd be happy.

But I think you do have to have some enforcement mechanism and ultimately the President of the United States is the one who's got to resolve these differences and I am sure that he would set up some kind of an administrative mechanism to make sure that the differences are resolved.

But I think what we have to finally conclude is whether it is better to have legislative guidelines with flexibility, or a legislative deference and let the administration see whether it can go forward on its own.

I think Senator Warner has pointed out that we had strong opposition to legislate the Goldwater-Nichols Act. I was very much involved in that for several years. And as I recall, General Powell even initially was fundamentally opposed to it and years later sat at this table in front of the Armed Services Committee and said, "I am glad we have Goldwater-Nichols."

So it may be necessary to have some kind of mechanism to resolve that. But I think we also have to be careful that you don't make it so restrictive that you foster more friction than remove it. You've got strong institutional histories behind these two agencies basically, and different jurisdictions and different mind sets. And it may take some changing over a period of time to resolve that. But I think if you were to mandate, for example, that the FBI were to take over the counterintelligence investigations whenever there was the slightest hint of a spy case as such, it is going to cause serious problems with the CIA itself.

So I think there are ways to resolve it. I think your legislation at least has prompted us—all of us—to look at it very intensely and really to put an end to the kind of either bickering, not sharing of information. And I say, it cuts both ways, it's not only a case of

the CIA not sharing with the FBI. We have had cases in which there—in the Ames case we had at least one contact that the FBI was aware of that didn't share with the CIA. So it goes both ways. And what we have to do is to resolve these kinds of differences.

As I said, we see it ourselves every day on the Senate Floor when there is a debate over who has the power, the authority, to authorize programs or to appropriate for them. And it is something we have failed to resolve over the years. So, I think you've done a real service, Mr. Chairman and Mr. Vice Chairman, in prompting us to review it.

Chairman DECONCINI. Thank you Senator Cohen, we appreciate your testimony.

Senator Boren.

STATEMENT OF SENATOR DAVID BOREN

Senator BOREN. Thank you very much, Mr. Chairman, and thank you for your kind words. And also, I want to thank my colleague, Senator Cohen, for his.

Thank you for giving me this chance to discuss with you the importance of changing our laws and attitudes toward the ongoing threat of espionage and counterintelligence. I want to commend and join Senator Cohen in commending both you and the Vice Chairman and the members of the Committee for giving this problem the attention it deserves and for, I believe, advancing some very worthwhile proposals to deal with it.

The recent Ames case makes clear the need for reform. And let me say that, for a long time, I think we have had these ongoing concerns about whether or not we have dealt adequately with the espionage problem. One of the most haunting and interesting experiences I had a few weeks after becoming Chairman of this Committee was to have received a call from a very controversial figure in the history of American intelligence, the late Mr. Angleton, who told me he had checked me out thoroughly and felt that I was a reliable person and that he was near death and had something he had to tell me before he died.

He made two appointments to come see me in my office, he was suffering from emphysema, he was not able to leave his oxygen supply—and had to cancel them—and the third time he asked if I couldn't come to his house because he so desperately wanted to give me this information and he thought he didn't have much longer. And I agreed to go to his house and I got in my car in the Senate parking garage that morning to leave to go out—I was stopped by a policeman at the door who said he just received a call that Mr. Angleton had died. So I never received that last message.

And I always wonder when one of these cases comes up, the mystery that always remains unsolved, was Angleton right at least to some degree or was he completely off on an extreme tangent.

But as you know, Senator Cohen and I introduced a bill that would have addressed some of the deficiencies in the legal and security systems 4 years ago. We reintroduced this bill earlier this year. S. 1869 would strengthen the tools available to the Federal Government to deter, catch, and prosecute those guilty of spying against our country. The bill grows out of work, as Senator Cohen has indicated, performed by this Committee when I served as

Chairman and he served as Vice Chairman in 1990. Several members of the Committee, including the current Chairman and Vice Chairman, participated in that work.

The Boren-Cohen bill is the product of work performed by a distinguished panel of outside experts, as Senator Cohen has said. We did hold public hearings on their proposal in this Committee. And the independent bipartisan panel which issued the report was chaired by Eli Jacobs, a New York businessman who served on a number of national security advisory boards. And as you know, the panel involved members who are now high-ranking officials in the Clinton administration, including White House Counsel Lloyd Cutler, Secretary of State Warren Christopher, and CIA Director James Woolsey. Others participating in the Jacobs Group were Admiral Bobby Inman, former Director of NSA, former Deputy Director of CIA; former White House Counsel in the Reagan administration, A.B. Culvahouse; Sol Linowitz, our former Ambassador of the Organization of American States; Richard Helms, former Director of the CIA; and Seymour Weiss, former Ambassador and State Department official; and Columbia law professor, Harold Edgar, who is a noted scholar on national security law.

We attempted to have a very balanced group—one that would be sensitive to national security concerns, but also one that would be very sensitive to the constitutional safeguards that individual citizens should have under our system of government.

The panel determined—and as Senator Cohen said, it was a comprehensive review, not of just one or two cases, but all of the major espionage cases in recent decades—that most modern spies sell secrets for financial rather than philosophical motives. And for that reason, they are not likely to be discouraged by the political changes that have swept through the Eastern Block.

Indeed, the large part of the espionage problem is impervious to the political change in the former Soviet Union and in Eastern Europe and it is the phenomenon of a U.S. citizen who, with access to highly-classified information, who volunteers his service to a foreign intelligence service for money, that we are dealing with. No foreign government obviously is going to refuse an opportunity to acquire information in its own national interest, even some of those countries with which we have had close alliances in the past, during the cold war period.

The changes proposed by the panel in the legislation were presented in a rare open intelligence hearing on May 23, 1990 and a second open session was held a month later. The changes proposed in the legislation have many common features, as Senator Cohen has indicated as he walked through the differences in the two bills, Mr. Chairman, with the bill which you and Senator Warner have introduced and which I have cosponsored with you.

The provisions fall into three main categories: Improving the Government's personnel security system; providing additional penalties for espionage activities; and enhancing counterintelligence investigative capability. The Boren-Cohen bill would establish uniform requirements binding on all branches of Government for access to top secret information, and would require that all persons considered for such access make personal financial reports during that period and for 5 years after their employment had terminated.

Because, after all, there could be agreements to reap the financial benefits once someone has left Government service, not while they're still in service. And so it may not show up in terms of a change of lifestyle while they're still employed.

It would make some Government employees subject to random polygraph testing, and it would establish a new criminal offense for possession of espionage devices where intent to spy can be proved. And I think that is something you may want to look at very carefully, the possession of these devices, because it would allow for de-encrypting and for de-codifying certain documents, and the possession of that equipment in itself, I think, should be an element of evidence which is available to be used in these cases.

Further, it would establish criminal offenses for selling and transferring top secret materials or removing them without authorization. It would tighten laws barring profit for espionage, and expand existing authority to deny retirement pay to those convicted of espionage in foreign courts. And here I would say, if I were the Committee, I think I would take some of the provisions of our bills and some of the provisions of yours in regard to depriving anyone who spies of any financial gain, perhaps putting all of them into the legislation.

The bill would permit the FBI to obtain consumer reports on persons thought to be agents of foreign powers without notification of that person. The FBI would be allowed to obtain subscriber information from telephone companies on persons with unlisted numbers who are called by foreign powers or their agents.

It would authorize the Attorney General to pay rewards of up to $1 million for information leading to the arrest or conviction for espionage or the prevention of espionage.

And finally, the legislation would subject physical searches in the United States to the same court order procedure that is required for electronic surveillance.

And I think again, from a constitutional point of view, that's a provision that deserves study and sensitivity on the part of the Committee. Because after all, we don't want to sacrifice basic constitutional principles here, even as we become more aggressive in the effort to stop espionage.

Many of the ideas expressed in the Boren-Cohen bill, as I have said, are now part of the DeConcini-Warner initiative, and I note many similarities between the bills, and as I have said, I am proud to be an original cosponsor, Mr. Chairman, of your bill.

I want to just make one or two observations regarding the differences and this will take me right to the points about which you have asked questions.

In the Boren-Cohen version, all Government employees with top secret access are subject to increased scrutiny. The DeConcini-Warner bill focuses on all the employees of the intelligence agencies and units. It also identifies a special class of employees—those with critical intelligence information who must provide additional financial information.

And while I understand that the scope of the law needs to be comprehensive enough to deter employees at all levels from disclosing national security secrets, I also believe that we must carefully

decide which employees hold sensitive enough positions to be subject to the close monitoring of their financial dealings.

It's obvious we do not have the resources to scrutinize all employees. Monitoring too many employees could mean that we do not carefully enough monitor those we should be watching. I realize that some estimates of the original Boren-Cohen bill placed the number of employees with top secret clearances at over 500,000 Federal and contract employees. And clearly because of that estimate, which has come about since we introduced the bill, I believe that we need to revisit that criteria to reduce the number of investigations. However, I believe that investigating all employees at intelligence agencies as proposed by the Chairman's bill would also lead to an exorbitant number of investigations.

So I would say that I believe in both of our bills. We have the problem of covering too many people. I believe that we would be better off to try to identify those that are in truly sensitive positions, both in the intelligence community and in the rest of Government—those in truly sensitive positions—and narrow the size of our universe to a manageable number of people that we can really monitor with some effectiveness.

So I think that both bills need some modification here and I think that the Committee needs to do some work on it. I think we all realize that if we say we are going to monitor 500,000 people, that really means we aren't going to monitor anyone very well. I don't know what that magic number is, whether it is 25,000 or 50,000 or 10,000, that we can really monitor with some larger degree of assurance, but I think that is an issue that needs to be carefully addressed by the Committee—the size of the universe to be monitored.

In addition, I believe that section 807 in the DeConcini-Warner bill should be revisited and as has been said, section 807 would require earlier coordination between the FBI and the Intelligence Community on counterintelligence matters than is currently required, expanding the FBI's role at earlier stages in the investigation.

I certainly agree with the provision's intent of improving the investigative process that took 7 years to identify Rick Ames. I think however, and I have said here that rather than a legislative mechanism, that Congress should encourage the interagency process that is taking place. And of course, since I wrote these words a couple of days ago, the President now has issued this Executive order.

Now let me say, I join with what Senator Cohen has said. I think that the fact, Mr. Chairman, Mr. Vice Chairman, members of the Committee, that this bill has been introduced and that it included section 807 has been a very healthy thing. I think you have sent up a red flag that needed to be flown.

Vice Chairman WARNER. Yes, but the administration didn't pick up the flag in their bill. They are silent on this.

Senator BOREN. Well, not on the bill, but apparently they are moving on it in the Executive order, and we'll need to study it. I know, I have expressed my concerns to Director Woolsey and I do believe that he is moving. I think the fact that the interagency group—and again I compliment both the Committee for raising this issue strongly and I think he has reacted with the interagency

group that has been set up as we have now seen in the resulting Executive order of the President to bring closer coordination.

I would also tell you that I have a high regard for the current Deputy Director of Operations, Mr. Price. I had an opportunity to work with him during my time on this Committee. And I think he is a person who will not approach this matter with defensiveness, but when engaged by the Committee fully, I think would be willing to give very good and constructive advice.

I have been thinking here about the Executive order. As you know, in the past—and remember when we passed some of our intelligence reform proposals—we decided we didn't want to leave it just to Executive orders. And you will recall the reforms we adopted in this Committee after the Iran-Contra matter when Senator Cohen and I had, in essence, negotiated with President Reagan the issuance of an Executive order that would change the way in which findings are issued so they would have to be in writing, they couldn't be retroactive, they would have to have certain additional information.

We didn't leave it just to an Executive order, because we felt that could change with changing administrations; that we needed the protection of statutory law to make sure that the provisions of Executive orders would survive from one administration to the next and we felt those reforms, in the aftermath of the Iran-Contra affair, were so important that they should be embodied in statutory law.

I would say to the members of the Committee that, Mr. Chairman, that I believe that the reforms that are embodied—and again, you would want to study this Executive order carefully to see if it goes far enough and to see if it is the appropriate mechanism—I think even with the Executive order it may well be appropriate for this Committee to legislate in the whole area of closer cooperation between law enforcement, counterintelligence, and our intelligence gathering agencies, in particular, the CIA and the FBI as the two lead agencies, and to some degree the Department of Defense.

We have done this in a number of ways which still allow some flexibility. You may recall that when we passed the Independent Inspector General bill, we put in a provision that the Committee be notified, within 10 days, whenever there was a situation in which there was a disagreement between the Director of CIA and the Inspector General about how to proceed. We didn't say they had to notify us all of the time. We didn't say we were going to micromanage. But if there was a major disagreement, there should be a notice sent to this Committee so that it could stand back and serve as a watchdog and it could prod the process in the right direction.

It seems to me that what I know of the overall form of the Executive order—and I have to say my knowledge is only sketchy at this point—the idea of establishing a counterintelligence center with representation of the FBI, the CIA, and the DOD is a very good one. And the idea of rotating leadership of that center is a very good one. You might well want to enact that statutorily—the existence of that center—so that it is not left to the whim of the next administration.

I think you might also want to do something like this. Each agency—and this would have to be highly compartmented, only a very small group of maybe the principal representative of each agency only, because these cases are very sensitive—and this point I do want to make and I think it is important, and that is the reason I would urge the Committee to really walk through this in perhaps an informal way in which there could be great candor with people like Director Woolsey and especially with Deputy Director Price and I would also urge you to bring back the former Deputy Director of Operations, Mr. Stolz, who many members of this Committee worked with and have him as an expert witness in an informal way, or perhaps just conversations with him. He was a person of tremendous integrity, you'll remember. He left the Agency over the appointment of Mr. Hugel during the Casey years and then was brought back. He has enormous knowledge in the operations area as well.

One of the reasons why it is very difficult to just have an automatic takeover, let's say, of all counterintelligence matters, espionage cases, by the FBI from the inception, is that some of the sources of information, some of the human sources and some of the information gained is so sensitive that it is very, very highly compartmentalized even within the CIA. Some cases—and I am sure the Chairman and Vice Chairman in particular, and other members of the Committee can think of cases in which we have dealt with situations where maybe on two or three or four or five people in the whole CIA or the National Security Council, including the President, knew about a particular matter, I can think back over my 6 years as Chairman and there were some cases where probably not over 10 people in the entire Government, including leadership of the two Committees, the President of the United States, and three or four other people knew about certain matters. So there is a need sometimes to highly compartmentalize information and sources.

I think, however, you could still protect that and bring the FBI in appropriately on cases if you said that when there was due cause, or sufficient basis for opening a serious investigation, when you reach that threshold level, that whether the FBI discovers that information or the CIA, that it be brought to the Center; that if it is a highly sensitive case that it be discussed only with the principal representatives of the three agencies. In other words, you are really limiting that knowledge initially to three people—the chief representative of the CIA at the center, the chief representative of the FBI, and the chief representative of the DOD.

I would think they would then try to resolve whether or not it is a case in which the resources, let's say of the FBI, should be brought in at that point in a very major way. You could perhaps craft this in a way that the Committee would be informed of situations, or at least the leadership of the Committee would be informed of situations in which there was a split decision of the Center. If you had a unanimous opinion among the CIA, the FBI, and the DOD principal representatives, those 3 people, as to how to handle a counterintelligence case, then I don't think there is any reason for anyone to get involved. Obviously they are working it out on a good basis. But if they weren't, if the Committee were

then informed of a problem, and in a year's time you could see where, was there one split decision, or were there 50 split decisions, you'd see whether or not this mechanism was working.

But in the meantime, you might want to statutorily put it in place. You might want to statutorily provide for the rotation of the chairmanship of that committee between agencies. And you might want a mechanism under which the Committee would be informed about splits and divisions which occurred at that level in the committee.

Senator Warner asked, did the Jacobs Panel focus on this matter. Not specifically. But our Committee—and I know both of you will recall, and others that were on the Committee at the time—we did focus on the problem, not in the Jacobs Panel but in general in our Committee—and the problem of how the law enforcement agency, principally the FBI and the CIA were not always coming together. We looked at it not only in the context of counterintelligence, but in other contexts.

Remember the final report on the BNL case, where we found there was a lack of sensitivity. It's not only sometimes that the intelligence community doesn't tell law enforcement agencies when they stumble over a violation of law, and we found that in the BNL case. And I won't rehash that whole case, but you recall there was a whole question of information we picked up abroad that might result in a violation of criminal law in the United States in that case. Did it ever go where it should have gone to the FBI, to the Justice Department, even to the Federal district judge in that case.

So in that final report in the BNL case—and the Committee might want to look back at it, we saw the mirror image of that—that not only sometimes is law enforcement information of a counterintelligence nature, perhaps not flowing to the intelligence community as it should, perhaps partly because their own fault of not sharing enough information to get the feedback, but also violations of law that the intelligence community stumbles upon, whether it is money laundering, drug dealing, or something else, very often do not get to our law enforcement officials in the proper way, either.

And as Senator Cohen has said, this is a very complex situation, where we have two different cultures at work, two different major goals. The intelligence community's goal is not to prosecute people or put them in prison. Its general goal is to collect information. Law enforcement is to collect information for a purpose, usually prosecution, and to stop the breaking of the law.

But I think you might want to really think about how you might craft a counterintelligence center. From what I have seen of the Executive order of the President, I think it is a step in the right direction. I do think that both Director Woolsey and the Director of FBI should be commended for beginning this process of working together. I do believe that they are making every effort to take constructive steps, but I think this Committee can add to the positive work that has been done already. I think this Committee can make a contribution. And I think it should consider a statutory enactment, but as I say, with some flexibility and with some mechanism that would enable you merely to monitor it to see if it is working right, or to see if the warfare of the differences between the two major agencies involved are continuing.

I might just conclude by saying at the time that Senator Cohen and I first introduced our legislation, the cold war was coming to an end and many people asked why we should continue to worry about espionage. And although ideologically inspired spying has been decreasing, spying for financial gain has been on the rise. And I might say, in fact, as we have all seen it, it is ironic. As the cold war has wound down, the level of espionage, if anything, has gone up. Some of this espionage is to steal economic secrets, business secrets, and technological secrets as opposed to military secrets, and some of that spying is going on not for the old Soviet Union or for its component parts, but for some of those that were our allies.

Those tempted to spy now may not think they are putting their country in jeopardy as much as they would have during the cold war, when they thought maybe stealing a military secret might endanger the lives of their grandchildren. Senator Cohen and I, however, had difficulty in focusing enough attention on our proposal at the time that it was first unveiled. Hopefully the recent developments have made it clear that the end of the cold war does not mean that the threat of espionage has been reduced. And with the desire of more nations to collect information, as I have said, on national economic interests, the threat to our country may actually be increasing.

So no one is under the illusion that either the bill that Senator Cohen and I introduced, or the bill, Mr. Chairman, that you and Senator Warner have introduced and which I have cosponsored, will eliminate all espionage. But I think that both of these bills and perhaps a blending of the provisions of the two could give the Government a greatly improved ability to deter U.S. citizens from spying and to detect those that are not deterred and to help prosecute those who trade our security for their enrichment.

So I hope that Congress, led by this Committee, will take this opportunity to enact meaningful reform this year.

Chairman DECONCINI. Senator Boren, thank you very much, and thank you for addressing section 807 and offering some other alternatives. I have indicated, as the Vice Chairman has, we are not married to this particular wording. What we are trying to do is find, first of all, if a legislative fix is necessary, and my early conclusion is that it is, but I may be dissuaded. And second, how to do it.

But in 1990, when you introduced your legislation, I believe it was 1990——

Senator BOREN. Yes.

Chairman DECONCINI. Actually, you had no reason to focus on this because there was a 1988 MOU——

Senator BOREN. Right.

Chairman DECONCINI [continuing]. Which is classified so I cannot put it in the record and the Vice Chairman and I are going to ask that it be declassified, because it spells out very clearly what they are to do.

Senator BOREN. Yes. How it's supposed to work.

Chairman DECONCINI. How it is supposed to work. And obviously it didn't. And let me ask you this question, hypothetical somewhat, but in the Washington Post on May 2, and it is not always the best source, because it doesn't give its source, but—and that troubles

me—but it references to 1989 when Ames returned to CIA headquarters. Redmond was again his superior as Deputy Chief of the Soviet Division. At that time according to CIA sources, Redmond was critical of Ames's work habits and tried to get him transferred. As one former CIA official said recently, Redmond pointed out that everywhere Ames had been, there'd been trouble.

Now if, in fact, and I don't know that this is fact, such a statement had been made and there was such a feeling, wouldn't that require, in your judgment, complete turning over of the case of Mr. Ames to the FBI?

Senator BOREN. Yes. Yes. I think it would. Or under the example—and again, we are dealing with a story that we don't know whether it is accurate or not—but I think that—and none of this ever, of course, reached the attention of our Committee at the time, as it wouldn't, naturally, unless you got beyond just a threshold—we were informed when there was a serious investigation proceeding, for example, and we were sometimes unfortunately informed after the fact, like the Howard case and some other things.

But I would say that under the kind of mechanism that might be established here, that apparently is being set up by the Executive order, which might be enhanced by some additional statutory enactment on the part of the Committee, that is the kind of thing that should have been reported, if you had had this Counterintelligence Center in being. Should be reported there, and it at least should have come to the three principal representatives—perhaps only to them to begin with. If this person had held such sensitive posts—to determine whether or not the FBI should have been brought in at that point. I think that kind of mechanism would have worked well in this situation.

Chairman DECONCINI. My problem is, even though you don't make it a criminal penalty for non-transferring or informing of allegations or what have you, when people swear to uphold the laws of the country, it seems to me that they are more cognizant of that than perhaps with an MOU that not everybody is aware of, because it's classified for one thing.

Senator BOREN. That's right.

No, I would say this, Mr. Chairman, that also we have to realize that we are dealing here with judgments in hindsight. It's clear to all of us now, and as Senator Cohen said, a Vega salary and a Jaguar life style. That's clear in retrospect. Very often it's hard, especially with those with whom you're working closely. I think you have sort of a natural trust of those you've worked with. Those in Operations deal in a world in which what is fact and what is fiction, what is appearance and what is reality often becomes very blurred. And sometimes these distinctions are difficult.

I think that one of the other things—and I talked to Director Woolsey about this the other day—is there probably needs to be a balance here. Obviously, it was alleged, at least, and I wasn't involved in intelligence matters during the period of time of Mr. Angleton, but it was alleged that he was so much on the alert that at least some have charged that it bordered on paranoia and that he overreacted to the degree that he may have been violating people's constitutional rights, and he was seeing a communist everywhere.

Somewhere there is a balance between that sort of viewpoint and the tendency to not be alert enough and to never be suspicious enough about those with whom one is working. And I think that the trick is to catch that balance, and probably we're in a period of time——

Vice Chairman WARNER. Let me pick up on that point there.

Senator BOREN. Yes, sir.

Vice Chairman WARNER. There seems to me two central issues we have got to address. One, this balance between the constitutional rights of individuals and the need to strengthen our security.

Senator BOREN. Yes.

Vice Chairman WARNER. And I at the present time indicate that we have got to lean a little bit now in the interest of security.

But let's go back to this Jacobs Panel and your work and Senator Cohen, and let's get something out on the table here.

Senator BOREN. Right.

Vice Chairman WARNER. Because I was a member of the Committee then.

Senator BOREN. Yes, sir.

Vice Chairman WARNER. And I have gone back and I have researched exactly what we did. We had two hearings, and then it was a decision by yourself and the Vice Chairman Cohen to drop it; you didn't go forward. Now, I listened carefully to Senator Cohen. I didn't follow-up because time didn't permit. He said, well, the cold war had lessened and we became a product of the lessening concerns of the cold war.

But it seems to me the recollections in our Committee and maybe a few footnotes and so forth indicates that the civil rights groups came in very heavily opposed to what was being done. Why didn't you bring this bill to markup?

Senator BOREN. No.

Vice Chairman WARNER. Why didn't the Full——

Senator BOREN. No, Mr. Vice Chairman——

Vice Chairman WARNER [continuing]. Committee have an opportunity to focus on that?

Senator BOREN. I'm not interested in saying why didn't we get this done at the time. We should have gotten it done at the time. And we should have moved on it ever since.

But again, I think that what happens around here is, as we know, it usually takes some sort of jolt, some kind of shock. If we go back and look at the history of most legislation, even safety legislation, we'll find it was some egregious event that caused us to pass the law. Long range planning is one of those things we do most poorly.

We did not go forward with the markup, frankly, because we found insufficient interest in the Committee and outside the Committee. We did poll a number of people. Some of the members of our Committee expressed some misgivings or concerns and we finally, we had so many other pressing things, as you recall, we were trying to work on the reorganization——

Vice Chairman WARNER. Fair enough, Senator. I think——

Senator BOREN. So that's what happened, I would say it was a general—the message we got, the two of us was, don't you two have something better to do than to push this now.

Now, on the civil rights thing, though, let me say this. We had some very good assistance from those that I would say are in the civil rights community, individual rights community—the ACLU I mention, not to reopen an earlier controversy, but Mr. Halperin, for example, at the time, worked on this legislation. I mentioned Mr. Weiss. Sol Linowitz, who is, as I think all of us know, a great civil libertarian as well as a diplomat and public servant in this country.

And when the panel met, there was real sensitivity to civil rights and individual rights' concerns, and then afterwards, we in essence discussed it with the ACLU and other groups that had these concerns, and Mr. Halperin was one of a half-dozen people from those various communities and organizations that looked at it, made constructive suggestions. And I believe by the time we were ready to go forward and hoped to go forward, when time ran out on the year and interest flagged, we had a fairly good basis of support from what I would call the civil rights community.

So I believe——

Vice Chairman WARNER. I am not here to try and——

Senator BOREN. So I believe that the Committee now, my word on this is that if the Committee decides to go forward with comprehensive reform in this area, and if it does so especially with due sensitivity to those concerns, I do not believe the Committee will find itself blocked or impeded by responsible members of those organizations.

Vice Chairman WARNER. I didn't suggest they blocked or impeded.

Senator BOREN. No, no.

Vice Chairman WARNER. They did have a constructive role.

Senator BOREN. Yes.

Vice Chairman WARNER. They are going to have a constructive role, they will be present and testifying today.

Senator BOREN. Right.

Vice Chairman WARNER. And I just don't want this Committee or the Senate to overreact because of the shock and dismay.

Senator BOREN. We have to be careful about that.

Vice Chairman WARNER. As you said, that often is the impetus for legislation.

Senator BOREN. Yes. Sometimes legislation that goes too

Vice Chairman WARNER. Lastly, you addressed section 807, and I lay down this format. You've got two independent segments of our Government, FBI and the CIA, and at some point someone has got to be in charge, someone has got to be accountable, and perhaps it was not a focus of the Jacobs Panel and your early legislation because you thought it was working because of the MOU you pointed out for the Chairman, when in fact, it was at that very period in time that some of the early Ames situation was developing——

Senator BOREN. Right.

Vice Chairman WARNER [continuing]. In such a way that had it come to the forefront at that time earlier, maybe we would have been spared.

Senator BOREN. Well, I would go back to my suggestion that I made a minute ago—and I think that this ought to apply in two areas, and I would urge the Committee, as you are looking at coun-

terintelligence concerns and how the law enforcement and intelligence gathering agencies—CIA and FBI—react on this. I would also urge you to think about what I said about the BNL case and our report there. How do they interact when CIA uncovers and stumbles across drug dealing, money laundering, violations of the law, and maybe then doesn't inform—the alarm bells don't go off, oh, we should inform the FBI about that.

I think in both situations, I really think the way to handle it—and I understand the conflict—I hear you saying, well, we've got to go all or nothing. In other words, someone has to be accountable. I agree with that. Someone has to be accountable. And so you are saying let's select, either the FBI will be solely in charge of counterintelligence, or the CIA, for example.

I am not sure that in this case that model is the right model, because of the unique situation, the kind of information you're dealing with, the compartmentalization and the high sensitivity of some of the information that you are dealing with on human source and other information gained on the CIA side. That's the reason I think if you set up this center in the right way, with three principal representatives of the Agency rotating, so that one person is the Chair, that person should be responsible for the operation of that center, that person can be held accountable by this Committee, whether it happens to be the FBI representative that year or the CIA representative that year. And you fix responsibility in this small group of three, and that that is not some sort of cast-off assignment that is unimportant. You know, well, let's just put somebody that we don't want to be the deputy director of this or that and put them over there on that coordinating committee, that's unimportant. You make that a very important post. You scrutinize the people that are selected for that to make sure they are really top flight people. And then you set up a reporting mechanism back to this Committee when a situation develops and summarize the number of situations in a year in which the three representatives are split.

Vice Chairman WARNER. We've got to move along.

Senator BOREN. I think that's a better model than going all the way.

Vice Chairman WARNER. I'm not committed to any type of legislation, but I am committed to the principles of command and control, someone's in charge——

Senator BOREN. I agree with you.

Vice Chairman WARNER [continuing]. And committed to the principles of accountability.

Senator BOREN. When everyone is in charge, no one is in charge, and I accept your point.

Chairman DECONCINI. Senator Boren, thank you very much. We could go on for some time. Other Members have, as the Chairman announced, not made their opening statements, which we are going to permit them to do now before we have our next panel, if you care to stay here, if any of them want to ask questions.

We will first yield to, as they showed up here, Senator Bryan.

Senator BRYAN. Mr. Chairman, thank you very much. In the interests of time and so that we can explore this issue with each of

the witnesses, I would ask unanimous consent that a written statement that I have, be made a part of the record.

Chairman DECONCINI. Without objection.

Thank you, Senator Bryan.

[The statement of Senator Bryan follows:]

STATEMENT OF SENATOR RICHARD H. BRYAN

Mr. Chairman, the Ames case has revealed a laxity of security in the CIA that is a scandal. The system totally broke down. The Agency failed to act for years on suspicious behavior by Ames and his wife, and the consequences were disastrous. Ames compromised our ability to track down Soviet spies, as it was his primary job to hunt them down. His actions may also have resulted in the arrest, and even execution of Russians who risked their lives to provide us intelligence information. Yet, even after his arrest, Ames displayed a callous disregard for the seriousness of his actions.

I want to thank the Chairman and the Vice Chairman for introducing legislation, of which I am a cosponsor, that attempts to address some of the serious flaws that were uncovered in our counterintelligence system. "The Counterintelligence and Security Enhancements Act of 1994" is an important step toward improving our counterintelligence and national security.

Mr. Chairman, there are many critical questions that must be answered regarding Mr. Ames and his ability to continue to wreak havoc on our intelligence capabilities for many years. For instance, I was shocked to hear reports that Ames had repeatedly shown up making suspicious financial transactions. Yet, despite the information being available to the FBI and the CIA, the red flags were ignored. This is inexcusable.

I also have serious concerns regarding a possible over-reliance on the polygraph. Mr. Ames said following his arrest that there is no special trick to passing the polygraph. How can we possibly account for Ames passing a polygraph test in the middle of his most active period of espionage?

Mr. Chairman, the intelligence community must make it a top priority to find answers to these questions, and make real changes where necessary. In addition, I feel that those who were asleep at the switch must be held accountable. I am pleased that the administration has proposed legislation on counterintelligence, and I look forward to reviewing this legislation carefully. However, I am worried the administration proposals may not go far enough.

As a member of the Senate Intelligence Committee, I am well aware of the thousands of hard-working, dedicated, patriotic personnel in the intelligence community who work daily to ensure American policy makers are the best informed leaders in the world. Yet, the Ames case has led the public to question the purpose and effectiveness of our intelligence community. We must take strong action to restore the wide credibility gap that now exists between the public and the intelligence community. I look forward to working with the this Committee and the DCI in this effort. Thank you.

Chairman DECONCINI. Senator Graham.

Senator GRAHAM of Florida. Thank you, Mr. Chairman.

Also in the interest of time, I will waive an opening statement.

Chairman DECONCINI. Thank you.

Senator Kerrey.

Senator KERREY of Nebraska. Thank you, Mr. Chairman.

Make it three for three. I will just put my statement in the record.

[The statement of Senator Kerrey follows:]

STATEMENT OF SENATOR J. ROBERT KERREY

Mr. Chairman, I suggest that our goal today should be to learn from the Ames case and to fix the defects in the intelligence community that the case reveals, but not to become fixated on the case itself. Before he was revealed as having betrayed his country and his colleagues, Ames was a loser and a mediocrity, and I can't understand why the CIA hired him and kept him around. But his betrayal does not alter the fact that the CIA's work is essential, and that it is done by people of great dedication, great patriotism, and, in many cases, great bravery.

As to the best way to fix the defects, I will hear today's testimony with a predisposition to a legislative solution. The Presidential Decision Directive (PDD) creates a new center and a new board, new job titles to soothe the egos of these agencies, but I don't see how it stops espionage. There are several simple things you can do to stop espionage: First, hire the best people; second, motivate, lead, and retain the best people and fire the poor performers; third, put the FBI in charge of the counterintelligence and law enforcement investigations and when you smell a rat, get the FBI in early. Now, you don't need legislation to hire and motivate and retain the best. You do need legislation to adopt procedures to fire the mediocrities. Senator Gorton has started the process to put that legislation in this year's Intelligence Authorization. And, given the spotty record of CIA–FBI cooperation, you probably need legislation to establish that relationship.

If any of the witnesses disagree with that approach, this is your opportunity. Thank you, Mr. Chairman.

Senator KERREY of Nebraska. But I would, if it is possible, do a follow-up question to Senator Boren as long as you're here. I must say, Senator Boren, I have got the benefit of having looked at what appears to be the details of the Presidential Policy Directive, and it's two pages long, creates a new board, a new center. Not clear to me that there's clear lines of responsibility. I mean, I must say I feel toward the two pages that I have read this morning sort of the same way that I do to Title III of the Health Security Act. I am more confused, not less confused about what it is they propose to do, whereas in section 807, I've got two paragraphs, and basically assigning to the FBI the responsibility to do CIA work, and I know therefore who is responsible.

Senator BOREN. Right.

Senator KERREY of Nebraska. The question that I have for you is as a Senator, as a citizen, as somebody who has been involved with intelligence work for a long time, what level of urgency do you attach to the need to solve this problem?

Senator BOREN. I think, Senator Kerrey, there is a level of urgency. One of my pet peeves has been the level of espionage from nontraditional sources and nontraditional countries as far as espionage is concerned.

And what I believe, as we enter the new period in our world will be a great increase in the amount of economic espionage, technological espionage, that is not strictly devoted to a military purpose or limited to a military purpose. I think that's going to increase, and I think what we are seeing around the world as economic strength becomes more and more determinate of national prestige and leadership, we're going to see what I would call a lot of things happen that will unlevel the playing field unless we're very aggressive about it.

One, aggressive in terms of stopping it from a counterintelligence point of view, stopping the spying against our country for economic secrets and stopping in third countries where, say, we and others may be competing for contracts, stopping the improper use of intelligence services of other countries to either bribe or steal secrets to bidding documents or other things that are going on. I think we have to become very tough in these matters. So I think that there is a strong level of concern.

Now, having said that, I have often said, as Chairman of the Committee, and I think all the Members who serve on this Committee and especially by the time you have served on it for 8 years, you leave with the feeling—and I say this not to excuse the CIA

for its mistakes—you leave with the feeling that it is a shame that we cannot share the successes.

Some day, for example, I hope that the story will be written about how many acts of terrorism were deterred during the Persian Gulf offensive, and what a remarkable job was done. It can't be told yet because it would endanger sources that are still in being.

And so we have 100 successes and the failure—the one failure becomes a great public matter and a cause celebre, not to underestimate for 1 minute the importance of it or the damage that it's done. The Howard case was another example; the Pelton case. We've had too many of them, I agree. And I think it shows a lack of sensitivity. I think there needs to be some revision of personnel training.

And I was getting ready to say that to Senator Warner and it slipped my mind. I think one of the things we need to do is go back and resensitize. Not go back to the Angleton years, but at least go back far enough to resensitize people within the Agency, that one of their responsibilities is to be on the lookout for anything that looks like suspicious behavior, even from people they have coffee with every day—not that we develop a paranoia inside the Agency, but we get back to this balance.

I think it is a serious problem, I think it needs to be addressed. I would urge this Committee to pass legislation and bring it out to the Senate Floor this year. And again, I would focus—we have so many points of agreement in the bills. The two points that I would focus on is one area that I mentioned where I think both bills fall short, both bills try to encompass monitoring too many people. Narrow down that universe so that you can do a really good job with a reasonable number of people. Otherwise, it is sort of like Senator Warner said, when everyone is in charge, no one is in charge. When we monitor everybody, 500,000 or a million people, we don't monitor anybody very well, so let's not fool ourselves. That would be cosmetic. So let's do that.

Chairman DECONCINI. Senator Boren, I'm sorry, we've got to move, unless the Senator has another question.

Senator BOREN. Thank you, very much.

Chairman DECONCINI. Thank you Senator Boren, very much, for your testimony.

Vice Chairman WARNER. Just a minute, before he leaves, I can't resist this. I am reading from a report of the U.S. Senate. The year is 1986. It was your predecessor as Chairman and Vice Chairman, page 45.

Senator BOREN. Yes.

Vice Chairman WARNER. Another aspect of counterintelligence awareness is the knowledge by Agency security officials of when to bring a matter to the attention of a U.S. counterintelligence agency. In the Edward Lee Howard case, CIA security officials failed to alert and involve the FBI in a timely fashion. And the Senate wrote, "the CIA has taken steps recently to guard against a recurrence of this problem."

Now professor, you have given us a lecture this morning. Am I correct about the old English proverb, that the road to hell was paved with the best of intentions.

Senator BOREN. Yes, sir. That's the reason I would not leave it, quite frankly, if I were you, while I would work in a non-adversarial, but as I say, a very candid role with some of the very good people you have in this community, I would not leave it strictly to the discretion of the executive branch. I would put in place some statutory enactment on this matter. I have given you my suggestions as to how to do it. But I would not leave it to the whim—I would put a statutory enactment in and if you put a reporting mechanism—whatever mechanism you put into law, if you put a reporting mechanism back to this Committee, as we did with our independent Inspector General. I think you'll find that it will work and that there will be accountability.

Vice Chairman WARNER. Your point is clear, and we close on a note. The intelligence in our country is served by many, many wonderful, the predominately, the majority of wonderful public servants. I think this is as much a protection to their reputation——

Senator BOREN. Absolutely.

Vice Chairman WARNER [continuing]. And their good will and their ability to perform their function.

Senator BOREN. This Committee, in doing some of the things it has done in the past and things you are now considering, has done more to protect our good, professional people who operate within the law and who operate well, than anything I can possibly imagine.

Chairman DECONCINI. Thank you, Senator Boren. Thank you very much.

Our next panel—and I apologize for the time and the delay, and we do have to move along, we have to be out of this room by 1 o'clock and I know they have busy schedules—is the Honorable Jamie Gorelick, the Deputy Attorney General; the Director of Central Intelligence, Mr. James Woolsey; and the Director of the Federal Bureau of Investigation, Mr. Freeh.

As I understand it, Ms. Gorelick will present the views of the administration with regard to pending legislation. She also plans to outline for us the legislative proposal which the administration has itself developed. And I would ask her if she could summarize that, because we have had some indication of that by our previous panels.

Following her remarks, we'll ask Mr. Woolsey and Director Freeh to make any comments they wish to make. It is my understanding they will describe for us the decisions taken yesterday by the President to improve the organization arrangements for the conduct of counterintelligence activities.

We welcome you to the Committee, and I recognize that you have made a substantial effort over the last few weeks. As Mr. Lake, the President's advisor on national security, indicated to me 1 month ago, he would see that it happened, and I compliment him and you for seeing that that has come about.

I, of course, want to be part of a constructive effort here to improve the situation. Section 807 that we have discussed at some length, you might make reference to that, Mr. Woolsey, and Mr. Freeh, when you comment after Ms. Gorelick.

Ms. Gorelick.

[The prepared statement of Ms. Gorelick follows:]

PREPARED STATEMENT OF JAMIE S. GORELICK

Mr. Chairman and members of the Committee:

It is a pleasure to appear before you today to present the administration's views on a number of legislative proposals currently before Congress that would enhance the Government's personnel security and counterintelligence programs. I would also like to use this opportunity to present to this distinguished Committee the administration's own legislative proposal in this area: The Counterintelligence and Security Enhancements Act of 1994.

While the United States is extremely proud of the many thousands of dedicated, loyal citizens who serve in sensitive positions and who deal daily with matters affecting grave national security interests, there are a very few individuals who, for reasons of financial gain or otherwise, betray their country.

Indeed, since 1980, the Department of Justice has prosecuted 68 individuals for espionage and related offenses. All of us should be concerned by the clandestine activities conducted by hostile foreign intelligence services and, likewise, by the acts of those few American citizens who have breached the trust reposed in them by the American people.

The five bills that have been introduced in Congress—H.R. 4137, S. 1948, S. 1869, S. 1889 and S. 1866—address three general areas of concern: Improvement of the personnel security system; penalties for espionage-related activities: and enhanced counterintelligence investigative capabilities. Many of these proposals include recommendations from the Jacobs Panel, a group of private citizens convened several years ago by Senators Cohen and Boren to advise the Senate Select Committee on Intelligence on improvements that could be made in the Government's counterintelligence program.

I will briefly discuss each of these bills. In addition, I will present the administration's alternative bill which I believe reflects the best framework for cooperation between Congress and the President on this issue. Before proceeding, however, let me say on behalf of the administration that we view the bills that have been introduced as evidence of a bipartisan effort to improve personnel security and counterintelligence measures, and we welcome the opportunity to work with the Committee and its representatives in this important effort.

I. PROPOSALS CONCERNING THE PERSONNEL SECURITY PROGRAM

a. The Five Congressional Bills

All five bills introduced thus far include proposals to improve the personnel security system. Three of them—S. 1866 (introduced by Senator Metzenbaum), S. 1869 (introduced by Senators Cohen and Boren), and H.R. 4137 (introduced by Representatives Hyde and Wilson)—would amend the National Security Act of 1947 by establishing certain uniform, minimum requirements for persons to be granted a top secret security clearance. All candidates for a top secret clearance would be required, among other things, to consent to access to their financial records, consumer credit reports, and records of foreign travel for the period of their access to top secret information and for the 5 years following termination of such access. Such individuals would also be required to report certain contacts with foreign nationals and all foreign travel not part of their official duties, and would be subject to investigation at any time to determine their continued access to top secret information. Waivers of the minimum requirements could be granted, but must be recorded and reported to both the Senate and House intelligence committees.

A fourth bill—S. 1948 (introduced by Senators DeConcini and Warner)—would require that employees of intelligence agencies provide access to investigators to tax returns, bank and investment accounts, and other assets. In addition, those intelligence community employees with access to "critical intelligence information", e.g., information revealing the identities of covert agents or a technical collection system, would be required to provide a statement disclosing the nature and location of all bank accounts, investment accounts, credit accounts, and assets valued at more than $10,000 in which the employee, or any member of the family of the employee, has a beneficial interest.

We think it reasonable that people whose positions afford them access to the most sensitive information should be subject to heightened scrutiny and agree with the desirability of uniform minimum standards. We question, however, whether the standards and mechanisms for access determinations should be mandated by legislation. The problem with a "legislative solution" is that, at best, it fixes rules as of a point in time. This is not the best way to address the dynamics of administering a personnel security program applying to many thousands of employees in many different and diverse agencies.

The administration is actively addressing the issue of more uniform standards and heightened scrutiny. By centralizing this authority within the administration, the individual needs and circumstances of the various agencies affected can be considered and accommodated, and the flexibility needed to respond to changing conditions and lessons learned can be retained.

In addition, the legislative proposals that have been introduced address only selected aspects of personnel security requirements. We are concerned that imposing certain requirements by statute, while other requirements lack statutory authorization, may place the executive branch in a more difficult position in defending the non-statutory procedures against legal challenge. Nevertheless, we are carefully considering the bills that have been introduced as we move forward with this process.

Two bills also add to the National Security Act of 1947 a section providing uniform eligibility requirements for access to cryptographic information. The requirements include periodic counterintelligence scope polygraph examinations.

Espionage cases in the last decade have demonstrated that personnel with access to U.S. cryptographic information and keys are targeted by hostile intelligence services. These bills rightly recognize that such information and material is uniquely important to the national security. Our principal concern here, as with legislated uniform standards for access to top secret information, is that we believe such standards should be set by the President, not Congress, in order to preserve needed flexibility with respect to individual agency needs and changing circumstances.

A fifth bill—S. 1890 (introduced by Senator Heflin) would require that the head of each agency within the intelligence community submit to the President, and to the House and Senate intelligence committees, a list of all positions that are classified at or below the level of GS–15 and that require access to "information critical to the national security", a term that is not further defined. Thereafter, any individual occupying such a position would have to file financial disclosure statements under the Ethics in Government Act of 1978.

However, as many of you already know, disclosures required by the Ethics in Government Act are not designed to elicit the kind of information, with the requisite degree of specificity, that is required for counterintelligence purposes. Consequently, the remedial effect of that provision is quite minimal.

b. The Administration Alternatives

As I stated above, the administration feels strongly that standard-setting in the counterintelligence area is most properly left to the executive branch. Accordingly, while we are very appreciative of the hard work and thoughtful proposals of the sponsors of these bills, the administration has developed its own legislative proposal—one that we feel takes into account the need to address the circumstances and needs of the various agencies affected by this legislation, while preserving much-needed flexibility to react to changing situations.

Our bill establishes a broad framework for granting access to classified information. It would, for the first time, provide a statutory basis for the personnel security system used to adjudicate access to classified information and would require that the President direct issuance of a regulation binding on all executive branch agencies to implement this system. The administration intends to accomplish this through an Executive order that would be implemented by agency regulations.

The administration is also considering a separate Executive order to enhance our counterintelligence capabilities with respect to employees with access to particularly sensitive classified information. Among other things, the administration would like to require that certain employees with access to classified information provide consent, during the initial background investigation and for such time as such access is maintained, and for 5 years thereafter, for access to financial records, consumer reports, and travel records. However, this will require legislation because the Right to Financial Privacy must be amended to permit employee consent that is valid for more than 90 days.

In addition, the administration is also considering requiring financial disclosure of persons occupying positions designated by agency heads as requiring access to particularly sensitive classified information. Such information might include the identities of covert agents, technical or specialized national intelligence collection systems, cryptographic systems, and certain Department of Defense special access programs.

We are also contemplating the use of automated financial record data bases already maintained by the Department of the Treasury where warranted in background investigations. These data bases include reports of currency transactions by financial institutions, international transportation of currency, and foreign bank and financial accounts. A joint test was recently conducted by the Financial Crimes Net-

work of the Treasury Department and the Department of Defense. Preliminary analysis indicates this may be a very useful tool in the early detection of espionage.

This order has not been finalized, and we look forward to consulting with the Committee and its representatives on this draft order before it is submitted to the Office of Management and Budget for agency clearance.

II. PENALTIES FOR ESPIONAGE-RELATED ACTIVITIES

Three of the five bills introduced—the exceptions are S. 1866 introduced by Senator Metzenbaum and S. 1890 by Senator Heflin—include new penalties for various espionage-related activities. Many of these proposals reflect recommendations made earlier by the Jacobs Panel.

In general, the administration supports expanding the existing statute regarding forfeiture of collateral profits of crime to include espionage offenses, and denying retired pay to persons convicted in foreign courts of espionage involving U.S. information. These two initiatives are included, in substantial part, in the administration bill.

Bills already introduced in Congress would also create new criminal offenses for the sale or transfer of top secret documents to a foreign government, and for the unauthorized removal and retention of top secret documents. These new offenses are an attempt to eliminate trial testimony about the nature of the information compromised as now required by 18 U.S.C., sections 793 and 794, to prove its relationship to the national defense. We are anxious to explore new options in this regard, but there are technical and practical aspects of the proposal to criminalize the sale or transfer of top secret documents to a foreign power that deserve more consideration. For example, it is unclear whether the term "knowingly" modifies "sell or otherwise transfer," thereby only requiring a voluntary and intentional transaction, or whether it means that the offender must know the information has been classified top secret. We also believe that, if such a provision is to be passed, it should encompass all classified information.

With respect to the unauthorized removal and retention of top secret documents, we believe this provision may have merit in egregious cases and deserves further study. Its practical result, however, must not be for prosecutors to take cases of minimal importance in situations that could be better addressed by agencies more carefully policing their personnel. In terms of this policing, it is obvious that greater uniformity of rules and of the application of those rules is needed.

Another provision found in the bills would create a new criminal offense for the possession of espionage devices, defined as devices "primarily useful for the purpose of surreptitiously collecting or communicating information." For the crime to be complete, possession of such a device must be accompanied by the intent to use it to commit espionage. The essential element of the offense—that the device is primarily useful for the surreptitious collection or communication of information—may be quite difficult to establish. Moreover, it would appear that the gravamen of the offense is the possession of paraphernalia with requisite intent, regardless of whether the items have an innocent primary purpose. We believe this proposal needs more careful thought before going forward, but generally supports its objective.

The administration plan is a combination of the most significant and relevant proposals regarding penalties for espionage-related activities found in the five bills currently pending in Congress. Consequently, the administration's plan encompasses what we believe are two of the most important and practical provisions found in the bills: Forfeiture of collateral profits and denial of annuities.

III. ENHANCED COUNTERINTELLIGENCE INVESTIGATIVE CAPABILITIES

There are a number of useful proposals contained in the various bills that would enhance our capability to detect and investigate agents of foreign powers, and are included in the administration's legislative proposal.

All four of the bills would amend the Fair Credit Reporting Act to authorize the Federal Bureau of Investigation to obtain consumer reports on persons believed to be agents of a foreign power. This welcome proposal is absolutely essential for the FBI and would resolve an anomaly in existing law. Let me be more specific.

The Right to Financial Privacy Act allows counterintelligence investigators access to bank records of an individual who is the target of an investigation, yet the Consumer Credit Reporting Act does not allow similar access to records which would serve to identify the bank the individual uses. The administration has requested a similar provision in the past as part of the intelligence authorization process that would permit access to consumer records on the same controlled basis as is now the case under the Right to Financial Privacy Act. We also note that, unlike the DeConcini/Warner bill, the administration bill would permit the FBI to disseminate

consumer credit information to the military services conducting all counterintelligence investigations in close cooperation with the Bureau.

Three of the four bills contain provisions that would enhance the ability of investigative agencies to gain access to financial records. S. 1869 (Cohen/Boren) and H.R. 4137 (Hyde/Wilson) would amend the Right to Financial Privacy Act to require persons with access to top secret information to authorize nonrevokable access to financial records for the period of access to top secret information and for 5 years thereafter. Although passage of this provision would be helpful, we believe that limiting these authorizations to persons with top secret access may not capture all persons with access to particularly sensitive classified information. The President should have the flexibility to designate employees to be covered.

S. 1948 (DeConcini/Warner) would authorize similar access to financial records but is also limited in the sense that it is applicable only to employees of the intelligence community. A critical aspect of this bill is, however, that it contains a confidentiality section that prevents an entity from disclosing to the customer that it has received or satisfied a request made by an authorized investigative agency. In most cases—the exception being routine background investigations—it is essential to the integrity of the investigation that the person on whom records have been requested not know of the inquiry.

The administration bill includes a provision, very similar to that proposed by Senators DeConcini and Warner, authorizing consensual access to financial records and consumer reports, with the exception that its scope is not limited to employees of the intelligence community and encompasses all persons with access to classified information. The administration intends to designate employees who will be covered by this provision in an Executive order. In addition, the bill limits when the Government may use that consent to actually obtain the financial information.

Several of the bills already introduced would also clarify the venue of U.S. district courts to try cases involving espionage outside the United States and provide for rewards for information concerning espionage. The venue proposal is designed to cure what is essentially a technical problem, and the administration fully supports it in its entirety.

As for offering rewards, we are in full agreement that rewards are a useful incentive, but we are concerned that whatever funds are set aside for this concept will have to be provided by Congress. In addition, if this provision is passed, we must be cautious not to undermine the existing obligation on the part of individuals with security clearances to report suspected breaches of security. Specifically, it is our view that this proposal contains sufficient administrative discretion to allow us to consider any pre-existing obligation to report as a factor in determining if a reward is appropriate.

The final provision I wish to discuss with you causes us some concern. Section 807 of S. 1948, the DeConcini/Warner bill, attempts to revise and define the division of counterintelligence responsibilities between the Federal Bureau of Investigation and the Central Intelligence Agency. These responsibilities are currently set forth in Executive Order 12333 and its implementing procedures.

The President has directed a comprehensive reexamination of the effectiveness of our counterintelligence efforts based on the principles of integration, cooperation, and accountability. A directive that delineates the specific steps that will be taken to achieve improved cooperation and coordination of our counterintelligence activities is now on the President's desk for signature. Director Woolsey and Director Freeh can provide an overview of this proposed directive. We think legislation in this area is unnecessary.

I close as I began, by commending the sponsors of these bills for their conscientious and valuable efforts. I would like to emphasize the administration's willingness to work with the Committee to achieve improved counterintelligence measures. I should also note that some of these proposals may require additional resources to implement effectively, and we will work cooperatively with Congress to accomplish this. Thank you for the opportunity to appear before you, and I will be happy to answer any of your questions.

TESTIMONY OF JAMIE S. GORELICK

Ms. GORELICK. Thank you, Mr. Chairman, members of the Committee.

It's a pleasure to appear before you today to present the administration's views on a number of legislative proposals that are currently before Congress, that would enhance the Government's personnel security and counterintelligence programs.

I would also like to use this opportunity to present to this distinguished Committee the administration's own legislative proposal in this area, the Counterintelligence and Security Enhancements Act of 1994.

While the United States is extremely proud of the many thousands of dedicated and loyal citizens who serve in sensitive positions and who deal daily with matters affecting the grave national security interests of this country, there are a few individuals, who for reasons of financial gain or otherwise, betray their country. Indeed, since 1980, the Department of Justice has prosecuted 68 individuals for espionage and related offenses.

All of us should be concerned by the clandestine activities conducted by hostile foreign intelligence services, and likewise by the acts of those very few American citizens who have breached the trust reposed in them by the American people.

Now, five bills have been introduced in Congress: H.R. 4137; S. 1948; S. 1869; S. 1889; and S. 1866. And they address three general areas of concern that I would like to discuss.

They are improvement of the personnel security system; penalties for espionage-related activities; and enhanced counterintelligence investigative capabilities. Many of these proposals include recommendations from the Jacobs Panel, a group of private citizens convened several years ago by Senators Cohen and Boren, to advise the Senate Select Committee on Intelligence on improvements that could be made in our counterintelligence program.

I will briefly discuss each of the bills and present our alternative bill, which I believe reflects the best framework for cooperation between Congress and the President on this important issue. Let me say on behalf of this administration that we view the bills that have been introduced as evidence of a bipartisan effort to improve our personnel security and counterintelligence capabilities, and we welcome the opportunity to work with this Committee and its representatives on this important effort.

Now, let me first discuss the five bills that are pending. All five include proposals to improve the personnel security system. Three of them—S. 1886, S. 1869, and H.R. 4137—would amend the National Security Act of 1947 by establishing certain uniform minimum requirements for persons to be granted top secret security clearance. And all candidates for a top secret clearance would be required, among other things, to consent to access to their financial records, consumer credit reports, and records of foreign travel, for the period of their access to top secret information and for the period of 5 years following the termination of their access.

They would also be required to report certain contacts with foreign nationals, all foreign travel not part of their official duties, and they would be subject to investigation at any time to determine their continued access to top secret information. Waivers of these requirements could be granted, but would have to be recorded and reported to the Senate and House Intelligence Committees.

A fourth bill, S. 1948, introduced by Senators DeConcini and Warner, would require that employees of intelligence agencies provide access to investigators to tax returns, bank and investment accounts, and other assets, and those Intelligence Community employees to, "critical intelligence information" would be required to

provide a disclosure statement relating to bank accounts, investment accounts, etc.

We think it reasonable that people whose positions afford them access to the most sensitive Government information should be subject to heightened scrutiny, and we agree with the desirability of uniform minimum standards.

We question, however, whether the standards and mechanisms for access to termination should be mandated by legislation. The problem with the legislative solution in this area is that it fixes rules at this particular point in time, and given the dynamics and the interest of different agencies in this regard, we believe that the best way to address the personnel security system that applies to many thousand employees in different and diverse circumstances, is administratively. That is the recommendation of the Joint Security Commission, and we are actively pursuing a uniform Government mechanism for dealing with these issues.

We believe that by centralizing authority within the administration, the individual needs and the circumstances of the various agencies can be considered and accommodated, and the flexibility needed to respond and address changing conditions and lessons learned can be retained.

The other problem is that the legislative proposals address only selected aspects of personnel security requirements. And we are concerned that by imposing requirements by statute, while other requirements lack statutory authorization, that may place the executive branch in a more difficult position when we are trying to defend the non-statutory procedures against legal challenge.

We are carefully considering these bills and we will be happy to engage in a dialog with this Committee on those provisions.

Now, two provisions also would add to the National Security Act of 1947—a section providing uniform eligibility requirements for access to cryptographic information. Other requirements include periodic counterintelligence scope polygraph examinations.

Espionage cases in the last decade have demonstrated that personnel with access to U.S. cryptographic information and keys are targeted by hostile intelligence services. These bills rightly recognize that such information and material are uniquely important to the national security.

Our principal concern here, as with the legislative uniform standards for personnel for access to top secret information is that we believe that such standards should be set by the President to preserve the needed flexibility with respect to individual agency needs and changing circumstances.

A fifth bill, S. 1890, would require that the head of each agency within the intelligence community submit to the President and to the House and Senate Intelligence Committees a list of all positions that are classified at or below the GS–15 level that require access to, "information critical to the national security," a term that is not further defined. Thereafter, any individual occupying such a position would have to file a financial disclosure statement under the Ethics in Government Act.

As you already know, disclosures required by the Ethics in Government Act are not designed to elicit the kind of information with the requisite degree of specificity that is required for counterintel-

ligence purposes. And we question the remedial effect of this particular provision.

As I stated above, our administration feels very strongly that the standards setting in the counterintelligence area that we have discussed is most properly in the executive branch. And accordingly, while we are appreciative of the thoughtful proposals of the sponsors of these bills, we have developed our own legislative proposal that we feel takes into account the need to address the circumstances and the needs of the various agencies that would be affected by this legislation, while preserving much-needed flexibility.

Our bill establishes, first, a broad framework for granting access to classified information. It would, for the first time, provide a statutory basis for a personnel security system used to adjudicate access to classified information. And it would require that the President direct issuance of a regulation binding on all executive branch agencies to implement this system. We intend to accomplish this through an Executive order that we are working on right now that would be implemented by Agency regulation.

We are also considering a separate Executive order to enhance our counterintelligence capabilities with respect to employees with access to particularly sensitive classified information. Such employees would provide consent during their initial background investigation and for such time as access is maintained and for 5 years thereafter, for access to certain financial records, consumer reports, and travel records.

Now, this will require legislation, because the Right to Financial Privacy Act limits the current employee consent to a 90-day period of validity.

In addition, we are also considering requiring financial disclosure by persons occupying positions designated by agency heads as requiring access to particularly sensitive classified information. Such information might include the identities of covert agents, technical or specialized national intelligence systems, cryptographic systems, and certain DOD special access programs.

We are also contemplating the use of automated financial record data bases, that are already maintained by the Department of Treasury, where warranted, in background investigations. These data bases include reports of currency transactions maintained by financial institutions, international transportation of currency, and foreign bank and financial accounts.

A joint test was recently conducted by the Financial Crimes Network of the Treasury Department and the Department of Defense, and preliminary analysis indicates that this may indeed be a very useful tool in the early detection of espionage. This order has not been finalized. We look forward to working with this Committee on the draft order before it is submitted to OMB.

Three of the bills introduced—the exceptions are S. 1866 and S. 1890—include new penalties for various espionage-related activities. Many of these proposals reflect recommendations made earlier by the Jacobs Panel. In general, we support expanding the existing statute regarding forfeiture of collateral profits of crime, to include espionage offenses, and denying retired pay to persons convicted in foreign courts of espionage involving U.S. information.

And these two initiatives are included in substantial part in the administration's bill.

Bills already introduced in Congress would also create new criminal offenses for the sale or transfer of top secret documents to foreign governments, and for the unauthorized removal and retention of top secret documents. These new offenses are an attempt to eliminate trial testimony about the nature of the information compromised, as is now required by Title 18. And we are anxious to explore new options in this regard. But there are technical and practical aspects of the proposal to criminalize the sale or transfer of top secret documents to a foreign power that I will tell you deserve more consideration and more discussion between us.

For example, it is unclear whether the term knowingly modifies sell or otherwise transfer, and thereby only requires a voluntary or intentional transaction, or whether the offender must know that the information has been indeed classified as top secret.

We also believe that if such a provision is passed, it should not be limited to top secret information.

With respect to the unauthorized removal or retention of top secret documents, this provision also has merit in egregious cases and deserves further study and work together. It may not be practical for prosecutors to take cases that are, in fact, of minimal importance in terms of the compromise of information, and we need to determine the best way to focus our prosecutorial resources in this regard. And it is also important that we achieve uniformity in the application of these rules administratively.

Another provision in two of the bills would create a new criminal offense for the possession of espionage devices and for the crime to be complete, possession must be accompanied by the intent to use the device to commit espionage. The essential element of the offense, which is that the device be primarily useful for the surreptitious collection or communication of information may be difficult to establish, and again, this is a provision that we believe needs more careful thought.

Our plan is a combination of the most significant and relevant proposals regarding penalties in the espionage-related activities area that are found in the five pending bills. And we believe that it encompasses two of the most important aspects of the five pending bills. That is, forfeiture of collateral profits, and denial of annuities.

I'd like now to turn to the issue of enhanced counterintelligence investigative capabilities that you have principally focused on this morning. There are a number of useful proposals in the various bills that would enhance our capability to detect and investigate agents of foreign powers, and they are included in our legislative proposal.

Four of the bills would amend the Fair Credit Reporting Act to authorize the FBI to obtain consumer reports on persons believed to be agents of a foreign power. And we welcome this proposal. It is absolutely essential for the FBI, and it would resolve an anomaly in existing law.

The Right to Financial Privacy Act now allows counterintelligence investigators to have access to banks' records with respect to an individual who is the target of an investigation, but the

Consumer Credit Reporting Act does not allow similar access to records that would identify the bank.

The administration has requested a similar provision in the past, as part of the Intelligence Authorization process, and we note that, unlike the DeConcini-Warner bill, the administration bill would permit the FBI to disseminate consumer credit information to the military services conducting counterintelligence investigations in close cooperation with the Bureau.

Now, three of the four bills contain provisions that would enhance the ability of investigative agencies to gain access to financial records. S. 1869 and H.R. 4137 would amend the Right to Financial Privacy Act to require persons with access to top secret information to authorize nonrevokable access to financial information for the period of access to top secret information and for 5 years thereafter. Although passage of this provision would be helpful, we believe that limiting it to persons with top secret clearance may not capture all persons with access to particularly sensitive classified information. And we believe that the President should have the capability and the authority to designate the employees who are to be covered.

The DeConcini-Warner bill would authorize similar access to financial information, but it is limited in that it is applicable only to employees in the intelligence community. A critical aspect of this bill is, however, that it contain a confidentiality section that prevents an entity—a financial entity—form informing or disclosing to the customer that it has received or satisfied a request that is made by an authorized investigative agency. In most cases—the exception being routine background investigations—it is essential that the investigation proceed with that confidentiality. The integrity of the investigation must be maintained and the person on whom records have been requested must not know of the inquiry.

Our bill also includes a provision that is very similar to that proposed by Senators DeConcini and Warner, that authorizes consensual access to financial records and consumer reports, except that our bill is not limited to employees of the intelligence community, and it encompasses all persons with access to classified information. We intend to designate the employees who will be covered by this provision in an Executive order.

In addition, the bill limits when the Government may use that consent to actually obtain financial information. A few—several of the bills would also clarify the venue of the U.S. district courts to try certain cases involving espionage outside the United States, and we have incorporated those proposals in our bill.

As for offering rewards, we are in full agreement with the necessity for being able to offer rewards. Our construction of this provision is slightly different than we've seen in some of the bills, but we believe that we can work with the Committee on this provision.

Finally, I'd like to discuss a provision that causes us some concern, which is section 807. It attempts to revise and define the division of responsibility, of counterintelligence responsibility between the Bureau and the CIA. These responsibilities are currently set forth in Executive Order 12333 and its implementing procedures. We have undertaken a comprehensive examination of the effective-

ness of our counterintelligence efforts, based on the principles of integration, cooperation, and accountability.

A directive that delineates the specific steps that will be taken to achieve improved cooperation and coordination of our counterintelligence activities has been signed this morning by the President. Director Woolsey and Director Freeh can provide an overview of this proposed Directive. But we think that legislation in this area is unnecessary and I would be happy to answer your questions in this regard.

I close as I began, by commending the sponsors of these various bills for their conscientious and valuable efforts. I would like to emphasize our strong willingness to work with the Committee to achieve improved counterintelligence measures, and I would note that these—some of the proposals require additional work by us and additional colloquy with this Committee.

I thank you for the opportunity to appear, and I would be happy to answer any of your questions.

Thank you very much.

Chairman DECONCINI. Thank you very much, Ms. Gorelick. I appreciate your testimony and your analysis of the bill. I am going to ask the staff from our Committee to attempt, after your presentation here and what we have, to lay out these bills for the Members in a spreadsheet so we can get some clear distinctions between the bills.

Ms. GORELICK. We may be able to help in that regard, sir.

Chairman DECONCINI. Mr. Woolsey.

[The prepared statement of Director Woolsey follows:]

PREPARED STATEMENT OF R. JAMES WOOLSEY

Mr. Chairman and members of the Committee, I welcome the opportunity to testify before this Committee on the critical question of counterintelligence. I support fully the statement of Deputy Attorney General Gorelick. The Counterintelligence and Security Enhancements Act of 1994—the President's bill which the Deputy Attorney General described in her opening statement—addresses many of the issues incorporated in the various legislative proposals put forth in both the Senate and the House. I urge this Committee to give full support to the President's bill.

But legislation is only a partial solution. We need new procedures to ensure effective coordination between law enforcement and intelligence. As we were supporting the President in crafting the bill you have before you today, we were also active in the National Security Council Review which led to Presidential Decision Directive 44 authorizing significant changes in counterintelligence coordination. By placing the policy and coordinating machinery of counterintelligence in the hands of the National Security Council itself, the President can be confident of the full cooperation, not only of the CIA and the FBI, but of all agencies and departments of Government involved in counterintelligence. I pledge to you the full and unwavering cooperation of the CIA and the intelligence community in seeing that this Presidential Decision Directive is effectively implemented, without regard to bureaucratic impediments.

These two documents—the administration bill and the Presidential Directive—are essential if we are to strengthen counterintelligence. But they are not enough.

As I have informed the Committee in the past, I am committed to learning all that we can from the Ames case. I am committed to seeing expanded cooperation between law enforcement and intelligence. As far as I am concerned, even one case of unnecessary friction between CIA and FBI is one the President and the Congress should not tolerate and the Nation cannot afford. And I am committed to changing not only the way we conduct our business, but the way we think about our roles and responsibilities.

In the aftermath of the sentencing of Aldrich Ames, we have been able to accelerate the inspector general's investigation and the damage assessment launched at the CIA since there is no longer a possibility that they will interfere with Ames'

prosecution. However, I do not intend to wait until those reviews are completed before taking several key actions.

These actions are guided by a straightforward formula: for counterintelligence to be more effective we need constant interaction between three groups of government officials: investigators, managers, and overseas intelligence collectors. I am taking action in all three areas.

First, the investigators. They need vital information, and as we all know, that means access to financial information. At CIA I have ordered all employees to provide a full accounting of their personal finances. The legislation the Preisdent is proposing would give us the essential tool to check these records by allowing investigators earlier access to financial data for corroboration.

Second, the managers: those who oversee employees with access to classified information. Managers do not simply manage issues or regions, they manage people. And they have to be alert to irregularities which could point to a counterintelligence problem. Last week I signed a directive to all CIA managers underscoring their personal responsibilities for the quality of the security and counterintelligence aspects of their operations. I have provided them with a list of specific actions. To help them, I have directed mandatory training courses in counterintelligence.

Third, foreign intelligence collectors. Foreign intelligence collection and counterintelligence must be inseparable. I have made clear to our officers serving abroad that counterintelligence is a top priority, and working effectively with the FBI is imperative.

I would ask this Committee to support the President's bill, to give us the tools to build on what has happened in order to improve our ability to serve the President, the Congress, and the American people. Thank you.

TESTIMONY OF R. JAMES WOOLSEY

Director WOOLSEY. Thank you, Mr. Chairman, members of the Committee. I welcome the opportunity to testify before this Committee on the critical question of counterintelligence. I support fully the statement of Deputy Attorney General Gorelick.

The Counterintelligence and Security Enhancements Act of 1994, the President's bill, which the Deputy Attorney General described in her opening statement, addresses many of the issues incorporated in the various legislative proposals put forth in both the Senate and the House. I urge this Committee to give full support to the President's bill.

But legislation is only a partial solution. We need new procedures to ensure effective coordination between law enforcement and intelligence. As we were supporting the President in crafting the bill that you have before you today, we were also active in the National Security Council review, which led to Presidential Decision Directive 44, authorizing significant changes in counterintelligence coordination. By placing the policy and coordinating machinery of counterintelligence in the hands of the National Security Council itself, the President can be confident of the full cooperation not only of the CIA and the FBI, but of all agencies and departments of Government involving counterintelligence. I pledge to you the full and unwavering cooperation of the CIA and the intelligence community in seeing that this Presidential Decision Directive is effectively implemented without regard to bureaucratic impediments.

These two documents—the administration bill and the Presidential Directive—are essential if we are to strengthen counterintelligence. But they also are not enough.

As I have informed the Committee in the past, I am committed to learning all that we can from the Ames case. I am committed to seeing expanded cooperation between law enforcement and intelligence. As far as I am concerned, even one case of unnecessary friction between CIA and FBI is one that the President and the

Congress should not tolerate and the Nation cannot afford. And I am committed to changing not only the way we conduct our business, but the way we think about our roles and responsibilities.

In the aftermath of the sentencing of Aldrich Ames, we have been able to accelerate the Inspector General's investigation and the damage assessment launched at the CIA. However, I do not intend to wait until those reviews are completed before taking several actions. These actions are guided by a straightforward formula. For counterintelligence to be more effective, we need constant interaction between three groups of Government officials—investigators, managers, and overseas intelligence collectors. I'm taking action in all three.

First, the investigators. They need vital information, and as we all know, that means access to financial information. At CIA I have ordered all employees to provide a full accounting of their personal finances. The legislation the President is proposing would give us the essential tool to check these records by allowing investigators earlier access to financial data for corroboration.

Second, the managers. Those who oversee employees with access to classified information. Managers do not simply manage issues or regions, they manage people. And they have to be alert to irregularities which could point to a counterintelligence problem. Last week I signed a directive to all CIA managers underscoring their personal responsibilities for the quality of the security and counterintelligence aspects of their operations. I provided them with a list of specific actions. To help them, I have directed mandatory training courses in counterintelligence, and as I have said before, Mr. Chairman, members of the Committee, following the completion of the Inspector General's investigation, which I ordered begun last month—actually in March—if recommendations are made which would require me to take action to discipline individuals who have behaved negligently or improperly in the past, I'll review those issues and make those decisions at that time.

Third, foreign intelligence collectors need to be part of this picture. Foreign intelligence collection and counterintelligence must be inseparable. I have made clear to our officers serving abroad, that counterintelligence is a top priority and working effectively with the FBI is imperative. We can address, perhaps in your questions, some of the issues related to teamwork that will be, I think, affected by the Presidential Decision Directive.

I ask this Committee to support the President's bill and the new Directive, to give us the tools to build on what's happened in order to improve our ability to serve the President, the Congress, and the American people.

Thank you, Mr. Chairman.

Chairman DECONCINI. Thank you, Mr. Woolsey, very much. Judge Freeh.

[The prepared statement of Director Freeh follows:]

PREPARED STATEMENT OF LOUIS J. FREEH

The Aldrich Ames espionage case has been a sobering experience for America.

There are invaluable lessons to be learned from it. Any moles who are still in place must be unmasked.

Steps must be taken to prevent future spies from succeeding.

The root cause of the Ames case—the things that enabled him to gravely damage our national security for so long—were counterintelligence procedures and programs that did not work.

There also were human failings.

However, our task is not to find scapegoats.

Rather, we must minutely examine this case to discover precisely what went wrong and then develop and scrupulously maintain programs that will prevent such catastrophes.

We need to find out if there are others like Aldrich Ames who are at this moment camouflaged within the national security bureaucracy as they carry out their deadly work.

We also need large—and constant—doses of preventive medicine.

Development of the needed countermeasures against spies requires no magic. We know what needs to be done.

The difficult part will be to develop complete cooperation among all Federal officials with national security responsibilities; for without complete cooperation, it will be only a matter of time before another Aldrich Ames endangers our Nation's well-being.

Only spies are aided when Government agencies engage in senseless turf battles with each other; agencies can become so obsessed with competing against each other that they fail to carry out the needed steps to unmask spies.

It staggers the imagination to think that anyone who has sworn to protect this country would put petty bureaucratic goals ahead of the national interest; that otherwise dedicated public servants would think that the well-being of their unit or division or agency was more important than the safety of hundreds of millions of American citizens.

For the safety of our people is what this is really all about.

The cold war with the former Soviet Union may have ended.

But it would be dangerously naive not to recognize that the United States is faced with the prospect of grave threats: for example, rogue nations or terrorists obtaining a nuclear weapon and then using it against this country.

The Presidential Decision Directive that has just been issued will be invaluable in our programs against espionage.

The Directive calls for total cooperation against the common enemy—foreign spies. Starting in 1991, the FBI and CIA did develop a high level of cooperation in the Ames case. The Directive will build an effective new structure atop that promising beginning.

It is essential that the counterintelligence programs of the FBI and CIA fully complement each other—and such cooperation is at the heart of the Directive.

Information concerning possible violations of the espionage statute must be provided to the FBI in a timely and appropriate manner.

To achieve this goal, the FBI and CIA have agreed to the assignment of a senior FBI counterintelligence official to lead the CIA's Counterespionage Group.

The FBI is also committed to assigning other FBI counterintelligence specialists to the Group to ensure that both law enforcement and counterintelligence expertise are available to properly coordinate the efforts of the two agencies.

The FBI also has agreed to place CIA personnel in appropriate positions within the National Security Division of the FBI. This exchange of personnel will help develop the working relationships essential for success.

We must have prompt action and obtain positive results. There is no place for a torrent of empty words. Our job is to protect the American people, not to obtain column inches in the press or sound bites on television.

With cooperation and good faith by all, our programs against espionage can be vastly improved.

And there can be nothing less than total cooperation by everyone involved in these important and sensitive matters.

No FBI employee will be allowed to put narrow, bureaucratic goals ahead of the welfare of our country.

If there is anything less than full cooperation in these crucial counterintelligence efforts and in both the spirit and letter of the new Presidential Decision Directive by any agency, and I cannot quickly solve the problem, I make this promise:

I will promptly return to the Senate Select Committee on Intelligence and give you the grim, unvarnished facts.

TESTIMONY OF LOUIS J. FREEH

Director FREEH. Yes, thank you, Mr. Chairman.

With the Committee's permission, I will submit my statement in the consideration of time. Let me just highlight a few things if I may.

First of all, I do want to thank this Committee for its extraordinary support of this entire governmental and institutional review. I think it was not only necessary, but has resulted in very productive changes.

I also want to say that given the notoriety of the difficulties with respect to singular cases, in particular the Ames case, we should not overlook the fact that the vast majority of cases performed on a day-by-day basis by thousands of dedicated men and women in the intelligence services, do not get the recognition other cases get, as noted by our previous witness, and really are the mainstay in the majority of the cases, even in my brief experience.

With respect to the two initiatives here, I do fully support the Counterintelligence and Security Enhancements Act of 1994, as outlined by the Deputy Attorney General. I think they are positive steps, and I think the integration of those proposals and the proposal by this Committee can be accomplished in short order.

With respect to the Presidential Directive signed today, when I testified here in early March, I noted that there were institutional problems between my Bureau and the CIA, focused specifically at that time on the Ames case. There were also indications of other problems. I said during my testimony that the next time I appeared, and in very short order, I was hopeful that the administration would be able to address these problems head on with the support and the impetus of this Committee, and reach some workable and efficient solution.

I believe that we have done that. I am very, very satisfied with the Presidential Directive. I think it gives the agencies, the Government, and the American people, the flexibility, the cooperation, and more importantly, the accountability that's necessary to fix this problem. It is a problem, it needs to be fixed. Neither this Committee nor the American people want to hear about bureaucrats squabbling in Washington, on a case-by-case basis, as to what our mission is, which is to protect the national security.

I think this directive gives us a working solution and it is the best solution that I have seen so far.

Let me outline it very briefly for you. I know you have just received it this morning. However, the Directive does call primarily for the cooperation—total cooperation against the common enemies, foreign spies in particular.

It is essential, obviously, that the counterintelligence programs of the FBI and the CIA be fully integrated and complement each other. They do this now in a variety of ways, overseen, as the activities should be, appropriately, by the NSC, reporting directly to the President.

The structure, as you will see from the Directive, calls for the assignment of a senior FBI counterintelligence official to lead the CIA's counterespionage group. That is the key group, as you know, where the hand-off and the fulcrum of the friction in the past has developed between the two different but important roles of the agencies.

The FBI is also committed to assigning other FBI counterintelligence specialists to the group to ensure that both law enforcement and counterintelligence expertise are available to properly coordinate the efforts of the two agencies.

The Directive calls for the creation of the National Counterintelligence Policy Board, a much smaller group than the current NAG–CI. Having presided over that group of 21 people, I can tell you that there is a better way to run a railroad. I think this does it. The reporting goes directly to the President's Assistant for National Security and to the President. There is a rotating chairmanship of that policy board, which holds directly responsible the National Counterintelligence Operations Board, again, fully represented in a concise and I think efficient way, both the CIA interests, the Department of Defense, the FBI, of course the Departments of State, NSA, as well as the military components.

On the Counterintelligence Center changes, as you can see, we have basically bifurcated the current Counterintelligence Center, giving to the CI the appropriate and more traditional aspects of counterintelligence missions and particularly the coordination and the initiation of activities overseas.

On the National Counterintelligence Center—that's the new Agency component, which again, is represented by the principal parties, but not overrepresented, by all of the community interests. We have a rotating chairmanship, again between the FBI, the Department of Defense, and the CIA. There is a Deputy Director who will either be an FBI Director, Deputy, or CIA, but the FBI will either hold the Chair or be deputy of that key center. I think that is clearly what has been lacking in the past, as well as underrepresentation in the espionage group, which is critical.

My view is that this Directive will put into place the accountability necessary. There will be a single person both on the policy board and the new National Center, supported by the other subgroups, which the President certainly can call upon for responsibility purposes, as well as this Committee.

I think that with respect to 807, which you asked me to comment on, as I testified earlier, I believe that the 807(B) provision, which is the access provision, is the much more critical aspect with respect to my mission and the FBI's law enforcement mission. The access is, in my view, strengthened and enhanced by the interchangability of the Director and Deputy Director's jobs, particularly the running by the FBI of the counterespionage group.

With respect to the first provision of the statute, my view is that to give the FBI total counterintelligence responsibilities as outlined in that section, would, perhaps, tip the balance too far away from what I think are the most efficient missions of both agencies. For instance, the military counterintelligence services have had a very, very good history, with many, many successes, some in direct tandem with our prosecutions. The Pollard case is an example. To take away those responsibilities and put them in the FBI, in my view, would not be prudent, given the very good success rate of those military agencies and also our ability to work with them cooperatively and effectively.

I think that the Directive, which has articulated responsibilities, will solve the problems as I see them and as I have reviewed them

in the last 7 months as FBI Director. The only promise I can make to this Committee is that if this doesn't work, obviously we'll be back here again. It is not my intent to be back here reporting that this has failed, that is not anybody's intent in the executive branch.

I have worked very, very effectively with Director Woolsey in the past couple of weeks. This Directive was put together in 45 days. It has all the positive aspects that I think we need, and I think it'll work and I think it'll be efficient. This Committee and obviously the President and the Attorney General should hold me and the Director of Central Inteliigence responsible for making it work.

I appreciate your time.

Chairman DECONCINI. Thank you, thank you, Director, very much.

Senator Warner has to depart momentarily to the Armed Services Committee, so I am going to yield to him for the first questions.

Vice Chairman WARNER. I thank you, Mr. Chairman. I just want to ask two questions, and then I will return.

Director Woolsey, the Secretary of the Navy is up, and as you know, I have some impartial interest in those matters.

Director WOOLSEY. I do indeed.

Vice Chairman WARNER. First, Director Woolsey, I commend you on the manner in which you've handled these difficult situations of late, and indeed, Mr. Freeh, I think you've been a valuable and coequal working partner.

I have just been able to go through this new PDD overnight, because it was given to us, briefed yesterday, Madam Attorney General, and therefore we are not up to speed as much as we would like on it. But it seems to me that it was a good, hard effort to try and reconcile a difficult problem.

And it is interesting, there are 10 attempts, beginning with the National Security Act of 1947, down to the CIA MOU that the Chairman referred to, to deal with this problem. So we know it has existed a long time, and men and women of the best of intentions have tried to deal with it, and apparently it still exists.

Vice Chairman WARNER. So my first question to the Attorney General, will you provide the Committee with a copy of the PDD that was signed this morning?

Ms. GORELICK. Absolutely, sir. I think we have it here today.

Vice Chairman WARNER. And I would appreciate and the Chair would likewise, so we can go to work on that.

Not just because Congress has an urge to legislate, but would it not be advisable for this Committee, in consultation with this panel, to consider legislating this very proposal? And I mention that, because how do we have an assurance that the next President might think this is not a good step and try to undo presumably what was done in the best interests of the country with this effort?

Ms. GORELICK. Let me say first, Senator, I think that this proposal does represent the best thinking of the entire community, and we believe that it will indeed work, and we believe that there is no necessity for legislation. There may be some necessity for fine tuning, which is certainly easier with executive branch action than legislation. And if there were a change in another administration,

a different approach, that now being apprised of the way in which it can work this Committee does not like, it's certainly free to act.

The problems with legislating, and I think that the——

Vice Chairman WARNER. Well, let's just consider it—I want to be brief here——

Ms. GORELICK. Yes.

Vice Chairman WARNER. Let's just consider the advisability or the inadvisability of trying to legislate the framework of this proposal, so at least Congress has a grip on it should a successor administration think it needs a different approach. At least we have a voice.

Let me ask also, did you give any consideration to designating a member of the NSC as a part of this counterintelligence board, and possibly that individual becoming the permanent chairman, again, fulfilling some of the concerns I have that there is a clarity of command and control and accountability.

Ms. GORELICK. There is actually clarity, Senator. The entire structure reports into the NSC and the chief of the——

Vice Chairman WARNER. That I know, I followed that, but let's think about——

Ms. GORELICK. And the board, the board itself, if you will, has membership on it by the NSC.

Vice Chairman WARNER. But Congress established, incidentally, a coordinating board for—and if you'd look into this—the low intensity conflict in the fall of 1986. I was a participant in that legislation.

Ms. GORELICK. I am aware of that legislation.

Vice Chairman WARNER. You're aware of it?

Ms. GORELICK. Yes.

Vice Chairman WARNER. And I think that's the first time that Congress legislated in such a manner as to hold the NSC accountable to the Congress in some respects.

Ms. GORELICK. Yes.

Vice Chairman WARNER. Just look at that option, if you would, as we go along in our continuing dialog on this issue.

And lastly, you gave a very detailed report of your thoughts and ideas, and, I felt, a very objective and pragmatic assessment of the pieces of legislation relating to the other issue, that is, the delicacy of this balance of invasion of constitutional rights of individuals and the need to strengthen our security interests.

Where do you think we should go? Tighten it a little bit toward the balance of national security, and can we do that without violating any constitutional rights? In other words, just generalize a bit on that?

Ms. GORELICK. I think that there are steps that we can take that would enhance considerably our ability to protect our national security and not impinge in any measurable way on our civil rights or civil liberties. We have tried to craft a very careful proposal in that regard.

Vice Chairman WARNER. That's the answer that I felt that you would give, and I thank the Chair, and I will be back.

Chairman DECONCINI. Thank you; thank you.

Let me pursue some of the things we discussed here. Particularly, I'll get to section 807, because that seems to be the area, if

there is disagreement or if there is an area for us to work in, I feel confident that we can come up with a solution there and certainly with these other differences, as you have laid out, Ms. Gorelick, on the similarities and areas of cooperation that we can do with the other sections.

Now, the administration's proposal in the President's order, as I understand it, it is somewhat limited, I must say, in that your proposed legislation does not deal at all with the relationship between the FBI and the CIA where counterintelligence matters are concerned, correctly. You leave that to the Presidential order.

Ms. GORELICK. Yes, sir.

Chairman DECONCINI. Yes.

And I want to explore that a little bit with you and with Director Woolsey and Director Freeh.

First of all, this Committee has held two closed hearings where this matter was discussed in some depth, and frankly, it seemed that the relationship between the FBI and the CIA had seriously deteriorated. Now, Mr. Freeh testified before a closed hearing that it is unprecedented, that relationship now, and Mr. Woolsey concurs with that personal relationship and the professional relationship between the two of them and the agencies now.

Director Freeh said that it stemmed back to 1991, I would question whether that had been unprecedented since 1991, but certainly I accept that now they are working very closely.

So let me ask both Mr. Woolsey and Mr. Freeh to comment on precisely what is the problem here. Or let's put it this way: What the problem was prior to the two of you working out a better arrangement?

Let's say there is no problem for our discussion here now. Was there any question that there was a problem before both of you were appointed and confirmed between the FBI and the CIA in counterintelligence?

I'll start with you, Mr. Freeh.

Director FREEH. There is no question in my mind that there was a problem. I think the problem comes down to communication. As I testified previously in the closed hearing, we took the opportunity after the hearing to exchange points of conflict on a particularized basis with respect to individual matters and cases. The FBI prepared its version and the CIA prepared its. I reviewed them both, and it seemed to me that the common denominator to all our problems was that nobody was consulting on a regular, frank basis, with respect to the particular matters.

Chairman DECONCINI. So there is no question in your mind that there was a problem?

Director FREEH. No, no question.

Chairman DECONCINI. And Mr. Woolsey, your answer to that question?

Director WOOLSEY. Agree.

Chairman DECONCINI. OK.

Now, in 1988, because of the lack of communication, from the best I can derive, between the agencies, and because, as you have now testified, there was a problem going back some time, President Reagan actually directed that the two agencies sign a new memo-

randum of understanding to spell out how the two agencies would cooperate.

You both are familiar with that MOU?

Director FREEH. Yes, sir.

Chairman DECONCINI. And you've read it?

Director WOOLSEY. Yes, sir.

Chairman DECONCINI. OK.

It's a classified document. As I indicated, I would like to get it unclassified, and maybe you can help us do that.

Quite clearly, the obligation of the CIA to bring to the FBI counterintelligence cases at the very early stage, that's the understanding, that's the law now that is reiterated in a number of the 10 proposals that have been put out, and it is referenced in some manner with more clarity in the MOU.

Yet, I think it is quite clear from the Ames case, if not other cases that I don't know about, that notwithstanding this MOU, this did not happen. Would you agree that it did not happen? Would you agree that it did not happen in the manner that this MOU intended?

Director FREEH. I would say in a number of articulated instances, it did not happen, and again, my view is that there were failings both on the part of the FBI and the CIA, from what I have read.

Chairman DECONCINI. And Mr. Woolsey, you concur——

Director WOOLSEY. Agree.

Chairman DECONCINI [continuing]. That it did not happen?

So my question is really whether doing anything further by MOU or Executive order is going to solve the problem?

Now, Mr. Freeh, you indicate that it's a different atmosphere, and it's set up a board and a commission and what have you. My question is really how is this new Directive going to work if, in fact, all of these past attempts, well-intended, ordered by the President of the United States, said cooperate, lay no blame on either side here of these two agencies. How can you concur that it is going to work now other than the fact that you and Mr. Woolsey have a tremendous cooperative relationship going now that may be truly unprecedented. How else is it going to work?

Director FREEH. Well, I think it works by putting into place a structure such as that contemplated in the Presidential directive, and then enforcing that and holding the people accountable for its enforcement. It is all well and good that the Director and I have what I believe to be a very strong and efficient working relationship. It is probably just as important that all the deputies and all the employees in both agencies understand that. It seems to me a two part requirement. There has got to be a good faith requirement with respect to the enforcement of any document, whether it be the Constitution of the United States, a statute, a Presidential directive, or an MOU. If that is lacking, history has shown, even with respect to the Constitution of the United States, there is a lack of enforcement.

Beyond the good will, which I think we have now and which I certainly will enhance and contribute to, we have a structure. We have a structure that for the first time, beyond the MOU, integrates the agencies at every critical level where the exchange of in-

formation and the access to information has to be available. I think it does it clinically and I think it does it efficiently. And I think there's enough points of responsibility here, beginning with me, as the head of the FBI, to enforce this mechanism and make it work, and I expect that the Attorney General will do that and I think that's part of the bargain.

Chairman DECONCINI. Do you concur with that, Mr. Woolsey?

Director WOOLSEY. I do, Mr. Chairman. I have a word or two I'd like to add on it, if I might.

Chairman DECONCINI. Please.

Director WOOLSEY. The Presidential Decision Directive essentially does two things. It takes the interagency coordinating and policy and program mechanism which now exists, and reports to me indirectly through the somewhat cumbersome mechanism that Director Freeh described, and has it now streamlined and report to the President through the National Security Advisor. It is not just a general reporting to the NSC as a whole, the NSC being——

Chairman DECONCINI. You mean the President's proposal?

Director WOOLSEY. The President's proposal. The National Counterintelligence Policy Board is hereby established and directed to report to the President through the Assistant to the President for National Security Affairs. That is a recognizable individual; it's not the National Security Council staff in general, and it is not even the National Security Council, which is four individuals with two advisors. It's a recognizable individual.

Chairman DECONCINI. That's a good point.

Director WOOLSEY. Which I think is important.

I think that that reform will make it easier, frankly, for all members of the counterintelligence community, broadly conceived, to participate more fully and effectively in that structure, that policy and program structure than has been the case under the previous Executive order.

Now, the second thing that it does that is of extraordinary importance, and Director Freeh has mentioned this, is that it fosters teamwork both by ordering that the director of the counterespionage group in the CIA's own Counterintelligence Center be headed by an FBI official, a senior FBI official, and it also directs that senior CIA counterintelligence officers will permanently staff appropriate management positions in the FBI's counterintelligence work.

Chairman DECONCINI. Who will do the staffing?

Director WOOLSEY. CIA counterintelligence officers in appropriate management positions in the FBI's counterintelligence work, and the key thing, though, from the point of view of the hand-off that Director Freeh described a minute ago, is that the chief of the center in the CIA that does counterespionage will be permanently staffed, in the words of the directive, by a senior executive from the FBI.

I might share with you, because I think it is very important, what the espionage, the counterespionage group in the CIA's Counterintelligence Center does, because this is, in many ways, as far as I am concerned, right at the heart of what the President has directed. It is the focal point within the CIA for managing research and investigation of all counterintelligence leads. This is where all

leads come, whether they come from our own espionage overseas, or from defectors, or from liaison work with foreign intelligence services, or from technical operations, or from volunteers, all those leads come in most of the time, the lion's share of the time, to the CIA, in one way or another, or to the intelligence community. And they come in, when they come to the CIA, to this Center. Putting an FBI official at the head of this Center puts the FBI official in the position to be in, right at the beginning, in order to ascertain just exactly what the equities are in these very difficult case-by-case decisions in which Director Freeh and I ultimately have to decide and most of the time our staffs decide——

Chairman DECONCINI. Let me interrupt you.

Director WOOLSEY [continuing]. How to manage these cases.

Chairman DECONCINI. Because this goes to my problem with this. First of all—and I'll ask both of you to respond to this in a moment—but going to this Center that you point out and what do you do now in a Center is paramount here. Is the senior FBI official going to be in a position to know every security problem that comes to the Center. The answer is yes, correct?

Director WOOLSEY. Yes.

Chairman DECONCINI. Now, will he also know problems, security problems that come to the Operations Directorate, whether or not they come to the Center or not? And that, to me, is the reason that this author came up with what we did in 807—is how do we get the operations in the CIA, when there are problems, as factual or not, and just as a hypothetical, the Post pointed out that Mr. Ames' supervisor supposedly said, and let's say he didn't, but let's just use a hypothetical, that a supervisor of one of the people in counterintelligence or in their Operations Directorate made a statement to a superior that pointed out that everywhere Ames had been, there'd been trouble. Now not necessarily that that was in the Operations Directorate, would that come to this Center, or would it go to the FBI.

Director WOOLSEY. I—we'll have to go into the details of this, I think, probably, Mr. Chairman, in Executive Session, but the short answer is that I can't conceive, in this structure, of a substantive issue being raised about counterespionage, whether it's from the polygraph of a CIA employee, a foreign intelligence agent's report about what may be known in some foreign country that could have come from a leak in our own Government, or any other source that's not going to come as soon as it appears to have any counterespionage implications. I can't conceive of any lead like that that does not come to the counterespionage group.

Chairman DECONCINI. Well, do you think in the Ames case it came there early enough, now that you know what you know?

Director WOOLSEY. The answer is that when the initial leads of any kind came in in the Ames case, far antedated both Director Freeh's and my service in these positions and I won't be able to give you an answer on exactly what was done right and what was done wrong there, until we finish our Inspector General's reports some months in the future.

Chairman DECONCINI. Mr. Woolsey, that is the problem I have with this whole exercise. It seems very clear that there was a problem—you both said there was a problem—and we just may have a

disagreement, that this Executive order setting up this National Counterintelligence Board that has an operation, as the FBI Director over the CIA counterintelligence department, is going to bring out from the operations within the CIA, these problems. It is so clear to me that that is where the problem lies, that anybody who wants to do a good job and wants to follow the 1988 MOU and not be in violation of it, once they have received an allegation—whether they did it or not on the Ames case I'll question—but once they've got an allegation, they're going to consult with the FBI. It appears maybe they didn't in the Ames case, and maybe they did.

But what do we do to get that early information residing in the CIA over to be considered by the FBI. And I just don't know that this does it or if there is a way to do it.

Director WOOLSEY. This is the place where all such leads come within the CIA itself, Mr. Chairman.

Ms. GORELICK. Senator, if I might.

Chairman DECONCINI. Yes, Ms. Gorelick.

Ms. GORELICK. I don't believe that the proposed section 807 would provide any different result. That is, what we have done here is two things. One, we have put—we have created the appropriate level of integration. We have put the FBI in any place that it can meaningfully be in order to detect threats to our national security in the counterintelligence area. And second, we have created accountability to the President and to Congress. Legislating, as the proposed section would, would not change the result that you were positing. That has to be—if the hypothetical that you present is correct, is factually correct, that has to be addressed by sensitizing people within the CIA to go to the Center and to address their concerns. And when they go there they will now find the FBI.

Chairman DECONCINI. Yes, but Ms. Gorelick, let me just pursue 807, because 807 says, in part, section B, the head of each agency within the intelligence community shall ensure. Now, that is a law that directs that they do it, not an Executive order that they are supposed to do it. You know, this is a law—you disobey the law. Shall ensure that the Director of the Federal Bureau of Investigation is provided appropriate access to the employees and the records of the agencies as may be necessary to carry out the authorized counterintelligence or law enforcement investigation. Which to me could go far beyond just the Center where the FBI person is seated now.

And the second question, and you can answer them both, it seems to me, taking the FBI designee, putting him over here, even for a short period of time until he starts rotating, 4 years or something, as the head of this, is exactly what we have had. We have had an FBI person out there. Now he wasn't the head of it, but he was out there. And he testified in closed hearings—it wasn't classified as to what he said because it's been printed in the press—that there were numerous occasions where they couldn't get information. They couldn't get information from the counterintelligence unit. And now this has changed through your Executive order, that they must get it or they will get it because he will be the head of it and supposedly have it. But nothing addresses the problem of operations. And even in analytical areas of the CIA, outside of the

counterintelligence area, of how do you get that problem over to the law enforcement authority.

Ms. GORELICK. There are really two answers to the question.

First, the chief of the Counterintelligence Center Espionage Group, who will be a member of the FBI, is charged with seeking and demanding and achieving access to the information that he or she needs. That's number one. And I think you can direct to Director Freeh the question whether there is a significant difference, as we certainly believe there is, between the status quo and what would be the case with the CIA in charge of the Center.

Number two, the board is charged with coordinating and resolving any conflicts that arise over the implementation of this agreement, the purpose of which is to put the FBI in a position to address all leads, all information, all relevant information, in the counterintelligence area.

So we have not only charged the FBI, within the context of the CIA, to achieve the goal of knowing where the threats are to counterintelligence, but we have put in a method of redundancy in this board to resolve any conflicts.

Chairman DECONCINI. Then you think by that the DeConcini-Warner bill, which gives the overall responsibility for the conduct of counterespionage to ensure that the FBI is brought in on such cases at the earliest time. That's the purpose of 807, obviously. And that it was that the FBI who called the shots if there was a difference of agreement, to be very blunt about it, if they didn't work it out.

Now, is that what you expect to accomplish by the Executive order, that, in fact, if there is a problem and the FBI doesn't like or doesn't feel they can get what they want, can they call the shots?

Ms. GORELICK. They can certainly raise the issue to the highest level. The board will call the shots. It will be represented on the board. We will be represented on the board. Senator, I think you can fairly say you are the father or the co-father of this proposal. This is very much a proposal in the image of the DeConcini-Warner proposal.

Chairman DECONCINI. Well, as I said, Ms. Gorelick, I compliment the administration for addressing it, and my quarrel with it is that to me, as Senator Warner pointed out in the Goldwater-Nichols legislation, and Senator Cohen made some reference to it, the administration opposed that.

When we wanted to put an inspector general in the CIA a few years ago, Senator Cohen's bill, the administration opposed it. And they made these same arguments: You don't need it; we can handle it; we work together. And yet time and time again, it hasn't worked out. And I am only hopeful the administration would help construct some, even if it's loose, legislative fix, because it is so clear that the past MOU's, Executive orders, haven't worked. And what makes us think we can make this one work consistently is beyond me. Although the idea of a counterintelligence board is not offensive—I think it's a good idea—because I think you need to create some order of appeal by the CIA, if, in fact, the FBI did have responsibility that they decided we had to know this source, and that the CIA said, boy, that's dangerous, somebody has to appeal it.

But it troubles me that the resistance to do this legislatively and why it is so much, except the profoundness that seems to exist in administrations in the executive branch of Government. Don't legislate; let us tinker with it because we're better at it. And I think it is clear that that has't worked.

Ms. GORELICK. But let me try to address it if I can.

First, in order to be effective, we believe that rather than painting with a broad brush, laying responsibility on the heads of the FBI and the CIA, it is important to get down to the level of detail that really can make a plan effective. One of the reasons that the MOU was flawed was that it operated at a hortatory level. This is, if you will, down and dirty. It is very clear what the responsibilities are fairly deep into the organization. And we think that is the right way to operate.

Now, let me contrast it to Goldwater-Nichols, because that is a bill that I lived under at the Department of Defense, that is a structure that I respect enormously and that I think made a great contribution. That legislation created a chain of command within the Defense Department structure. Notably, for example, it did not merge the Army, Navy, and the Air Force.

And I suggest to you that you might take a lesson from that book by basically putting responsibility here where it should be, with the President, with the National Security Advisor——

Chairman DECONCINI. I thought it was done legislatively.

Ms. GORELICK [continuing]. And with—well, they are responsible under this program for accountability for the working relationship between the two.

It is important to note in this regard that much in the way of counterintelligence is gathered by the people who are gathering intelligence. And if you legislate too far in the area of merging the two agencies' roles, there are dangers both to the intelligence role and to the prosecutive and investigative role. We think we have the right measure here and we hope you will work with us on it.

Chairman DECONCINI. Well, I am going to work with you. Whether or not we can work it out, I don't know. It just seems to me by creating a National Intelligence Board which the—if there is anybody in charge here, as I understand it, it is going to be the National Security Advisor. The person.

Ms. GORELICK. Yes.

Chairman DECONCINI. In this case, Anthony Lake or his successor.

Now, he is a pretty busy man. When I have tried to talk to him about problems in the intelligence community, whether it's budgets or other things, he's very busy and I respect that. And I spoke to the President last week—not to drop names—about intelligence matters in Bosnia. And Mr. Lake really was too busy to talk to me. And so was the President for a couple of days. And I understand that. You know, what makes you think without a legislative mandate, the National Security Advisor isn't going to have some staff person take these problems up. It just, to me, isn't realistic.

Let me ask you, Mr. Freeh, my last question. If you will, and I know you will, give me a candid response to why section 807(a), which says "The Director of the Federal Bureau of Investigation shall have overall responsibility for the conduct of counterintel-

ligence and law enforcement investigations involving persons in critical intelligence positions. The Director shall coordinate all investigative activities undertaken with respect to such persons by authorized investigative agencies."

Why couldn't the FBI do that, with its professionalism, and secure the national security at the same time. Is it impossible? If this were passed, the FBI could not guarantee that they could conduct their investigations of counterintelligence and espionage and secure the national interest?

Director FREEH. Leaving the question of resources aside for a moment, I think that we're talking about an experiment. I think the assumption in 807 is that it would work, and God knows, if the Congress of the United States passed that statute, everyone in the executive would seek to implement it.

However, I think you are tampering with a delicate balance which, in my view, at least at this stage, and I would tell you if I believed differently, but I believe at this stage you are pushing the balance too far away from what I think are critical roles played by the Central Intelligence Agency in the counterintelligence field. I think to take the whole responsibility, lock, stock, and barrel, particularly when I think there is a modified and more conservative approach, i.e., the one in the PDD, I think is an experiment, although worthy of a test, is probably not something to be tested, in the absence of trying something which I think is more modified, more conservative, and in my view, more practical.

If I was at the point where I thought otherwise—and I might be there if this PDD didn't work, I'll certainly tell you—but I feel at this point, this is a structure that can work and will work.

Chairman DECONCINI. Well, Mr. Freeh, I respect your judgment, and you, Mr. Woolsey, and Ms. Gorelick. I just wish I had the confidence that you all have. And I fear that this confidence is based on the protectiveness of executive privileges rather than trying to find a real solution to this God-awful situation, and whether or not there are more or not, to me it is a disgrace what has happened, and the American public is losing confidence in our intelligence. There is more and more mail coming to me and questions all the time, how much do we spend—I can't say—is it this much? Well, that's what's been reported in the press. How can you spend that much on intelligence and have this kind of operation. And why doesn't somebody eliminate the CIA, as Senator Moynihan says. I mean, that is a real fear here.

If you think for a moment that this is a passing feeling, that when this Senator is gone next year, that all the Ames case and what have you, it's all going to be back to usual and we're going to go back to this new Executive order and maybe it will work and maybe it won't, and God forbid if it doesn't work, if the National Security Advisor is too busy, or this FBI fellow or gal over there can't get the information and is talked out of raising it up the chain of command, and we are sitting here, or I am sitting out as a non-public official anymore, I am going to be disappointed. I am going to feel like why didn't we do something that would correct this. If the FBI is what I think it is, and I have had quarrels with them on occasion, but if they are what I think it is, I don't see why

they can't be in charge, if there's a problem. If there's no problem, it's going to work out.

And just the fact that it is stated in the law, Judge Freeh, that the FBI would have overall authority—I am not directing this to Mr. Woolsey—but any successor, in my judgment, because he is already doing it, is going to say, by God, this is what they want, we got to give it to them, whether it comes out of the operations department or the analytical department, and isn't even in the counterintelligence department. And I just would like to see some legislation. Even if we have to legislate, as Senator Warner points out, what you want to do here, at least it makes it clear that the people of this country want it done by their lawmakers, they want a change here. They are not looking for just—and I hate to say this—another MOU or Executive order.

Thank you.

Vice Chairman WARNER. Mr. Chairman.

Chairman DECONCINI. I yield to the Vice Chairman.

Vice Chairman WARNER. I would add that you and I understand the battle royal that heats up when we go to the Floor with the annual bill. I think you, Mr. Woolsey, can appreciate, having been an observer of legislative actions here. Believe me, we are getting communication from our colleagues that, you know, the Moynihan approach may well be revisited, not just with one, but with two, and many others. So that's a sort of firestorm that the Chairman and I are headed into. And not that we need to put on the armor of just having some legislation, or something of this nature, but the both of us are struggling to try to be impartial and objective and the Chairman's question to you was well-intended, and I would simply say to the Director, would you like an opportunity to reply to that question, because it seems to me there are some real intangibles connected with the intelligence business that we may not fully appreciate should a law comparable to 807, as now drafted, be implemented.

Director WOOLSEY. Well, I would only say that I agree with what the Deputy Attorney General and the Director of the FBI said. I think 807(a) is really what we're talking about here, would tip the balance very far indeed. Foreign intelligence collection is responsible for the lion's share of the counterintelligence leads. And intelligence collection and counterintelligence collection are not only very closely related, often they are the same thing, the same reports.

So the way 807(a) is worded, it seems to me to move very close to something that I know neither Director Freeh nor the Attorney General nor the President nor I want, which is to effectively get the FBI into the business of foreign counterintelligence collection. It assigns overall responsibility for the conduct of counterintelligence.

And so I agree with both the Deputy Attorney General and the Director of the FBI, that the legislation is not wise.

I certainly——

Vice Chairman WARNER. Well, let me try and recast it in a different way, because you know, we have what we call in the military a little bit of salute and march off here this morning. All the forces were reconciled here with midnight, we've got PD signed this

morning and a nice, coherent policy being enunciated by the three witnesses. But that's the way things work around here. But the Chairman's question is important and I will try and recast it.

If Congress were to enact 807(a) as now drafted, is it your professional judgment, Director Woolsey, that this would be counterproductive to our efforts to gather intelligence?

Director WOOLSEY. It is indeed.

Vice Chairman WARNER. Why?

Director WOOLSEY. Because it would establish an overseas rivalry between the FBI and the CIA that now, on the whole, does not exist, and existed back in the late 1940's and early 1950's. It would take us back to some of the strife of that time.

I think 807(a) is badly drafted and is unwise.

Vice Chairman WARNER. Do you want to follow-up on that?

Chairman DECONCINI. No, no. The only thing is I would ask, Mr. Woolsey, is how can you conclude it would take us back to 1947 or whatever? I mean, that is a totally different era we were talking about historically, with the communist threat, and you know, those are to me just as wild as if I said this is going to fix all espionage. It isn't, if you passed 807. Those kind of statements are just to me the exact posturing that does nothing——

Director WOOLSEY. Well, Mr. Chairman——

Chairman DECONCINI [continuing]. Constructive here to take us back to the days that the FBI was—and we're going to compromise everything.

Director WOOLSEY. Mr. Chairman.

Chairman DECONCINI. That isn't what the FBI would do and you know it is not what the FBI would do. At least you know with Mr. Freeh as the Director of it.

Director WOOLSEY. It is certainly not true what Mr. Freeh would do, but it was a conflict historically——

Chairman DECONCINI. Forty years ago, Mr. Woolsey.

Director WOOLSEY. Well, it was a conflict related to——

Chairman DECONCINI. Good Lord.

Director WOOLSEY [continuing]. Lack of clarity in jurisdictional arrangements which have been clarified rather substantially over the years. We work together overseas with the FBI very well now. And my concern about section 807 is that it would disrupt that overseas cooperation.

Yes, indeed, Senator Warner, I think it is bad legislation.

Vice Chairman WARNER. Let me address several other items which I understand in my absence have not been fully covered.

First, FBI access to tax returns. The bill put in by the Chairman and myself contains a provision giving the FBI access to tax returns in counterintelligence cases, pursuant to a court order issued by the Foreign Intelligence Surveillance Court, the court that issues orders for electronic surveillances.

Why was this not included in the administration bill, Madam Attorney General?

Ms. GORELICK. Senator, I would like to discuss that issue with you in private rather than in public hearing.

Vice Chairman WARNER. All right.

So you would ask for a closed hearing, and the Chairman——

Ms. GORELICK. In the first instance, I think we should meet and discuss it and then you can obviously decide whether that is something you wish to pursue.

Vice Chairman WARNER. All right.

Removal of classified information to unauthorized location. The DeConcini-Warner bill has a provision making it a misdemeanor for persons to remove classified documents to an unauthorized location with the intent to keep them there. The Government would not have to prove that such documents had actually been disclosed without authority to an unauthorized person in order for liability to be established.

Did you consider that provision?

Ms. GORELICK. Yes. And as I think I indicated in my opening, that is an area that I think I would like to further discuss with you. I think that it should work only in tandem with their being uniform executive branch rules that are enforced uniformly, and we have some question about when the criminal sanction is appropriate and when a lesser civil or administrative sanction is appropriate for cases in which there really was not criminal intent, but merely a—a lack of appropriate attention to the rules and regulations governing this material.

Vice Chairman WARNER. As we get further into the Ames case, and presumably in the debriefing learn more about his modus operandi, perhaps we should revisit this provision. Because my inclination is to believe that he did violate a lot of the existing procedures established by the Agency in collecting information which otherwise would not have been given to him in his position.

Would that not be right, Mr. Director?

Director WOOLSEY. Well, we'll know more about that after the debriefing is completed.

Vice Chairman WARNER. Let's turn to economic——

Ms. GORELICK. Senator, if I might just say on that, I have litigated cases in this area, I have written on this area. You will have my acute interest to it.

Vice Chairman WARNER. Fine.

On economic espionage. Judge Freeh, in previous appearances before the Committee has indicated that the administration would benefit from legislation making acts of economic espionage illegal. The distinction here is that such acts involve the theft by foreign governments of information that is not classified, but is proprietary in nature. Supercomputer blueprints and other sensitive technologies fall within this category.

Therefore, Judge, is it true that the FBI is seeing increased efforts by foreign governments to use their intelligence agencies to clandestinely acquire proprietary data belonging to U.S. corporations? Would legislation making such acts illegal be of assistance to the FBI? And why doesn't the administration bill include a provision related to this issue?

Director FREEH. Yes, sir.

We have seen a marked increase in the growth of state-sponsored, foreign service-sponsored economic espionage, which we estimate and the business communities estimate could cost in the nature of billions of dollars a year in technology.

The administration, that is, the Department of Justice, is in the process of drafting a trade secrets act. That's what we believe we need for the unclassified information. Right now, prosecutions are pigeonholed under one of the fraud statutes or sometimes under one of the RICO provisions. But there is no statute that addresses the unadulterated crime.

Vice Chairman WARNER. All right.

So you are advising the Committee that it is now, Madam Attorney General, under consideration by the administration, specifically within your Department, and that the Congress can assume that a legislative proposal will be forthcoming?

Ms. GORELICK. It is under consideration and it may result in a legislative proposal or not, but we will let you know either way.

Vice Chairman WARNER. Last question.

The administration bill requires the President to issue regulations within 180 days providing uniform access to classified information. What specifically does the administration intend to do in this area? Is the administration planning to follow the recommendations of the Joint Security Commission on these issues? Will the Committee have an opportunity to review these regulations before they are issued?

Ms. GORELICK. Yes and yes.

We are reviewing the recommendations of the Joint Security Commission, which as you know only recently issued its report. We are actively considering a set of regulations that would centralize certain principles with regard to personnel security and certainly we will engage in a dialog with this Committee on those.

Chairman DECONCINI. Thank you.

Senator Kerrey.

Senator KERREY of Nebraska. Thank you, Mr. Chairman.

I apologize, I did read the testimony, but I understand from staff that you all basically are singing out of the same hymn book and that you give a ringing endorsement of the administration's proposal.

Let me state what I did for the record in my opening statement which is that I don't want to focus undue attention on the Aldrich Ames case. I see Ames as a loser, a mediocrity, and the question that I have is how could an individual like that have been hired in the first place and how did he manage to maintain his employment status for so long. That is essentially what causes the Committee to recommend legislation to deal with this problem.

But I don't believe that the betrayal either calls into question the essential nature of the CIA, which is still, in my judgment, essential for the protection of the United States, nor does it alter the fact that this work is done by people with great dedication, great patriotism, and in many, many instances, also great bravery.

You've offered testimony saying essentially that we can fix this problem with some legislation, but that what we really need is a new board, a new center, that to bring the FBI in as directly as section 807 proposes would compromise the security of the United States and make it difficult for us in fact to carry out our mission.

I remain skeptical of that. I just openly say to you that I am still predisposed to section 807. It is simpler, it is straightforward. As the Chairman said, it doesn't solve all the problems, but I have

more confidence that that fix will get us to where we want to go than I do in what appears to me as I indicated in an earlier question to Senator Boren, a rather complicated procedure that might soothe some egos, but doesn't necessarily and clearly set forth how it is that we're going to do counterintelligence and how it is that we're going to get rid of individuals who, for financial reasons or other reasons, decide that they are going to participate in espionage against the United States.

It seems to me that there are some things, though, that can be done without the need for legislation. I would like, first of all, to direct a rather simple question in that regard. It seems to me that what, Mr. Woolsey, you are faced with is a task of hiring the best people and then retaining, by motivating, leading, and holding on to the best people, and at the same time, moving out those who are judged to be mediocre, to be not up to the standards, hopefully high standards, of the CIA.

In that regard, I must say I applaud the work of Senator Gorton in the Committee, who offered an up or out amendment that would allow and give you some authority to, in fact, move people out that are mediocre and I think you need that kind of management authority.

I am concerned, first of all, in the area of recruitment. I mean, I listened to all the new procedures that we are going to put in place that will allow us to investigate and do background and all sorts of other things on individuals. All three of you were confirmed by the Senate, and I suspect all three have opinions on what this kind of scrutiny does to your willingness to serve. And I would just ask each of you if you think this kind of scrutiny might, in fact, make it difficult for us to recruit individuals who are going to be asked, at times perhaps, to risk their lives in service to their country.

Director WOOLSEY. Senator Kerrey, I'll start because I have already ordered the preparation of financial disclosure forms to be required for all CIA employees.

I believe that in the area of financial disclosure to the Government, we're not talking about public disclosure here, of course, for most employees, the way we effectively have for those of us who are confirmed by the Senate on many issues—we're talking about disclosure to the Security Office within the CIA. I believe that almost all of our employees, including prospective recruits, will see the importance of that issue to counterintelligence and will be willing to comply. We'll try to make the forms somewhat easier to fill out than some of these Government forms that one has to deal with. And I believe that we will not have a problem with respect to morale, merely because we'll ask each employee on an annual basis to file a relatively straightforward financial disclosure form for the Security Office. I can't speak to the other agencies.

Senator KERREY of Nebraska. Ms. Gorelick, in your—in 804(e) of the administration's proposal, in fact, it says that permission is given to disseminate an employee's financial or travel records to any Federal agency, "if such information is clearly relevant to the authorized responsibility of such agency."

Can you tell me why that provision was put in there and comment as well on, based upon your own experience with confirma-

tion, and we're not talking about going out and recruiting people. I mean, I am quite serious about this.

Ms. GORELICK. I understand.

Senator KERREY of Nebraska. I don't want—I mean, in my judgment, you know, you didn't need—the CIA didn't need any special procedures to be able to tell that Rick Ames was a bad apple. I mean, I am concerned that we not spread a huge net out here in response to this betrayal that might make it difficult to do the most important thing that the Agency has to do, which is to recruit and retain the best and the bravest and the finest that they can possibly get.

Ms. GORELICK. Let me address that question directly.

First of all, our language tracks the language of the Financial Privacy Act.

Second of all, our legislative proposal limits to two instances the circumstances in which we would actually request access to underlying financial and travel records. We would ask for consent up front from employees, but we would only use the consent when an employee is suspected of giving classified information to a foreign power, or when an issue of unexplained affluence is raised in a background investigation.

That is, we would not, on a routine basis, without those two criteria, go and look at and seek access to underlying financial and travel records.

So we are very mindful of the considerations that you raise and that was why I gave the response I did to Senator Warner, that I think that one can measurably improve our ability to protect our national security while remaining quite sensitive to the privacy interests of our employees.

Senator KERREY of Nebraska. Why didn't you include provisions that would provide for penalties for unlawful dissemination of information? As the DeConcini-Warner bill did.

Ms. GORELICK. That I do not know the answer to, and I will have to submit that for the record, Senator.

Senator KERREY of Nebraska. Judge Freeh, can you talk to me a little bit, you know, you are out there recruiting all the time, subject to us giving you enough money to bring on new agents. What, in your judgment, does this do to your recruitment strategies, or do you already—most importantly, do you already have procedures in place aimed to detect this kind of thing.

Director FREEH. We do not have all the procedures in place that we would wish. We will get them to a great extent with this proposal. I don't think it is going to impact adversely on our ability to recruit. Having been through two Senate confirmation hearings myself within 24 months, people, particularly people who are attracted to the FBI or the CIA, or the Department of Justice, have now a reasonable expectation of scrutiny, not just with respect to the threshold requirements, but the ongoing scrutiny, which is something not taken for granted. Once the employee is on board, from the Director on down to the file clerk, that scrutiny is ongoing and intensifies sometimes without any basis, as developed after an investigation.

But that is something which I think honest men and women who want to serve their country expect and I don't believe it will have any adverse impact on recruitment.

Senator KERREY of Nebraska. From what you know of Rick Ames, would he have survived FBI's just sort of visual observations and survived as an agent?

Director FREEH. Once he was on board? I don't know. It would depend on the kind of work he was doing, where he was doing it, and obviously the observations and abilities of the people working with him and his supervisors.

Senator KERREY of Nebraska. Would you dismiss for cause, someone who was a philanderer and an agent?

Director FREEH. Depending on the definitions of philandering. If it violated our policies with respect to employment, yes, absolutely.

Senator KERREY of Nebraska. You have evaluations of agents that include ethical and moral behavior?

Director FREEH. We certainly do. I sent out a new directive to our agents a couple of months ago—we call it the Bright Line Test in the FBI—specifying particular grounds for dismissal, including lying in the context of an internal investigation, disclosures of information, Title III information, grand jury information outside the Department of Justice, and I think those are and should be, all dismissable grounds.

Senator KERREY of Nebraska. You do not need an Act of Congress to implement that policy?

Director FREEH. I don't believe, so, sir; no.

Senator KERREY of Nebraska. And do you carry out that kind of policy for security reasons, esprit de corps reasons, what are the reasons for using those kinds of evaluations?

Director FREEH. We do it primarily for security reasons, but also to maintain the integrity of the FBI.

Senator KERREY of Nebraska. Do you reward agents who take risks?

Director FREEH. Yes, we do.

Senator KERREY of Nebraska. Do you encourage the taking of risks, or do you—I mean, do you explicitly say that we know that we are in a risky business and that we are going to pay attention to and reward people who are out there on the line taking risks?

Director FREEH. That is certainly the message that I have conveyed to the employees and it is the message that I think has been around for a long time. We focused on it recently for a couple of reasons, but that is certainly the message that we want to give.

Senator KERREY of Nebraska. Do you need congressional authority to do that?

Director FREEH. I don't believe so.

Senator KERREY of Nebraska. I don't either think you need congressional authority, and Mr. Woolsey, you and I have had a discussion about this privately and I say again for emphasis, I believe it is the number one problem here. I do see it as a hands-on management problem, a requirement, you know, to make common sense judgments based upon the mission at hand. I heard and saw some nodding of agreement when earlier, Senator Cohen compared the disagreement between the FBI and the CIA to appropriators and authorizers. There's two essential differences between those

two kinds of situations. One is when the appropriators and the authorizers are disagreeing, much less is at stake, typically. Second, they typically occur as well in an environment—in a public environment. We don't cloak secrecy around them and keep them from the public.

And I do think these kinds of comparisons, though I think they are appropriate for doing some kind of analysis, they aren't terribly appropriate for us trying to figure out what our policy ought to be. And I believe very strongly that there is still an element of overreaction here in this legislation and believe that an awful lot that needs to be done can be done with adjustments and a toughening of management practices.

I say, I don't find the provisions of section 807 still to be that difficult. It seems to me that that is a reasonable thing to put in place. It seems to me that if it produces a particular problem 1 year from now or 2 years from now, we can adjust the policy.

I asked Senator Boren about the urgency to act. I think there is an urgency to act in this regard, to try to find out whether or not there is other espionage occurring I think is extremely important for us to do. I don't think that we can trust that current procedures have taken care of the problem. And thus, given what's at stake and from my standpoint what's at stake is the Nation's security, not whether or not the CIA and the FBI get along—frankly, I don't care if you get along, you know. What matters to me is the security of the country. And I tend to favor the legal changes provided under 807. They are simple, they are straightforward, and they respond to the urgent situation. If they create a problem for us down the road, we can adjust fire at that point. It just seems to me that we have got an overwhelming reason to act and that we ought not come up with something, frankly, that looked to me like it was written by Ira Magaziner and not by you all.

Ms. GORELICK. Well, Senator Kerrey, let me try to respond to that in two ways.

First of all, I am concerned that the section 807 proposal is itself an overreaction. I mean, it could and our fear is that it would strip the CIA of responsibility to gather foreign counterintelligence generally. And as Director Woolsey said, our concern is that the same capable people abroad who are gathering intelligence are also gathering counterintelligence.

Director Freeh and his people are not currently equipped to undertake that overlapping responsibility. And it was our view that the appropriate way to address the concerns here are to ensure, in a proposal well thought out by these two gentlemen and by others, that the FBI is on-scene and in a position to undertake authoritatively, responsibility for responding to counterespionage, without creating an overlap of responsibility in counterintelligence gathering abroad. That is the concern and it is a legitimate one and it is not one born of turf but rather one born of an administration looking to deploy its limited resources in the most effective way.

Senator KERREY of Nebraska. I must say though, Ms. Gorelick, if I were to read the summary that I received of what the Board and the Center are supposed to do, if I were to read it aloud, I think it would cause people to be confused as to what it is that is going on. It is hardly a straightforward, simple response to the

problem. And though perhaps I would hold a different view if I had been here to listen to your testimony rather than just reading it, I just alert you that I am not persuaded that the alternative that is being suggested by the administration is preferable to the straightforward response in section 807.

Ms. GORELICK. I think that the problem of timing, where we were not really able to brief fully this Committee because we did not have a signed order until this morning, is one that we have to address and deal with. But I do believe that if we had the opportunity further to speak with you about it and how it would work, and maybe we haven't stated it as artfully and directly as we should have, but——

Senator KERREY of Nebraska. I think it is stated very artfully. That's the problem.

Ms. GORELICK. I meant correctly. And when I say artfully, I don't mean cleverly, I mean in a way that communicates. It is a very straightforward proposal. It is not intended to be a mechanism which is confusing. And I——

Senator KERREY of Nebraska. I think if you compared the two proposals side by side, and asked any objective audience which one is more straightforward, section 807 is more straightforward.

Ms. GORELICK. I would grant that, but I guess it is our collective view that it is too blunt an instrument.

Senator KERREY of Nebraska. Mr. Chairman, I have no other questions.

Chairman DECONCINI. Thank you, Senator.

Vice Chairman WARNER. Mr. Chairman, may I ask that the statement by the Senator, Mr. Slade Gorton of Washington, be included in the record. He was here earlier today.

Chairman DECONCINI. It will so be included in the record at the appropriate point.

[The statement of Senator Gorton follows:]

STATEMENT OF SENATOR SLADE GORTON

Mr. Chairman, I wish to commend you and the Vice Chairman for holding this hearing on a vitally important subject—safeguarding national security interests.

With the continuous hemorrhage of national security information again at the center of our attention, it is safe to say that the system is broke and requires fixing.

During the past 10 years, there have been 51 arrests of individuals for espionage. In addition, I suspect that there is a higher number of cases in which arrests were not made. Forty-five of these individuals were Americans, most of whom volunteered to sell out their country by providing highly-classified information to other governments. There is no pun intended in terming their reprehensible actions as a sellout, for most, as we know, exchanged the security of their country for personal gain.

Studies have shown that there are underlying reasons for this financial gain including job and family frustration. Often, these are the telltale indicators that something is wrong or, that a problem is smoldering. When these indicators are ignored, it suggests to me a breakdown of the system of awareness and of leadership.

Aldrich Ames is not the first CIA officer to commit espionage. In fact, he is the fifth current or former CIA employee to be arrested in the past 10 years.

The history of lack of cooperation or insufficient cooperation between CIA and the FBI on counterintelligence goes back many years. But the problem is not limited to these two agencies. The Defense Department is important in the world of counterintelligence and over the years it has experienced many of the same problems with both agencies. This suggests to me the worst kind of bureaucratic muddling in which each agency is more interested in protecting its own turf than in the Nation's security.

But this kind of problem is easily fixed when top leadership mandates that it be fixed. This was the case when DCI Turner and FBI Director Webster—college class-

mates—mandated cooperation in the late 1970's. But, in the years since, the problem has gotten worse, not better.

Today, counterintelligence strategy and policy is headed by the Director of Central Intelligence. But, the country's counterintelligence policymaking structure has been ad hoc and changing over the years. With a situation of constant flux, questions arise about who is in charge and who is responsible.

I understand that President Clinton has just signed a new Presidential Decision Directive which fixes the policy and coordination structure for counterintelligence. I am most interested in hearing the features of that Directive today for I will introduce today legislation that brings stability and more permanence to our counterintelligence policy structure and to the problem of coordination. At this time, I ask the Chair to include this legislation in a comprehensive legislative package on counterintelligence.

NATIONAL COUNTERINTELLIGENCE REFORM ACT

Features

1. Creates a national policy and program framework to ensure an integrated and coordinated effort to counter espionage against the United States.
2. Establishes a senior policy decision board—the National Counterintelligence Review Board (NCIRB)—to review and approve United States counterintelligence policies and programs. In addition, the Board would serve as the final review authority for the proper and timely disposition of counterintelligence cases.
3. The Board would consist of the Attorney General of the United States who would serve as Chairperson, the Secretary of Defense, the Director of Central Intelligence and the Director of the Federal Bureau of Investigation. The NCIRB would report to the President through the National Security Council.
4. Establishes a National Counterintelligence Program (NCIP) which will be administered by the National Counterintelligence Center (NCC). The NCC shall be responsible for providing a focused and coordinated national program to analyze and counter foreign intelligence efforts against the United States. The NCC would also prepare an integrated National Counterintelligence Threat List for approval by the NCIRB.
5. The NCC will consist of personnel from the Central Intelligence Agency, the Federal Bureau of Investigation and the Department of Defense. The Directorship and the Assistant Directorship of the NCIC would rotate on a periodic basis between the Central Intelligence Agency and the Federal Bureau of Investigation. The NCC would be located within the Department of Justice. It would also provide staffing support to the NCIRB.
6. The jurisdiction of the NCC would include foreign intelligence threats against the United States both domestically and against U.S. installations, personnel, and information abroad.
7. The Director of the NCC is responsible for developing governmentwide foreign counterintelligence policy and for approving the allocation of resources to deal with the foreign intelligence threat.
8. The bill would require individual agencies to continue with their counterintelligence responsibilities to protect agency information, equipment, operations, and personnel.

103D CONGRESS
2D SESSION

S. _____

IN THE SENATE OF THE UNITED STATES

Mr. GORTON introduced the following bill; which was read twice and referred to the Committee on _____

A BILL

To amend the National Security Act of 1947 to provide for improved coordination of national counterintelligence policy, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "National Counterintelligence Reform Act".

SEC. 2. AMENDMENT OF THE NATIONAL SECURITY ACT OF 1947.

The National Security Act of 1947 (50 U.S.C. et seq.) is amended by adding at the end the following new title:

"TITLE VIII—NATIONAL COUNTERINTELLIGENCE PROGRAM

"SEC. 801. DEFINITIONS.

"As used in this title:

"(1) BOARD.—The term 'Board' means the National Counterintelligence Review Board established in section 804.

"(2) CENTER.—The term 'Center' means the National Counterintelligence Center established in section 803.

"(3) COUNTERINTELLIGENCE.—The term 'counterintelligence' means information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments, foreign organizations, or foreign persons, or international terrorist activities.

"SEC. 802. PURPOSE.

"The purpose of this title is to establish a national policy and program framework to ensure an integrated and coordinated effort to counteract espionage against the United States.

"SEC. 803. NATIONAL COUNTERINTELLIGENCE CENTER.

"(a) ESTABLISHMENT.—There is established the National Counterintelligence Center.

"(b) COMPOSITION.—(1) The Center shall be headed by a Director and Deputy Director and shall be comprised of staff from—

"(A) the Central Intelligence Agency;

"(B) the Federal Bureau of Investigation; and

"(C) the Department of Defense.

"(2) The head of each agency described in paragraph (1) shall make available such resources, including, by detail or otherwise, such personnel, as may be necessary to meet the needs of the Center.

"(c) ROTATION OF DIRECTOR AND DEPUTY DIRECTOR.—The Director of Central Intelligence and the Director of the Federal Bureau of Investigation shall enter into an arrangement for the rotation, on a periodic basis, of the Director and Deputy Director positions of the Center between officials of the Central Intelligence Agency and of the Bureau.

"(d) FUNCTIONS.—The Center shall—

"(1) administer a focused and coordinated national program to analyze and counteract foreign intelligence efforts against the United States (which may be known as the 'National Counterintelligence Program');

"(2) develop a government-wide foreign counterintelligence policy under the direction and review

of the National Counterintelligence Review Board and approve the allocation of resources to deal with the foreign intelligence threat;

"(3) prepare and maintain an integrated and coordinated listing by country and subject of counterintelligence threats directed against the United States; and

"(4) provide staff and other support services to the National Counterintelligence Review Board.

"(e) IMPLEMENTATION.—In carrying out the functions described in subsection (d), the Center shall consider foreign intelligence threats against the United States domestically as well as against United States installations, personnel, and information abroad.

"SEC. 804. NATIONAL COUNTERINTELLIGENCE REVIEW BOARD.

"(a) ESTABLISHMENT.—There is established an interagency review board to be known as the National Counterintelligence Review Board. The Board shall report to the President through the National Security Council.

"(b) COMPOSITION.—The Board shall consist of 4 members, as follows:

"(1) The Attorney General, who shall serve as Chair.

"(2) The Secretary of Defense.

"(3) The Director of Central Intelligence.

"(4) The Director of the Federal Bureau of Investigation.

"(c) FUNCTIONS.—The Board shall—

"(1) review and approve United States counterintelligence policies developed and recommended by the Center;

"(2) review and approve United States counterintelligence programs administered by the Center;

"(3) serve as a forum for the resolution of interagency disputes arising from decisions made by the Center with respect to the criminal prosecution, exploitation for intelligence purposes, or other disposition of counterintelligence cases; and

"(4) review and approve the national counterintelligence threat list described in section 803(d)(3).

"SEC. 805. RULE OF CONSTRUCTION.

"Nothing in this title alters or affects the responsibility of any department, agency, or other entity of the United States to continue its counterintelligence activities to protect information, equipment, operations, and personnel.".

Chairman DECONCINI. I want to thank the witnesses for the time that they have given in preparation of the legislation introduced by Senator Warner and I last night on behalf of the administration, and the Presidential Decision. And we will be working with you, and maybe have to have further hearings, Ms. Gorelick, depending on Senator Warner's desire to pursue some of those financial areas.

Thank you for your testimony.

Ms. GORELICK. Thank you.

Director WOOLSEY. Thank you, Mr. Chairman.

Vice Chairman WARNER. May I also join in that, and commend you, Madam Attorney General. We've known each other in your previous position with the Department of Defense. I wish to commend the President and yourself for your appointment as the Deputy Attorney General.

Ms. GORELICK. Thank you, Senator Warner. I look forward to working with you.

Vice Chairman WARNER. Thank you.

Chairman DECONCINI. Thank you.

Thank you for staying so long. I apologize for how long it took.

Ladies and gentlemen, we have another panel and we are not going to be able to do it now. We have discussed, the staff has, with Mr. Kohler, Ms. Martin and Mr. Whipple. We will—we lose the room here shortly after 1 o'clock, so we will not be able to stay in this room. I want to proceed, and I understand that the panel can return at 2:15. We will meet in room 219, right next door. It is a smaller room. We will open it to the public, as this hearing is open, and take those three witnesses at that time.

Thank you.

[Thereupon, at 12:55 p.m., the Committee recessed.]

AFTERNOON SESSION

[2:31 P.M.]

Chairman DECONCINI. The Committee will come to order and continue the hearings from this morning regarding pending legislation.

I want to thank our panelists for waiting to be with us again this afternoon, because we just flat ran out of time, and your testimony is very important.

We have three witnesses today: Mr. Robert Kohler, Vice President and General Manager of TRW Avionics Surveillance Group; and Ms. Kate Martin, Director of the Center for National Security Studies of the American Civil Liberties Union; and Mr. David Whipple, Executive Director for the Association of Former Intelligence Officers, and himself a former intelligence officer.

If you would please summarize your statements, and your full statements will appear in the record, and we will start with you, Mr. Kohler.

Excuse me. I'm sorry, Senator.

Vice Chairman WARNER. Mr. Chairman, if I can join you in welcoming, and I appreciate your willingness to return this afternoon. The Chairman and I did not want to abbreviate in any way your contribution to this very, very important subject being examined by the Committee and eventually the Senate as a whole.

Thank you.

Chairman DECONCINI. Mr. Kohler.

[The prepared statement of Mr. Kohler follows:]

PREPARED STATEMENT OF ROBERT J. KOHLER

Mr. Chairman, I appreciate the opportunity to meet with the Committee to discuss the recently proposed changes to the laws and procedures regarding counterintelligence and security.

My perspectives on these issues have been formed and influenced by considerable professional experience dealing with sensitive, classified intelligence programs in both Government and the private sector. Throughout my career, I have worked in and managed programs under the aegis of countless security compartments, restrictions, rules, and regulations. I joined the Central Intelligence Agency in 1967, and served there for 18 years in a number of positions, including director of the Office of Development and Engineering in the Directorate of Science and Technology. I left Government service in 1985 and am currently an executive vice president of TRW and general manager of TRW's Avionics and Surveillance Group (ASG), responsible for managing a variety of avionics, communications, reconnaissance, and intelligence programs, many of them highly-classified.

My comments are intended to reflect some of the views and concerns of private sector industrial contractors, including the membership of the Security Affairs Support Association, regarding the proposed legislative changes. We in the private sector who perform as contractors for the U.S. Government take security very seriously, first and foremost because effective security is one of the critical underpinnings of our national security, but also because good security is good business. Contractors realize that failure to uphold rigorous standards of security places contracts, jobs, and profits at risk—if you cannot maintain adequate security for classified programs, then one of your competitors most certainly will.

Our concern for security is indirectly reflected in the fact that only four prosecuted espionage cases out of the more than 70 that have come to light since 1975 have involved employees of private sector contractors: Boyce/Lee (TRW, 1977), Harper (SCI Corp., 1981), Bell/Zacharski (Hughes, 1981), and Cavanagh (Northrop, 1984). Successful, competitive contractors treat the security requirements in Government contracts as seriously as cost and performance requirements and in many cases more seriously than do our Government counterparts. Those requirements frequently impose considerable burdens on industry, which adds to the expense of executing Government contracts. But we are willing to submit to those procedures when we believe they will provide the measure of security necessary to safeguard important information and technology.

There are tens of thousands of industrial contractors holding security clearances, almost all of whom would be affected by the changes suggested in the various legislative proposals to strengthen counterintelligence. Since we have such a significant stake in the security system—both in enforcing security standards on Government programs as well as being personally affected by the many reporting requirements—I suggest that the views and concerns of private sector contractors receive careful consideration.

The enormity of the reported damage caused by Aldrich Ames' espionage has shocked us all, and consequently energized the intelligence community and Congress to examine remedies and corrections to our security system. As we consider these changes, however, we should not act in haste. Imprudent measures enacted without an analysis of their costs and impacts run the risk of only complicating an already complex set of security laws, Executive orders, rules, regulations, and procedures. At the very least, I suggest it would be wise to withhold final action on any reform legislation until the Government has had the opportunity to complete at least a preliminary damage assessment of the Ames case. Otherwise, we run the risk of creating solutions that do not address the real vulnerabilities and problems. To echo the carpenter's credo, "measure twice, cut once."

As Congress studies the various legislative proposals, the following questions should be borne in mind: Will the recommended changes help deter someone from committing espionage in the first place? And, if someone is engaged in espionage against the United States, will these changes enable a more expeditious detection and arrest? Quite simply, will these new laws help catch spies? If the answer to those questions is "no," then we should forego the impulse to make changes only to be seen as "doing something" about counterintelligence and security concerns.

The legislative proposals offer a number of measures that would clearly strengthen and improve U.S. counterintelligence capabilities and procedures. Those positive provisions include: Rewards for providing information concerning espionage; clarifying the jurisdiction of U.S. courts to try cases involving espionage outside the United States; imposing new penalties for the unauthorized removal and retention of classified material or documents; requiring forfeiture of collateral profits acquired as a result of violating espionage laws; criminalizing the possession of espionage tools and devices; and denial of annuities or retirement pay to persons convicted of espionage in foreign courts involving U.S. information. These proposals are reasonable additions to the process of CI investigation and prosecution and are worthy of strong support.

There are other aspects of some of the proposed legislation, however, that would appear to require additional clarification and/or modification in order to be effective. For the purposes of this hearing, I will focus my remarks on S. 1948. First, there are significant definitional disparities and omissions. "Critical intelligence information" includes information regarding sensitive human and technical sources and methods as well as cryptographic systems, but it does not include information protected under Department of Defense Special Access Programs, materials protected under the Atomic Energy Act of 1954, diplomatic cables and other sensitive materials produced by the Department of State, or information regarding military capabilities or military contingency and operations plans. From the contractor's perspective, sensitive proprietary information would not be covered either, and in an era of increasing international economic competition, such information is also at risk. Clearly, "intelligence" information is not the only target for foreign espionage; those other categories of information also require effective protection, and they should be incorporated into a new definition of "national security information" for use in the legislation.

There are similar deficiencies caused by limiting the coverage of the legislation to "employees of agencies of the intelligence community." While community employees clearly have access to important secrets, so do employees of other Departments and agencies, who while not members of the intelligence community, routinely use and handle sensitive intelligence products, including materials that could reveal in-

telligence sources and methods. The proposed law would not cover White House staff, State Department employees (outside of the Bureau of Intelligence and Research), Defense Department employees (outside of intelligence components), or intelligence consumers at the Departments of Treasury, Justice, Commerce, Office of the Special Trade Representative, and so forth. Anyone with a security clearance and access to classified information is, hypothetically, a potential counterintelligence problem; the legislation should encompass the entire population that is at risk, and not create a category which will be incomplete, and hence, ineffective in limiting vulnerability to espionage.

Treatment of "contractors," a category I am here to represent, also requires additional clarification. For example, the legislation would require the reporting of various kinds of financial data as well as information about all unofficial travel, and since contractors to agencies of the intelligence community are defined as employees, we would be obligated to file the requisite information. It is not clear, however, whether we would have to report that information to each agency with which we held contracts or only one. This is a significant issue, since in the case of TRW, we hold contracts with almost every agency of the intelligence community, and a requirement to file reports with each agency would cause a veritable flood of paperwork to fall on the Federal Government. In TRW alone, we have 9,800 cleared employees, including 7,200 with access to Sensitive Compartmented Information, many of whom might well be defined as filling "critical intelligence positions" for the purposes of this law. If you consider the large number of companies in the defense and intelligence contracting field multiplied by the total number of employees, the potential for gross reporting "overkill" and consequent waste becomes evident.

There are two areas of S. 1948 that I believe are very problematic. First, the legislation creates a significant new requirement for employees in "critical intelligence positions" to report personal financial data, which I believe is overly intrusive, onerous, vague, and ultimately ineffective in strengthening counterintelligence capabilities. There are easily tens of thousands of people, Government employees and contractors alike, who would be considered to occupy "critical intelligence positions" and required to report "the nature and location of all bank accounts, investment accounts, credit accounts, and assets valued at more than $10,000" not just for themselves, but also for "any immediate member of the family." Setting aside the lack of definition of such vague terms as "credit account," such a reporting requirement would produce an avalanche of financial reports from a minimum of hundreds of thousands of people ("employees" plus family members) that would overwhelm the intelligence community. In an era of diminished resources and reduced personnel, who will handle that data, and how? What training will be provided to the staff handling that data, and how much will it cost? What additional technical support will be required? Absent special training, what competence do security officers in the intelligence community have to process, manage, and review, let alone understand, the financial reporting of this many people? Quite frankly, I have no confidence that the bureaucrats who have spent a career in a security office will have or will be able to acquire the requisite expertise and financial sophistication to understand the full range of financial transactions and compensation packages, especially for private sector officials.

Moreover, the law would require that the employee "advise promptly the Agency of *any changes* which occur with respect to the nature or location of the accounts or assets disclosed" (emphasis added). What constitutes a "change" for the purposes of this section? A cash withdrawal from an ATM machine or a purchase of a block of stock? The requirement for "prompt" reporting (undefined) would mean that not only would agencies be subjected to an initial onslaught of paper, but they would be deluged further by an unrelenting flow of reports of changes in employees' financial status. Again, regarding contractors, it is unclear whether such reports would have to be filed with each agency with which a contract was held. And if past history is any indicator, each agency would design its own reporting form and process, and contractors with multiple Government customers would be stuck with the burden of trying to provide the required information on multiple forms while trying to insure that no innocent mistakes are made in the process.

There are many other unanswered questions about how the financial data would be handled. What if the security person analyzing the data suspected or discovered financial improprieties? Would those suspicions be reported to the Department of Justice? How would this very sensitive financial data be controlled within an agency to prevent abuses of an employee's privacy? Would the data be accessible to the IRS? Other issues or questions would undoubtedly arise, but it is clear from this limited review that the process has not been adequately studied nor thought through..

The requirement that such financial disclosure be filed for 10 years after a person leaves a "critical intelligence position" is particularly onerous, and the burden it imposes will likely discourage qualified and able people from seeking those positions. We are already seeing the effect of excessive conflict-of-interest laws and regulations in discouraging people from entering Government. For example, it is very difficult these days to get anyone from industry to take a senior position with the Defense Department, because they will be unable to return to their chosen field for a significant period of time at the conclusion of their Government service. The absence of those people and their unique expertise is a very real loss for the U.S. Government. Adding one more penalty, and this one for 10 years duration, will only exacerbate the problem of qualified people being unwilling to make unreasonable sacrifices to serve in critical positions.

Referring back to the question posed above, "Will these changes catch spies?" I think the answer regarding the financial disclosure procedures specified in S. 1948 is an unambiguous "no." In the first place, a reasonably smart spy will simply file false financial disclosures and hide his ill-gotten gains. The system will be too inundated to discern the truth. Moreover, security elements in the intelligence community would not only be so swamped with paper and data that the material could not be realistically handled, but their efforts to manage that process would consume scarce resources and personnel that would otherwise be dedicated to more effective counterintelligence and security programs. The net effect would be less, not better, security.

We simply cannot afford to waste increasingly scarce resources on ineffective security measures. The Senate Select Committee on Intelligence itself recently mandated budget reductions in the National Reconnaissance Program and other intelligence programs because of perceived excessive security costs. But S. 1948 would create extraordinary new requirements and impose enormous new costs on both the intelligence community and contractors. I share wholeheartedly one of the key conclusions of the Joint Security Commission, that rather than trying to protect everything, we must engage in prudent risk management and provide appropriate levels of protection to those secrets and capabilities that are most critical to national security. Implementing the reporting requirements in this bill would mean that security officers would be trying to find a very small number of needles (spies) in a haystack that was growing geometrically. Our counterintelligence vulnerabilities will not be resolved by creating blanket reporting requirements that cannot work.

A more reasonable way to address the issue of financial reporting is to include reviews of relevant data as part of the routine background investigation process, both for an employee's initial screening and during any subsequent, update investigations. If a person comes under suspicion of espionage in the interim, then a CI investigation should be launched by the appropriate authorities and access to financial data should be obtained through regular investigative techniques and processes. I think it is also worth noting that there are already a number of existing statutes requiring that financial and other institutions report cash transactions of greater than $10,000, or the transportation of $10,000 in or out of the country, to the Federal Government, not for counterintelligence reasons but to combat money laundering, tax evasion, and other crimes. Insuring that CI investigators have access to that data might be a more effective way to discover the proceeds from espionage than creating a complex new reporting system.

The second problematic area of S. 1948 is section 3, "Disclosure of Consumer Credit Reports for Counterintelligence Purposes." My company manages one of the largest consumer and business credit information and related decision support services in the world, providing credit information on more than 170 million consumers, both in the U.S. and overseas. Consequently, any changes to the Fair Credit Reporting Act (FCRA), such as is proposed in S. 1948, should be considered with utmost care and concern for the privacy and well-being of our customers.

In fact, this is not a new issue for TRW or other credit reporting companies. We have been engaged in long-running discussions regarding access to credit records by the FBI for investigative purposes. The current law, the Fair Credit Reporting Act (Public Law 91–508), requires any investigation for purposes not specified in the law (employment, licensing, and other legitimate business purposes) to obtain a court order to gain access to a consumer's credit records. Those restrictions were legislated as a result of Government (including FBI) abuses of credit files in the 1960's, and the credit reporting industry still strongly supports those limitations. We believe that a "written request" from the Director of the FBI (or his "designee") for access to a consumer's records is unacceptable. Evidence sufficient to precipitate a written request should be adequate to obtain a court order or warrant.

We recognize that credit files may contain information useful to legitimate criminal or counterintelligence investigations. Our seminal concern, however, is that ac-

cess to that information be granted in ways that are fully consistent with the responsibility to protect innocent consumers from inappropriate Government intrusions on their privacy. As an alternative to section 3 of S. 1948, we suggest that the Committee adopt the language in section 123, "Furnishing Consumer Reports to Federal Bureau of Investigation for Counterintelligence Purposes," from H.R. 1015, which recently was voted out of the House Committee on Banking, Finance and Urban Affairs. The language in that bill has the strong support of the credit reporting industry. We believe that proposal will provide the FBI with the appropriate tools it needs for thorough CI and other investigations, while continuing to provide substantial protection for consumers' interests.

Mr. Chairman, as my remarks attest, these proposed legislative reforms to counterintelligence procedures and practices are extraordinarily complex. S. 1948 represents an excellent beginning to addressing some of the long-standing problems and obstacles regarding CI. My comments and recommendations are offered with the intent of building upon the foundation you have started. I would be happy to entertain any questions you and the other members of the Committee may have on my statement.

TESTIMONY OF ROBERT J. KOHLER

Mr. KOHLER. Thank you, Mr. Chairman.

I appreciate the opportunity to meet with the Committee to discuss the recently proposed changes to the laws and procedures regarding counterintelligence and security. As you mentioned, Mr. Chairman, you have the full text of my testimony, and I will try to highlight what I think are some of the important views from an industrial security perspective for purposes of time.

I think, as you know, Mr. Chairman, I spent 18 years in the Central Intelligence Agency where I was the Director of the Office of Development and Engineering in the Directorate of Science and Technology. As you mentioned, I left in 1985, and am currently an Executive Vice President of TRW, and as you noted, Manager of the TRW Avionics and Surveillance Group.

In both jobs I have had a lot to do with security and various modes of classification, rules, regulations, etc., so my comments here today are kind of coming with having had a foot in both camps over my career. But here today I want to represent private sector industrial contractors, including the membership of the Security Affairs Support Association, regarding the proposed legislative changes.

We in the private sector who perform as contractors for the U.S. Government take security very seriously. First and foremost, because effective security is one of the critical underpinnings of our national security, but also because good security is good business. Contractors realize that failure to uphold rigorous standards of security places contracts, jobs, and companies' profits at risk. If you cannot maintain adequate security for classified programs, then somebody, and one of your competitors, most certainly will.

Our concern for security is indirectly reflected in the interesting fact that only four prosecuted espionage cases out of more than 70 that have come to light since 1975 have involved employees of private sector contractors. Successful competitive contractors treat the security requirements in Government contracts as seriously as cost and performance requirements, and in many cases more seriously than do our Government counterparts.

Those requirements frequently impose considerable burdens on industry, which adds to our expense of executing Government contracts. But we are willing to submit to those procedures when we

believe that they will provide the measure of security necessary to safeguard important information and technology.

There are hundreds of thousands of industrial contractors holding security clearances, almost all of whom will be affected by the changes suggested in the various legislative proposals to strengthen counterintelligence. Since we have such a significant stake in the security system, both in enforcing security standards on Government programs as well as being personally affected by the reporting requirements, I suggest to the Committee that the views and concerns of private sector contractors receive careful consideration.

The legislative proposals offer a number of measures that would clearly strengthen and improve U.S. counterintelligence capabilities and procedures. Those positive provisions include rewards for providing information concerning espionage, clarifying the jurisdiction of U.S. courts to try cases involving espionage outside the United States, imposing new penalties for the unauthorized removal and retention of classified material or documents, requiring forfeiture of collateral profits acquired as a result of violating espionage laws, criminalizing the possession of espionage tools and devices, and denial of annuities or retirement pay to persons convicted of espionage in foreign courts involving U.S. information.

These proposals are reasonable additions, from our perspective, to the process of counterintelligence investigation and prosecution and are worthy of support.

There are other aspects of some of the proposed legislation, however that would appear to require additional clarification and/or modification in order to be effective. For the purposes of this conversation, I will focus my remarks on S. 1948. First, there are significant definitional disparities and omissions. "Critical intelligence information," includes information regarding sensitive human and technical sources and methods as well as cryptologic systems, but does not include information protected under Department of Defense Special Access Programs, materials protected under the Atomic Energy Act of 1954, diplomatic cables and other sensitive materials produced by the Department of State, or information regarding military capabilities or military contingency and operations plans.

From the contractor's perspective—and it was interesting to note, this was mentioned in this morning's conversation in hearings—from the contractor's perspective, sensitive proprietary information would not be covered either, and in an era of increasing international economic competition, such information is also at risk.

Treatment of contractors, a category I am here to represent, also requires additional clarification. For example, the legislation requires the reporting of various kinds of financial data as well as information about all unofficial travel. And since contractors to agencies of the intelligence community are defined as employees, we would be obligated to file the requisite information. It is not clear, however, whether we would have to report that information to each agency with which we held contracts or only one.

This is a significant issue, since in the case of my company, TRW, we hold contracts with almost every agency of the intelligence community, and a requirement to file reports with each

agency would cause a veritable flood of paperwork to fall on the Federal Government. In TRW alone, we have 9,800 cleared employees, including 7,200 with SCI accesses, many of whom might well be defined as filling critical intelligence positions for the purposes of this law.

If you consider the large number of companies in the defense and intelligence contracting field, multiplied by the total number of employees, the potential for gross reporting overkill and consequent waste becomes evident.

There are two areas of S. 1948 which I believe are very problematic. First, the legislation creates a significant new requirement for employees in, "critical intelligence positions," to report personal financial data, which I believe is overly intrusive, onerous, vague, and ultimately ineffective in strengthening counterintelligence capabilities. There are easily tens of thousands of people, Government employees and contractors alike, who would be considered to occupy critical intelligence positions, and required to report the nature and location of all bank accounts, investment accounts, credit accounts, and assets valued at more than $10,000, not just for themselves, but also for any immediate member of the family.

Setting aside the lack of definition of such vague terms as credit account, such a reporting requirement would produce an avalanche of financial reports from a minimum of hundreds of thousands of people, employees plus family members, and would overwhelm the intelligence community. In an era of diminished resources and reduced personnel, who will handle the data and how. What training will be provided to staff handling that data, and how much will it cost? What additional technical support will be required? Absent special training, what competence do security officers in the intelligence community have to process, manage, and review, let alone understand, the financial reporting of this many people? Quite frankly, I have no confidence that the bureaucrats who spend a career in the security office will have or be able to acquire the requisite expertise and financial sophistication to understand the full range of financial transactions and compensation packages, especially for private sector officials.

Again, regarding contractors, it is unclear whether such reports have to be filed with each agency with which a contract was held. And if past history is any indicator, each agency will design its own reporting form and process and contractors with multiple Government customers would be stuck with the burden of trying to provide the required information on multiple forms while trying to ensure that no innocent mistakes are made in the process.

There are many other unanswered questions from our perspective about how the financial data would be handled. What if the security person analyzing the data suspected or discovered financial improprieties. Would these suspicions be reported to the Department of Justice? How would this very sensitive financial data be controlled within an agency to prevent abuses of an employees privacy? Will the data be accessible to the IRS? Other issues or questions would undoubtedly arise, but it is clear from this limited review that the process has not been adequately studied nor thought out.

The requirement for such financial disclosure to be filed for 10 years after a person leaves a critical intelligence position is particularly onerous, and the burden it imposes would likely discourage qualified and able people from seeking those positions.

We are already seeing the effect of excessive conflict of interest laws and regulations in discouraging people from entering Government. For example, it is very difficult these days to get anyone from industry to take a senior position in the Department of Defense, because they will be unable to return to their chosen field for a significant period of time at the conclusion of their Government service. The absence of those people and their unique expertise is a very real loss to the U.S. Government. Adding one more penalty, and this one for 10 year's duration, would only exacerbate the problem of qualified people being unwilling to make unreasonable sacrifices to serve in critical positions.

Another problematic area of S. 1948 is section 3, Disclosure of Consumer Credit Reports for Counterintelligence Purposes. My company, TRW, manages one of the largest consumer and business credit information and related decision support system services in the world, providing credit information on more than 170 million consumers, both in the United States and overseas. Consequently, any changes to the Fair Credit Reporting Act, such as proposed in S. 1948, should be considered with utmost care and concern for the privacy and well being of our customers. In fact, this is not a new issue for TRW, or other credit reporting companies.

We have been engaged in long running discussions regarding access to credit reports by the FBI for investigative purposes. The current law, the Fair Credit Reporting Act, Public Law 91–508, requires any investigation for purposes not specified in the law to obtain a court order to gain access to a consumer's credit report. Those restrictions were legislated as a result of Government, including FBI, abuses of credit files in the 1960's, and the credit reporting industry still strongly supports those limitations.

We believe a written request from the Director of the FBI or his designee for access to a consumer's records is unacceptable. Evidence sufficient to precipitate a written request should be adequate to obtain a court order or warrant.

We recognize that credit files may contain information useful to legitimate criminal or counterintelligence investigations. Our primary concern, however, is that access to that information be granted in ways that are fully consistent with the responsibility to protect innocent consumers from inappropriate Government intrusions on their privacy.

As an alternative to section 3 of S. 1948, we suggest that the Committee adopt the language in section 123, "Furnishing Consumer Reports to Federal Bureau of Investigation for Counterintelligence Purposes," from H.R. 1015, which recently was voted out of the House Committee on Banking, Finance and Urban Affairs. The language in that bill has strong support of the credit reporting industry. We believe that proposal will provide the FBI with the appropriate tools needed for a thorough CI and other investigations, while continuing to provide substantial protection for consumer interests.

Mr. Chairman, as my remarks attest, the proposed legislative reforms to counterintelligence procedures and practices are extraordinarily complex. S. 1948 represents an excellent beginning to address some of the long-standing problems and obstacles regarding counterintelligence.

My comments and recommendations are offered with the attempt at building on the foundation you have started.

Thank you very much, Mr. Chairman.

Chairman DECONCINI. Thank you, Mr. Kohler.

Ms. Martin, if you would summarize your statement, your full statement will be put in the record.

[The prepared statement and attachments of Ms. Martin follow:]

PREPARED STATEMENT OF KATE MARTIN

Mr. Chairman and members of the Committee:

Thank you for this opportunity to testify on behalf of the American Civil Liberties Union on counterintelligence legislation in light of the Ames spy case. The ACLU is a non-profit organization of over 275,000 members dedicated to the preservation of individual liberties and constitutional rights.

INTRODUCTION

The arrest of Aldrich Ames has focused attention on the investigative powers and statutory authority of the Federal Government to investigate and prosecute espionage cases. At the same time, some Members of Congress have raised questions about the direction and effectiveness of our counterintelligence and intelligence efforts in light of the end of the cold war. Indeed, these hearings come at a time when all aspects of security and intelligence policies are under review: The administration is preparing a new Executive order governing the standards for classification; and the Secretary of Defense and the Director of Central Intelligence commissioned a comprehensive report on security matters.[1] The ACLU commends these efforts, having called for a comprehensive review and revamping of measures that restricted the civil liberties of Americans in the name of national security during the cold war.[2]

In looking at the issues related to counterintelligence work, we urge the Committee to keep in mind the important differences between law enforcement and collecting intelligence on our adversaries. Counterintelligence is an area where these two objectives may overlap, and therefore an area where it is extremely important to be clear about the objectives of investigations and the means being employed. Means that may legitimately be used to gather intelligence, including counterintelligence about one's adversaries, may not constitutionally be used against Americans or to make a criminal case against an individual.

In this connection, we also urge the Committee to examine very closely efforts by the Central Intelligence Agency to focus on organized crime and narcotics. These are traditionally law enforcement matters, and not matters related to the national defense and the preservation of the existence of the country. We see very serious dangers in any governmental effort to use the procedures and apparatus designed to protect the national defense to address what is essentially a law enforcement problem.

On the issue of how to prevent and pursue espionage cases, the American Civil Liberties Union believes that the counterintelligence activities of the United States can and should be reorganized to deal more effectively with spying while reducing the harm to civil liberties caused by the current system. We do not believe, however, that the answer lies in broadening the investigative powers of the Government at the expense of individual privacy. Indeed, the public record concerning the Ames case strongly suggests that the inability of the Government to identify Ames earlier did not result from any lack of investigative or statutory authority, but rather from a lack of interagency cooperation and a failure to utilize existing investigative authority.

---

[1] "Redefining Security," A Report of the Joint Security Commission to the Secretary of Defense and the Director of Central Intelligence (Feb. 28, 1994) ("JSC Report").

[2] *First Principles*, Vol. 18, No. 1, Feb. 1993, "Recommendations to the Clinton Administration on National Security and Civil Liberties Issues."

Accordingly, the ACLU opposes the enactment of sweeping new powers for the intelligence and law enforcement communities as a reflexive response to what appears to be a case of mismanagement and poor use of resources. Some of the pending legislative proposals have not been crafted in response to any study of the failures in the Ames case, but have long been sought by the law enforcement community. Congress has rejected them in the past; they have little to do with increasing counterintelligence effectiveness, but do diminish the civil liberties of Americans.

CURRENT PROPOSALS

There are four proposed bills in response to the Ames case: The administration proposal; S. 1869, attached to the competitiveness bill (S. 4), and H.R. 4137, the companion bill in the House introduced by Congressman Henry Hyde; and S. 1948, introduced by Senators Dennis DeConcini and John Warner. While some of the provisions overlap, the administration proposal is overall the most measured and appropriate response, although it also contains some troublesome provisions.

S. 1869 was introduced by Senators William Cohen and David Boren just days after the Ames case broke. It is almost identical to legislation introduced in 1990 based on the recommendations of the Jacobs Panel to the Senate Select Committee on Intelligence, and is extremely flawed in a number of respects.[3] The Senate summarily attached S. 1869 to the competitiveness bill (S. 4) last March without any debate or consideration, and we urge the Committee to seek its withdrawal in conference.

In 1990, we testified before the Senate Intelligence Committee on the findings and recommendations of the Jacobs Panel. Although the ACLU found much to commend in the Panel's study, we opposed the bill embodying its recommendations because many of them unduly restricted civil liberties. We oppose S. 1869 and H.R. 4137 for the same reasons.

We will be submitting to the Committee a comprehensive section-by-section analysis of that legislation as well as the administration bill and S. 1948. Following is an outline of some of our concerns.

ADMINISTRATION PROPOSAL

1. *Access to classified information* (secs. 801–803). We are concerned about this part of the administration's provision and do not understand what purpose it is intended to serve. It provides that the President shall issue a regulation governing access to classified information and that no person shall be given access, unless a determination is made after a background investigation. As the Committee is well aware, this is the procedure that is currently followed, in which the executive branch prescribes regulations governing access to classified information. While we believe that the current security clearance system needs to be overhauled, this provision would appear to give the administration a blank check in advance to make changes and then essentially codify those changes, without Congress having any input into the substantive process.

We believe the Committee should encourage the President to consult with the Congress and interested members of the public in drafting new regulations concerning access to classified information. Only after such executive branch proposals have been prepared should the Congress consider legislative approval.

We note that this provision also raises separation of powers concerns by applying to persons not just in the executive branch, but also to persons in the judicial and legislative branches, such as law clerks and staff members.

2. *Requests by authorized investigative agencies* (sec. 804). This section would provide that investigative agencies could obtain the personal financial and travel records of persons with access to classified information who were required to provide consent to such access. By and large, we commend the administration for its restrained and reasonable approach in crafting this provision. We believe that security investigations should focus on financial matters, rather than ideological ones as happened in the past, and this provision is an attempt to do so. We also believe that such intrusive techniques as are authorized here should be limited to circumstances where there is some basis to suspect the individual of wrong-doing, and that concept is also contained in the administration proposal.

[3] *See* Hearings before the Senate Select Committee on Intelligence on S. 2726 to Improve U.S. Counterintelligence Measures, 101st Cong. 2d Sess., S. Hrg. 101–1293 (May 23, and July 12, 1990) ("Jacobs Panel Hearings"). In the following Congress the Jacobs Panel bill was revised and reintroduced as S. 394, 102d Cong., 1st Sess. The Cohen and Hyde bills are based on S. 394.

However, we remain concerned about two matters: First, the lack of notice given to the affected individual that his private records have been searched by the Government. If such requests are made in the course of background investigations or reinvestigations, the individual should be given notice of any requests made under this section. Notice of such requests should be waived only in cases where there is an authorized counterintelligence or law enforcement investigation of a current employee, based on suspicion of the employee passing information to a foreign power.

Similarly, the provisions of this section should be limited to employees or others who currently have access to classified information. It is overly intrusive to require Government employees to waive their privacy rights even after they have left the Government. In addition, once someone has left the Government, there is no need to carve out special exceptions to standard law enforcement requirements of subpoenas or search warrants for obtaining private information about individuals.

3. *Disclosure of consumer credit reports for counterintelligence purposes* (sec. 3). We oppose this provision, which would expand the use of the national security letter exemption to cover credit reports. This proposal, which would expand the FBI's authority to investigate non-Government employees, was not crafted in response to the Ames case, but has been sought by the FBI for the past 4 years. There is no reason why Congress should now enact it. Any legitimate law enforcement need to obtain this information can be satisfied without this legislation either by obtaining a waiver from Government employees or by obtaining a search warrant or subpoena for non-Government employees.[4]

S. 1948 (DeCONCINI AND WARNER BILL)[5]

1. *FBI access to tax returns for counterintelligence purposes* (sec. 4). We oppose this provision, which would expand the Foreign Intelligence Surveillance Act (FISA) to tax records. The FISA is a carefully constructed and balanced statute designed for the unique circumstances of electronic surveillance for foreign intelligence purposes. Under no circumstances should it be applied to physical searches. As with credit records, this information can be obtained from employees through a waiver requirement or from others by a subpoena or warrant.[6]

2. *Criminal offense for unauthorized removal of classified documents* (sec. 7). We are very concerned about section 7 of the DeConcini bill, which would create a new criminal offense for the unauthorized removal of classified documents.[7] This provision could have the unprecedented effect of criminalizing whistleblowing and the provision of Government information to the press. At the Jacobs Panel hearing, Senator Metzenbaum raised the point that this provision could be used to prosecute a Government employee who sought to bring a classified document to Congress to expose unlawful activities, misuse of funds, abuse of authority, or significant dangers to public health. It could also be used against persons who give copies of classified documents to the press—even if they do not retain copies themselves on the grounds that they know the press is going to retain copies "at an unauthorized location." The Jacobs Panel which originally recommended such a provision indicated that they did not intend this result.[8]

We understand that this provision is aimed at Government employees who routinely remove classified information for personal reasons. We do not think that criminal penalties are the appropriate remedy for this problem. Such employees should be subject to administrative discipline, including loss of clearance and job. Employees should only be subject to criminal prosecution if they intend to sell the information to a foreign power. The proposed provision would come dangerously close to operating as an Official Secrets Act.

---

[4] The same provision appears in section 3 of S. 1948, and section 11 of S. 1869 and H.R. 4137.

[5] Section 2 of this bill concerns access to intelligence community employee records that is similar to section 2 of the administration bill; we generally support this approach, but have certain concerns regarding notice to the employees. *See* the section-by-section in the accompanying appendix. Section 3 of this bill is the virtually the same as the administration proposal on credit records, and we oppose it for the same reason.

[6] Section 13 of the Cohen and Hyde bills provides for a much broader expansion of the FISA to cover all national security physical searches. As explained in more detail in the appendix, we strongly oppose this provision.

[7] A similar provision appears as section 7 of the Cohen and Hyde bills. We note that the Cohen and Hyde bill would apply only to information classified at the level of top secret, while the DeConcini bill would apply to any classified information.

[8] Jacobs Panel Hearing, at 107–9.

SECRET SEARCHES

Finally, we would like to comment on the issue of warrantless physical searches for national security reasons, so called secret searches. We were extremely disturbed to learn that the U.S. Government in the Ames case searched the private home of a U.S. citizen without obtaining a warrant under the fourth amendment.[9] Furthermore, it apparently did so, in the course of pursuing a criminal investigation, aimed at using the fruits of this illegal search in a criminal prosecution. No matter the nature of the crime, there is no "national security" exception to the fourth amendment to justify this violation of one of the most fundamental liberties guaranteed by the Constitution: The right to be secure in one's home from unreasonable searches and seizures.

The Supreme Court has stated that "physical entry of the home is the chief evil against which the wording of the Fourth Amendment is directed." *United States* v. *United States District Court [Keith]*, 407 U.S. 297, 313 (1972).[10] Nonetheless, the executive branch claims the authority to conduct secret warrantless searches of Americans' homes in the name of national security.[11] We are appalled that instead of calling for the repeal of this Executive order, or at the very least, initiating a public discussion of the propriety of such searches after the end of the cold war, Attorney General Reno instead apparently simply ordered such a search in the Ames case. While the plea bargain in the Ames case has forestalled the judicial testing of this fundamental constitutional violation, this Committee should raise the matter with the administration.

There simply is no reason to deviate from the standard fourth amendment procedures, as articulated in the Federal Rules of Criminal Procedure (Rule 41). The concerns raised about espionage and intelligence investigations apply no less to other large scale investigations involving organized crime, money laundering, or international narcotics offenses. Accordingly, this Committee should resist any calls for special warrant procedures for national security physical searches, and should call on the executive branch to cease and desist all such searches of U.S. persons.[12]

REFORM OF THE CLASSIFICATION SYSTEM

Finally, we note that an important component of any counterintelligence reform is significant reform of the classification system. As the Joint Security Commission noted, "classification management is the 'operating system' of the security world. Classification drives the way much of security policies are implemented and security practices are carried out."[13] As Senator Howard Metzenbaum testified in response to the Jacobs Panel proposal:

> Once the material to be protected is limited to that which truly merits protection, far fewer people will need access to that material. There will be more respect, moreover, for the need to protect the information. There will also be more justification for the inconveniences and invasions of privacy that we are asked to impose upon people with access to these secrets.[14]

We heartily concur. We believe that drastically limiting the amount of classified information, and the number of people who have access to it will greatly facilitate the protection of the truly sensitive information that needs protection and will do so in a way that minimizes constitutional infringements. The administration's most recent draft of a new Executive order, dated March 17, 1994, contains several important provisions, which if finally adopted would represent dramatic progress in

---

[9] *See* Affidavit of Leslie G. Wiser, Jr., in Support of Warrants for Arrest and Search and Seizure Warrants, para. 26.

[10] *See also Payton* v. *New York*, 445 U.S. 573, 588–90 (1980) ("The fourth amendment protects the individual's privacy in a variety of settings. In none is the zone of privacy more clearly defined than when bounded by the unambiguous physical dimensions of an individual's home—a zone that finds its roots in clear and specific constitutional terms: 'The right of the people to be secure in their . . . houses . . . shall not be violated.' That language unequivocally establishes the proposition that '[a]t the very core [of the fourth amendment] stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.'" (quoting *Silverman* v. *United States*, 365 U.S. 505, 511 (1961)).

[11] *See* Executive Order 12333, section 2.4(c).

[12] The Cohen and Hyde bills provide for statutory authorization for secret physical searches by expanding the procedures established in the Foreign Intelligence Surveillance Act (FISA). We oppose this proposal because the FISA does not meet the full requirements of the fourth amendment with respect to physical searches. *See* accompanying appendix for a detailed analysis of this proposal.

[13] JSC Report at 11.

[14] Jacobs Panel Hearing, at 94.

this area. The Congress should encourage such adoption and then codify these standards in legislation.

CONCLUSION

The Ames case has brought significant public attention to the Government's counterintelligence practices and procedures. It is wholly appropriate for Congress and the executive branch to take the time to review them and to consider necessary reforms that improve counterintelligence at its core without threatening fundamental civil liberties. We think that much of the proposed legislation was hastily conceived, addresses issues outside of the problems raised in the Ames case, and raises significant civil liberties concerns. We urge the Committee to refrain from enacting such sweeping legislation. We are, however, prepared to work closely with the Committee on narrow legislation to provide greater access to records of employees with access to highly-classified information.

APPENDIX

ACLU TESTIMONY ON 1994 COUNTERINTELLIGENCE LEGISLATION

ANALYSIS OF 1994 COUNTERINTELLIGENCE LEGISLATION: ADMINISTRATION BILL; S. 1948; S. 1869; S. 1866; AND H.R. 4137

ADMINISTRATION BILL AND S. 1948 (DeCONCINI-WARNER BILL): THE COUNTERINTELLIGENCE AND SECURITY ENHANCEMENTS ACT OF 1994

Because the administration bill is similar to the DeConcini-Warner bill (S. 1948), we will analyze the two together. The DeConcini-Warner bill contains two provisions that are not in the administration bill, and four that are virtually identical; the administration bill contains one provision that is not in the DeConcini-Warner bill, but is identical to a provision in S. 1869 (Cohen-Boren bill) and H.R. 4137 (Hyde bill).[1]

I. Requirements for Employees with Access to Classified Information: Administration, Sec. 2; DeConcini-Warner, Sec. 2.

A. ADMINISTRATION BILL, "SECS. 802–03": "ACCESS TO CLASSIFIED INFORMATION"

This portion of the administration bill requires the President to issue regulations governing access to classified information, and mandates that "no persons shall be given access to classified information . . . unless, based upon an appropriate background investigation, such access is determined to be clearly consistent with the interests of national security."

This provision appears to codify the current system, which leaves to the President unbounded authorization over security clearance determinations for all persons seeking access to classified information (this provision, however, would also explicitly include staff in the legislative and judicial branches). It would deny Congress any substantive input into the standards and procedures for granting and adjudicating security clearances. We believe that Congress should not provide such sweeping statutory authorization without including fundamental due process protections to persons whose clearances are denied or revoked.

The administration bill fails to address Congress's 1993 call upon the Defense Department "to conduct a review of the procedural safeguards available to Department of Defense civilian employees," in light of the greater safeguards available to DOD contractor employees.[2] Indeed, the Defense Department and the DOD/CIA Joint Security Commission have both acknowledged deficiencies in the due process rights available to Government employees, particularly in cases involving special compartmented information and Special Access Programs, and have made recommendations

---

[1] The Cohen and Hyde bills are based on legislation originally introduced in 1990 (S. 2726) in response to the report of the Jacobs Panel report to the Senate Intelligence Committee. See Hearings before the Senate Select Committee on Intelligence on S. 2726 to Improve U.S. Counterintelligence Measures, S. Hrg. 101–1293, 101st Cong., 2d Sess. (May 23 & July 12, 1990). A modified version of S. 2726 was reintroduced in the next Congress as S. 394, 102d Cong., 1st Sess.

[2] Defense Authorization Act of 1994, P.L. 103–160, sec. 1183, 107 Stat. 1774.

for reform. Their responses, however, have failed to provide the full due process protections established for contractor employees.[3]

Because these due process rights are so important and are so vulnerable, the ACLU believes that Congress must legislate standards affirming the right to basic due process in security clearance cases for all employees. Congress should refrain from legislating a blanket authorization of security clearances that does not provide such protection. Accordingly, we recommend that sections 802 and 803 be dropped from the administration bill.

B. ACCESS TO EMPLOYEE RECORDS: ADMINISTRATION BILL, "SEC. 804"; DeCONCINI-WARNER, "SECS. 802–804"

These sections of the administration and DeConcini-Warner bills focuses appropriately on conditioning employees' (both Government and contractor) access to classified information on the Government's access to financial and travel information, by requiring the employee to waive their privacy right in the information. The DeConcini-Warner bill would apply only to persons employed in the agencies of the intelligence community. The administration bill would require waivers by all persons with access to classified information. Similar provisions in the Cohen-Boren and Hyde bills would apply only to persons with access to top secret information.[4]

These provisions require covered employees to provide access (upon the request of an investigative agency) to their financial records, other financial information, consumer reports, and travel records; the DeConcini-Warner bill would also include tax records.[5] The waiver requirement in the DeConcini-Warner bill would only apply for the length of the individual's employment with such an agency. The administration's waiver requirement would extend until 5 years after such employment. The DeConcini-Warner bill imposes additional requirements on persons holding "critical intelligence positions," involving direct access to human sources, technical collection systems, and crpytographic systems. They would have to affirmatively provide all financial accounts of themselves and their immediate family members and notice of all foreign travel.

The ACLU does not oppose the general approach of requiring such a waiver from Government employees who seek access to highly-classified information, although we do have specific concerns about each of the provisions. We think it addresses the espionage problem posed by the Ames and other cases in a reasonably narrow and focused manner. The most damaging cases come from persons who have access to the most sensitive information. It is not unreasonable to require those persons, as a condition of access to such information, to make available personal information that bears a close nexus to the factors that can indicate the possibility of espionage, namely financial and travel information. Such provisions recognize, by exclusion, that political, social, and other types of "lifestyle" information are not useful indicators of espionage.

Whichever provision is used as a model for legislation, it should include the following basic restrictions:

(1) waivers should at most be required only of persons with secret and top secret clearances (it should not be required at the confidential level); if possible, it should be limited even further to Special Access Programs and Sensitive Compartmented Information;

(2) it should only apply for the time the person has access to classified information; upon termination of employment or revocation of a clearance, the waiver should no longer apply;

(3) prior notice should be given each time access is sought, unless there is reasonable suspicion, based on clear and articulable facts, that the person is, or may be, disclosing classified information in an unauthorized manner to a foreign power or an agent of a foreign power; notice should be given

---

[3] Report of the Joint Security Commission on Redefining Security to the Secretary of Defense and the Director of Central Intelligence, Feb. 28, 1994, at 48–61; Department of Defense, "Security Clearance Denial and Revocation Procedures for Department of Defense Civilian Employees: A Report to Congress" (Mar. 1994).

[4] *See* below, section IX. So long as the circumstances under which the authority in the administration bill can be used remain limited as established in the draft, we do not oppose applying this requirement on persons with access to information classified at secret and above. We do not think it necessary to apply to persons with access to Confidential information.

[5] When asked by both the Senate and House Intelligence Committees why the administration bill does not include tax records, Deputy Attorney General Jamie Gorelick responded that she could only answer in closed session. We do not understand why the administration cannot answer this question in public, and urge the Committees to make any such explanation public so that the public has an opportunity to respond to the administration's assertions on this issue.

in cases of unexplained affluence or excessive indebtedness in the course of a background investigation or reinvestigation;

(4) the information obtained should only be used for specific counterintelligence purposes, and should not be disseminated for any other purpose;

(5) the waiver shall only apply to the employee; it cannot reasonably be applied to personal finances of spouses.

The DeConcini-Warner bill, for example, fails to require that the requesting agency provide notice to the individual each time access is sought, except where there is evidence of a security violation.[6] Such notice is necessary to allow persons an opportunity to clarify any ambiguities or possibly suspicious looking transactions before a more intrusive investigation is launched.

In addition, the DeConcini-Warner provision allows agencies to seek access in the course of any authorized counterintelligence or security inquiry. Section 804(a)(2)(B) of the administration bill, on the other hand, imposes much stricter limitations on such requests: i.e., only in situations where there is evidence that the employee may have disclosed classified information to a foreign power or its agent, or where, in the course of a background investigation or reinvestigation, there is "unexplained" affluence or excessive indebtedness. However, we think that the standard in the administration bill should be stronger: Rather than be based on "information or allegations indicating that the person is, or may be, disclosing classified information . . .," the standard should be when "such agency has reasonable grounds to believe, based upon specific and articulable facts available to it, that the person is, or may be, disclosing classified information . . ."[7]

DeConcini-Warner appropriately limits the waiver only to the period of Government employment; although, the additional requirements for persons in "Critical Intelligence" positions would apply for 10 years after leaving such a position, but only so long as they remained employed by the Government. The administration bill, on the other hand, would extend the waiver for 5 years after such employment. We believe that the waiver requirements should only apply during the period that the person has access to classified information requiring such a waiver. Once a person no longer has such access, the Government should be required to follow investigative procedures used in any law enforcement investigation. The conditions imposed upon employees for seeking access to classified information should not remain after such access is terminated.

The administration bill fails to minimize dissemination of the collected data (section 806(e)). Unlike the DeConcini-Warner bill, which allows dissemination of requested information by the investigative agency only to the employing agency and to the Department of Justice for law enforcement or counterintelligence purposes, the administration bill would also allow dissemination to any other agency "if such information is clearly relevant to the authorized responsibilities of such agency." We think that this last clause is too broad and therefore should be eliminated. The standards in the DeConcini-Warner bill on dissemination, including the civil damages remedy for unlawful dissemination (section 806(f)), are appropriate and should be used in the administration bill.

II. Disclosure of Consumer Credit Reports for Counterintelligence Purposes: Administration, Sec. 3; DeConcini-Warner, Sec. 3.

This provision appears in both the administration and the DeConcini-Warner bill in substantially similar form; a different version was included in the original Jacobs Panel bill and is also included in the Cohen-Boren and Hyde bills. The FBI has long sought this authority, and Congress has refused to grant it, and should not do so now. Significantly, this proposal does not deal with any problem arising from the Ames case. Those problems can all be dealt with through the waiver requirement for Government employees.

This amendment to the Fair Credit Reporting Act (FCRA) would allow the FBI, upon tendering a national security letter signed by the Director of the FBI, access to credit records held by consumer reporting companies on persons believed to be agents of a foreign power. As Congress recognized in the FCRA, consumer credit reporting companies are repositories for vast amounts of personal information, including credit history and buying patterns, much of which is inaccurate and incomplete. The FBI has asserted no reason, other than inconvenience, for obtaining this infor-

[6] *See, e.g.,* section 802(a)(1)(C)(ii) in section 2 of the S. 1869 (Cohen bill) and H.R. 4137 (Hyde bill), establishing a similar waiver for access to the records of persons who no longer have top secret access.

[7] This is the standard established in section 802(a)(1)(C)(ii) in section 2 of the Cohen and Hyde bills.

mation without following the statutorily prescribed procedures.[8] This highly personal and sensitive information should not be added to the narrow category of records subject to the national security letter exemption.[9]

The DeConcini-Warner and administration bills provide some additional protections to individuals that do not appear in Cohen-Boren or in Hyde, in the form of limits on dissemination and civil damages (and disciplinary action for violations by Government employees in the DeConcini-Warner bill only).[10] Although we think that these are important improvements on this long sought after authority, we still fundamentally object to the provision. The proposed exemption would erode current privacy statutes by giving the FBI authority to obtain these protected records in foreign intelligence cases without a subpoena or a court order and without notice to the individual that his or her records have been obtained by the Bureau.

Earlier this year, the House Banking Committee reported out a similar proposal, entitled "Furnishing Consumer Reports to Federal Bureau of Investigation for Counterintelligence Purposes." Section 123 of H.R. 1015 (Bereuter amendment). This proposal would require the FBI to obtain a warrant for such records, but would delay notice to the individual until 60 days after the investigation is completed. For nongovernmental employees, who have not waived their privacy rights, standard law enforcement procedures, including warrants, should apply.

III. Secret Searches of Tax Returns for Counterintelligence Purposes: DeConcini-Warner. Sec. 4.

The ACLU strongly opposes this provision, which does not appear in the administration bill, because it would for the first time authorize secret physical searches and seizures in direct violation of the fourth amendment, using the procedures set forth in the Foreign Intelligence Surveillance Act (FISA).[11] The FISA does not begin to address the fourth amendment problems posed by physical searches. The FISA was carefully crafted to address the specific needs of electronic surveillance for foreign intelligence purposes, specifically, that it is not possible to seize the contents of a telephone conversation if simultaneous notice is given. Physical searches follow separate procedures directly pursuant to the fourth amendment. There is no national security exception to the Constitution for physical searches, and see no reason to start one now.[12] Accordingly, we oppose the expansion of the FISA to cover searches of tax records or any other kinds of personal "papers" or property.

Moreover, the problem that this provision seeks to address can be dealt through the requirement of a waiver by persons with access to classified information that would include tax return information established in section 2. To the extent that the Government is here seeking access to the tax records of other persons, then it is simply reaching beyond the legitimate scope of this legislation.

Given that the administration is not seeking this authority, we see no reason for Congress to establish it.

IV. Lesser Criminal Offense for the Unauthorized Removal of Classified Documents: DeConcini-Warner. Sec. 7

This provision is only in the DeConcini-Warner bill and is not in the administration bill. A similar version of this provision was included in the original Jacobs Panel bill and is also included in the Cohen-Boren and Hyde bills.[13] The ACLU opposes this provision because it could have the unintended consequence of being used against whistleblowers and persons who leak information to the press. As Senator Metzenbaum commented at the Jacobs Panel hearing, this statute could be used to prosecute a Government employee who sought to bring a classified document to Congress to expose unlawful activities, misuse of funds, abuse of authority, or significant dangers to public health. It could also be used against persons who give copies of classified documents to the press—even if they do not retain copies themselves on the grounds that they know the press is going to retain copies "at an unauthor-

[8] In the *Las Vegas Sun*, April 13, 1990, FBI spokesman Mike Kortan said a major reason for the proposed expanded authority is to save time during investigations.

[9] At present, national security letter exemptions exist in the Right to Financial Privacy Act (12 U.S.C. 3414(a)(5)(A)) and in the Electronic Communications Privacy Act (18 U.S.C. 2709, as amended in 1993) for telephone subscriber information.

[10] We think that the section on disciplinary actions should be kept and included in the administration bill.

[11] In response to a question on this provision from Senator Warner, Deputy Attorney General Gorelick asked to respond in closed session. See note 5 for similar response to question on waiver of tax records.

[12] *See generally* section XX on national security physical searches, below.

[13] These other versions would only apply to the removal of top secret information. The DeConcini bill, on the other hand, would apply to all classified information.

ized location." While the Panel insisted that this was not the intent of the proposal, as drafted it would clearly have this effect.[14]

We understand that this provision is aimed at Government employees who routinely remove classified information for personal reasons. We do not think that criminal penalties is the appropriate remedy for this problem. Such employees should be subject to administrative discipline, including loss of clearance and job. Employees should only be subject to criminal prosecution if they intend to sell the information to a foreign power.

V. Rewards for Information Concerning Espionage: Administration. Sec. 4: DeConcini-Warner. Sec. 5.

This provision appears in both the administration and DeConcini-Warner bills, was included in the original Jacobs Panel bill, and is also included in the Cohen-Boren and Hyde bills. The ACLU has no position on this issue because we do not believe it implicates civil liberties.

VI. Jurisdiction for U.S. Courts to Try Cases Involving Espionage Outside the United States: Administration, Sec. 5; DeConcini-Warner. Sec. 6.

This provision appears in both the administration and DeConcini-Warner bills, was included in the original Jacobs Panel bill, and is also included in the Cohen-Boren and Hyde bills. The ACLU has no position on this issue because we do not believe it implicates civil liberties.

VII. Criminal Forfeiture for Violation of Certain Espionage Laws: Administration Sec. 6: DeConcini-Warner. Sec. 8

So long as the forfeiture of assets of persons occurs only upon their criminal conviction, the ACLU does not oppose this provision.

VIII. Denial of Annuities or Retired Pay to Persons Convicted of Espionage in Foreign Courts Involving United States Information: Administration, Sec. 7; DeConcini-Warner, Sec. 6

This provision appears in the administration bill, but not in the DeConcini-Warner bill. A similar version of this provision is was included in the original Jacobs Panel bill, and is also included in the Cohen-Boren and Hyde bills. The ACLU has no objection in principle to the end result contemplated by this section. However, we think that the proviso establishing judicial review in the Court of Claims that is in the Cohen-Boren and Hyde bills provides an important due process protection and should be included in the administration bill as well.

S. 1869 AND H.R. 4137: THE COUNTERINTELLIGENCE IMPROVEMENTS ACT OF 1994; S. 1866: THE PERSONAL SECURITY ACT OF 1994

The analysis of these bills is based on the ACLU's 1990 testimony before the Senate Intelligence Committee on the Jacobs Panel recommendations.[15] We oppose the overall approach of the Cohen-Boren and Hyde bills,[16] and believe that the administration bill should be the model on which any legislation is based (with the modifications that we have outlined above).

IX. Section 2: Amendment to the National Security Act of 1947, providing uniform requirements for persons granted top secret security clearances.

As with section 2 of the administration and DeConcini-Warner bills, we do not oppose the intent of this provision. (S. 1866, introduced by Senator Howard Metzenbaum, consists of just this section of the Cohen-Boren and Hyde bills.) We think the bills' focus on financial and travel information of Government employees with access to high-level classified information is appropriate and should be helpful in curbing espionage. New legislation should follow the administration model, with the modifications noted above.

X. Section 3: Protection of Cryptographic Information (Polygraph examinations for persons with access to cryptographic information).

The ACLU opposes all uses of polygraphs as an invasion of privacy, an affront to human dignity, and an unconstitutional violation of the prohibition against self-incrimination and unwarranted search and seizure. We do not think that Congress, in this or any other instance, should be passing laws authorizing their use. Rather,

[14] Jacobs Panel Hearing, at 107–9.

[15] Hearings before the Senate Select Committee on Intelligence on S. 2726 to Improve U.S. Counterintelligence Measures, 101st Cong., 2d Sess., S. Hrg. 101–1293 (May 23 & July 12, 1990).

[16] The Metzenbaum bill, S. 1866, is essentially section 2 of the Cohen-Boren and Hyde bills.

we think Congress should legislate a prohibition on the use of polygraphs for Government employees, just as it did in 1988 for most private employees by passing the Employee Polygraph Protection Act, 29 U.S.C. 2001.[17]

The ACLU presented extensive testimony on this issue to the DOD/CIA Joint Security Commission. That commission, after expressing concern about over-reliance on the polygraph, recommended its continued use for agencies that currently rely on it, but only with certain limitations on their intrusiveness, along with greater procedural safeguards and oversight.[18] Subsequent revelations about the ineffectiveness of the polygraph in the Ames spy case strongly warrant reconsideration of the commission's conclusions and serious consideration of greater restrictions on its use, if not an outright prohibition.

In 1983, the Office of Technology Assessment released its comprehensive study *Scientific Validity of Polygraph Testing*. The study concluded that "available research evidence does not establish the scientific validity of the polygraph test for personnel security screening," and that "the further one gets away from the conditions of a criminal investigation, the weaker the evidence for polygraph validity." The report went on to express concerns that persons were being falsely labeled as deceptive by these tests.

No amount of training or experience on the part of an examiner can overcome the glaring absence of scientific evidence supporting the underlying premise of lie detector testing, particularly in the area of pre-employment or random screening. No amount of procedural "safeguards" or detailed statutory instructions on how employment polygraph tests must be conducted can alleviate the fundamental unfairness of using such a dubious process to measure an individual's integrity. In short, the polygraph technique has no scientific validity. The so-called "lie detector" is really only a "stress detector" and a polygraph examiner has no scientific basis for distinguishing the stress that may indicate deception from any other stress, including fear, anger, humiliation, or frustration regarding the polygraph test itself.

Moreover, the ACLU believes that polygraph testing is unconstitutional because it violates the fourth amendment's prohibition against unlawful searches and seizures and the fifth amendment's prohibition against self-incrimination. The closest analogy to the type of search that occurs when the Government subjects an employee to a polygraph exam is a search of a person's private papers and diaries. As Justice Brennan wrote:

> An individual's books and papers are generally little more than an extension of his person. . . . [If production of such records could be compelled,] [t]he ability to think private thoughts, facilitated as it is by pen and paper, and the ability to preserve intimate memories would be curtailed through fear that those thoughts or the events of those memories would become the subjects of criminal sanctions however invalidly imposed.

Fisher v. *United States*, 425 U.S. 391, 420 (1976) (Brennan, J., concurring). It is clear that the scope of the protection afforded by the fourth amendment encompasses not only a person's home, but also her personal papers and therefore, by extension, her private thoughts.

We also believe that the fifth amendment shields employees from any attempt to compel disclosure of information that could incriminate an employee through the use of a polygraph. The fifth amendment privilege is broad enough to protect against "disclosures that the witness reasonably believes could be used in a criminal prosecution or could lead to other evidence that might be so used." *Kastigar* v. *United States*, 406 U.S. 441, 445 (1972). Thus, any rule that compels employees to submit to a polygraph test must necessarily be accompanied by a grant of immunity for any answers that may incriminate them.

---

[17] We concur with the Jacobs Panel that any use of the polygraph should at a minimum provide safeguards similar to those now in effect at the Department of Defense, in terms of limiting questions exclusively to counterintelligence matters and limiting the use and effect of the results of such examinations. DOD Directive No. 5210.48 (Dec. 24, 1984); see also EPPA, 29 U.S.C. 2007 (restrictions on use of exemptions: rights of examinees and qualifications and requirements of examiners). We would go further and limit them to cases where there is individualized suspicion of specific security violations, be accompanied by a guarantee of criminal use immunity, and be narrowly tailored to the specific focus of the investigation.

[18] Report of the Joint Security Commission on Redefining Security to the Secretary of Defense and the Director of Central Intelligence, Feb. 28, 1994, at 67. To the extent that this provision is aimed at State Department employees, we do not think that the polygraph should be introduced to agencies that do not currently use them, especially when this department, under the leadership of former Secretary of State George Shultz, has declared that these tests are neither proper nor effective.

For these reasons, we oppose this provision of the bill, and urge the Committee to remove it from the legislative package.

XI. Section 4: Amendment to the Right to Financial Privacy Act (RFPA) to permit access for purposes of security clearance investigations.

As with the other provisions, we do not oppose requiring individuals with high-level security clearances to consent to access to their financial records. As before, however, we think that the Government should have an affirmative obligation to notify the individual each time it seeks access to that individual's financial records, except upon a showing that "such records are sought for foreign counterintelligence purposes and that there are specific and articulable facts giving reason to believe that the customer or entity whose records are sought is a foreign power or an agent of a foreign power.[19] Information collected under the new provision should only be used for security clearance and counterintelligence purposes.[20]

We support the provision in these bills requiring the administration to report to the intelligence committees concerning the number of requests made for financial records (sec. (d)(4)). This, along with the additional safeguards that we have proposed above, will serve to minimize potential abuse of consensual access to financial records.

XII. Section 5: New Criminal Offense for the Possession of Espionage Devices.

At the Jacobs Panel hearing in 1991, several Senators raised a concern about the potential danger this proposal poses for innocent persons. We share that concern. Although we believe that it might be possible to write a clear and stringent enough intent requirement that the provision would not be subject to abuse and would not sweep innocent persons into its orbit, it is not clear whether that provision would be of much value.

We suggest that the Committee seriously consider whether this provision is likely to be useful in enough cases to justify seeking a way to make it acceptable. If so, we would be willing to work with the Committee to try to do that.

XIII. Section 6: New Offense for Selling to Foreign Governments Documents and Other Materials Designated as top secret.

This is the most far-reaching proposal in these bills and one that requires the most careful consideration. In light of the measured approaches in the administration and DeConcini-Warner bills, we do not think that Congress should consider broadening the espionage laws with this or any other provision. Moreover, it should not do so unless it also deals with the question of whether the general espionage and theft statutes apply to the provision of information to the press. Otherwise, congressional silence may be construed as approval of the result in the *Morison* case.[21]

In the *Morison* case the Government for the second time sought to apply the general espionage statute (18 U.S.C. 793) and the theft of Government property statute (18 U.S.C. 641) to the allegedly unauthorized transfer of classified information to the press. In *Morison*, the Government succeeded in getting a conviction that was sustained on appeal. The ACLU, which participated in Mr. Morison's representation, believes that neither statute was meant to apply to the provision of information to the press. The espionage laws, in our view, were not intended by Congress to cover actions leading to the publication of information. Indeed, a very careful and thorough review of the legislative history by two distinguished Columbia Law School professors, one of whom was a member of the Jacobs Panel, reached the same conclusion.[22] We also do not believe that the theft statutes were meant to or should apply in most cases to the transfer of information, including provision of information to the press.

XIV. Section 7: Lesser Criminal Offense for the Removal of Top Secret Documents by Government Employees and Contractors.

See section IV concerning S. 1948, above. We note that the provision in S. 1948 differs from this in one important regard: The DeConcini-Warner bill would apply to the removal of any classified information, the Cohen-Boren and Hyde bills would only apply to top secret information. However, this limitation does not cure the defects that this provision has with respect to whistleblowing and leaks.

---

[19] 12 U.S.C. 3414(a)(5)(A).

[20] The existing exception provides that financial records may only be disclosed to "a Government authority authorized to conduct foreign counter- or foreign positive-intelligence activities for purposes of conducting such activities." 12 U.S.C. 3414(a)(1)(A).

[21] *United States* v. *Morison*, 844 F.2d 1057 (4th Cir. 1988), *cert. denied*, 109 S. Ct. 259 (1988).

[22] *See* Edgar and Schmidt, "The Espionage Statutes and Publication of Defense Information," 73 *Colum. L. Rev.* 929 (1973).

XV. Section 8: Jurisdiction for U.S. Courts to Try Cases Involving Espionage Outside the United States.

This provision also appears in the administration and DeConcini-Warner bills. The ACLU has no position on this issue.

XVI. Section 9: Expansion of Existing Statute Regarding Forfeiture of Collateral Profits of Crime to Additional Espionage Offenses ("Son of Sam" law).

The ACLU opposes on first amendment grounds all statutes that withhold or require forfeiture of compensation to convicts from writing or speaking about their offenses (so-called Son of Sam laws). Thus, we absolutely oppose amending 18 U.S.C. 3681 to include additional espionage offenses. The first amendment applies to criminals and ex-convicts as fully as it applies to every other American. Son of Sam laws not only chill the first amendment rights of offenders, but also discriminate against a particular kind of speech by a particular class of persons. Furthermore, they harm the public by eliminating speech from the marketplace.

Finally, these statutes are neither an appropriate nor a necessary vehicle for compensating crime victims. Civil damage suits, judicially imposed fines, or other remedies could serve the same purpose. But imposing a direct chill on speech by denying compensation for it serves neither freedom of speech nor the public's right to know.[23]

XVII. Section 10: Denial of Annuities or Retired Pay to Persons Convicted of Espionage in Foreign Courts Involving United States Information.

A similar version of this provision is included in the administration bill. The ACLU has no objection in principle to the end result contemplated by this section. We think that the proviso establishing judicial review in the Court of Claims, which is not in the administration bill, provides an important due process protection and should be maintained.

XVIII. Section 11: Authorizing FBI to Obtain Consumer Reports on Persons Believed to be Agents of Foreign Powers.

This provision also appears in the DeConcini-Warner and the administration bills. The ACLU opposes this provision. See section II, above.

XIX. Section 12: Rewards for reporting espionage.

This provision also appears in the administration and DeConcini-Warner bills. The ACLU has no position on the use of rewards for information concerning criminal activity.

XX. Section 13: To Provide for a Court Order Process for National Security Physical Searches Similar to that for Electronic Surveillance.

Section 13 of the Cohen-Boren and Hyde bills propose to apply the Foreign Intelligence Surveillance Act (FISA) procedures to physical searches conducted in the United States for intelligence purposes. The ACLU strongly opposes this provision. However, we believe that Congress should enact legislation that requires the executive branch to obtain warrants and give formal notice when conducting physical searches within the United States based on national security. We believe that the fourth amendment prohibits warrantless, national security searches and that the President has no inherent authority to violate the fourth amendment for national security purposes.[24]

A. THERE IS NO NATIONAL SECURITY EXCEPTION TO THE FOURTH AMENDMENT

The ACLU is deeply troubled by the notion that there is a national security exception to the fourth amendment or any part of the Bill of Rights. We regard those rights as fundamental and absolute. While the Government has often exercised extraconstitutional power in the name of national security, no such exception exists, and the creation of one would swallow the very protections the Constitution was designed to uphold. As the Supreme Court has stated:

> [T]his concept of "national defense" cannot be deemed an end in itself, justifying any exercise of . . . power designed to promote such a goal. Implicit in the term "national defense" is the notion of defending those values and ideals which set this nation apart. . . . It would indeed be ironic if, in the

[23] In addition, inclusions of convictions by foreign courts in this forfeiture statute is a violation of due process for the reasons explained in the following section.

[24] The ACLU presented extensive testimony on this issue in 1990 before the House Intelligence Committee. *See* Hearing before the House Permanent Select Committee on Intelligence on Physical Searches for Foreign Intelligence Purposes, 101st Cong., 2d Sess. (May 24, 1990).

> name of national defense, we would sanction the subversion of . . . those liberties . . . which makes the defense of the nation worthwhile.

United States v. *Robel*, 389 U.S. 258, 264 (1967), quoted in *United States* v. *United States District Court [Keith]*, 407 U.S. 297, 332 (1972) (Douglas, J., concurring).

The ACLU reluctantly accepted the FISA as the best possible accommodation in light of the Government's practice of conductlng warrantless electronic searches and the Supreme Court's suggestion of a limited national security exception for electronic searches.[25] However, we have always had doubts about some elements of the FISA and are troubled by its implementation.

Notwithstanding the FISA, the ACLU firmly believes that no such exception exists for physical searches. The executive branch's claim of the right to engage in warrantless searches of homes and papers contradicts the most fundamental guarantee of liberty in the Constitution. Congress should put an end to this practice by enacting legislation that prohibits all physical searches without a warrant and without giving simultaneous announcement and notice of the search and an inventory of items seized.

The Framers themselves drafted the fourth amendment in the context of such national security claims. They understood well the way in which national security was and could be used as an exception to the legal limits of governmental power, especially with respect to searches and seizure under general warrants, and they rejected it. In the *Keith* case, the Supreme Court stated emphatically that "physical entry of the home is the chief evil against which the wording of the Fourth Amendment is directed." 407 U.S. at 313. In *Payton* v. *New York*, 445 U.S. 573 (1980), the Court reiterated that point:

> The fourth amendment protects the individual's privacy in a variety of settings. In none is the zone of privacy more clearly defined than when bounded by the unambiguous physical dimensions of an individual's home—a zone that finds its roots in clear and specific constitutional terms: "The right of the people to be secure in their . . . houses . . . shall not be violated." That language unequivocally establishes the proposition that "[a]t the very core [of the Fourth Amendment] stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion."

Id. at 589–90 (quoting *Silverman* v. *United States*, 365 U.S. 505, 511 (1961)).

The Supreme Court has never directly ruled on a national security exception for physical searches. In the only Supreme Court case dealing with a warrantless national security physical search, the Court took it for granted that the fourth amendment fully applied. *Abel* v. *United States*, 362 U.S. 217, 219–20 (1960) ("Of course the nature of the case, the fact that it was a prosecution for espionage, has no bearing whatever upon the legal considerations relevant to the admissibility of evidence.").

Since *Abel*, only one appeals court case has upheld a national security warrant exception for physical searches.[26] In *U.S.* v. *Truong*, 629 F.2d 908 (4th Cir. 1980), *app. after remand*, 667 F.2d 1105 (1981), *cert. denied*, 454 U.S. 1144 (1982), the court of appeals upheld the admission into evidence of the fruits of two warrantless searches of sealed packages that Truong had given to a Government informant for delivery overseas.[27] The court ruled that the searches were valid under the fourth amendment so long as their primary purpose was for intelligence gathering. But the court also held that once the primary purpose of the investigation had shifted to

---

[25] In *Keith*, the Court ruled that warrants were required for domestic oriented national security wiretaps, but did not address "issues which may be involved with respect to activities of foreign powers and their agents," 407 U.S. at 322, leaving the suggestion that it might have reached a different conclusion in such a case.

[26] In *U.S.* v. *Ehrlichman*, 546 F.2d 910 (1976), the D.C. Circuit upheld a district court ruling that the warrantless physical search of Daniel Ellsberg's psychiatrist's office was unconstitutional and rejected Ehrlichman's argument that it was legitimately conducted in accordance with the President's national security powers. The circuit court declined to rule on whether it would have been authorized if the President or the Attorney General had personally authorized the search. *Id.* at 925. A concurring opinion by Judge Leventhal discussed the important differences between physical and electronic searches and expressed strong doubts that an exception to the fourth amendment exists for national security physical searches. *Id.* at 933–40.

[27] The court found that a third search was not legitimate under the fourth amendment, but upheld the search anyway "because Truong did not have a legitimate expectation of privacy in the package." 629 F.2d at 917.

gathering criminal evidence, as it did, then a warrant was required for all subsequent searches. 629 F.2d at 915–16.[28]

The ACLU believes that the holding in *Truong* was wrong. No governmental purpose can justify ignoring the fourth amendment by sanctioning a warrantless, nonconsensual invasion into the privacy of one's home or papers. Even if the fourth amendment permitted such balancing, the Government's interest in protecting the "national security" would not outweigh the gross infringement on individual rights that results from such searches. Nor is national security an exigent circumstance justifying a search without probable cause, a warrant, or notice.[29] On the contrary, the Government must have probable cause of criminal activity (e.g., espionage, sabotage, treason, terrorism), must obtain a warrant from a judicial officer, and must knock, give notice and leave an inventory of items seized in any search.

B. FISA DOES NOT PROVIDE ADEQUATE PROCEDURAL SAFEGUARDS FOR PHYSICAL SEARCHES

Furthermore, what this provision fails to recognize is that the warrant is only one part, and at this point perhaps a small part, of the rubric of the fourth amendment constitutional protection. Warrants themselves are rarely turned down, by any judge, liberal or conservative. Thus, simply having one more person review the predicate standards for the warrant adds little protection to the rights of the target.[30] That protection comes largely from the public scrutiny of the search itself, as it is being conducted—the person being searched can monitor whether the officer is keeping within the restrictions of the warrant, and can review the inventory left to see exactly what was searched and taken—and from the open adversary process in court, where the propriety of the warrant and the search can be tested.

This bill would remove these fundamental fourth amendment safeguards in national security cases. The Constitution explicitly proscribes such conduct, and it is critically important that Congress not retreat from the fundamental workings of the fourth amendment. The proposed bill effectively denies a defendant, or any other target of a national security physical search, the fundamental right to challenge the legality of the warrant and the search in an open, adversary proceeding. Section 404(f) gives the Attorney General the authority to require in camera and ex parte proceedings on whether the warrant and the search was in fact valid. In FISA cases, the Attorney General almost always invokes this procedure, and the court always upholds it. However, without meaning to impugn any judges, deficiencies in a warrant can only be brought to light through an adversary hearing.

An equally important issue is how the search is conducted, and how the fruits are used. The first aspect is kept accountable, at least in part, by the people who are being searched themselves. One's home and property should be inviolate; if anyone is going to rummage through them, we must know about it when it is happening, in order to make sure they did not cross any bounds. It is not enough for a judge to determine that on his own. Also, if the search is secret, there is no way for someone even to know if his or her rights were violated so as to be able to go into court Thus, the agent should be required to knock, announce his or her purpose and that he or she has a warrant. The agent must also leave behind a copy of the warrant and an inventory of what was seized.

This principle finds its bedrock in statutory and common law.[31] While not explicitly stated in the Constitution nor established by the Supreme Court, we believe it is an absolute and fundamental element of any reasonable search or seizure. As Justice Brennan has noted, "[t]he protections of individual freedom carried into the Fourth Amendment . . . undoubtedly included this firmly established requirement of an announcement by police officers of purpose and authority before breaking into an individual's home." *Ker* v. *California*, 374 U.S. 23, 49 (1963) (Brennan, J., dis-

---

[28] The searches in *Truong* involved packages for overseas delivery, for which there is a lower expectation of privacy than for searches of one's home and personal papers.

[29] *See Ehrlichman*, 546 F.2d at 940 (Levanthal, J., concurring).

[30] We note that the Foreign Intelligence Surveillance Court has never denied a warrant application under the FISA; the court has essentially endorsed the standards and procedures followed by the Justice Department for FISA surveillance, which the Justice Department claims it also follows on its own for physical searches.

[31] *See Miller* v. *United States*, 357 U.S. 301, 313 (1958) ("The requirement of prior notice of authority and purpose before forcing entry into a home is deeply rooted in our heritage and should not be given grudging application. Congress, codifying tradition embedded in Anglo-American law, has declared in [18 U.S.C. 3109] the reverence of the law for the individual's right of privacy in his house. Every householder, the good and the bad, the guilty and the innocent, is entitled to the protection designed to secure the common interest against unlawful invasion of the house."); *see also id* at 313 n.12 ("Compliance is also a safeguard for the police themselves who might be mistaken for prowlers and be shot down by a fearful householder.").

senting). Justice Brennan demonstrated through an analysis of British and American common law that "[i]t was firmly established long before the adoption of the Bill of Rights that the fundamental liberty of the individual includes protection against unannounced police entries." *Id.* at 47.

In addition to knocking and giving notice at the outset of the search, the Government, whether or not the occupants are present, must leave an inventory of items seized or, if nothing was taken, a copy of the warrant indicating they were present. *See* F.R.Crim.P. 41(d) ("The officer taking property under the warrant shall give to the person from whom or from whose premises the property was taken a copy of the warrant and a receipt for the property taken or shall leave the copy and receipt at the place from which the property was taken. The return shall be made promptly and shall be accompanied by a written inventory of any property taken.")[32]; *see also United States* v. *Gervato*, 474 F.2d 40, 44–45 (3d Cir.), *cert. denied*, 414 U.S. 864 (1973); *Payne* v. *United States*, 508 F.2d 1391, 1394 (5th Cir.), *cert. denied*, 423 U.S. 933 (1975).

The fourth amendment prohibition against the warrantless and unannounced seizure of papers protects against photographing them, even if no physical property is actually seized. Taking photographs, or even just looking around, violates that right just as much as the actual seizing of tangible property.[33] These requirements help to ensure that, even with a warrant, the police not engage in a general search without the knowledge of the occupants and without their having an opportunity to sue for return of materials seized.[34]

The second issue, how the fruits are used, can only be tested in court at trial through the adversary process, via the suppression motion. This bill effectively denies a defendant an opportunity to participate in that process.

While conceived and understood in the context of foreign intelligence collection activities, this bill is equally designed for use in criminal investigations and prosecutions. The Constitution simply does not countenance a separate standard for the crimes of espionage and terrorism or for intelligence investigations. For such criminal investigations and prosecutions, the Government already has statutory and constitutional authority to act; but that power is necessarily balanced with fundamental protections for one's personal effects and for criminal defendants.

If the Government needs special authority to counter foreign espionage, it cannot come at the expense of individual rights. The only compromise is to allow such secret searches for pure counterintelligence purposes, but to deny any such information to be used against the target, whether for criminal or any other proceedings.

Thus, we do not think the FISA itself should be amended to accommodate physical searches, as this legislation proposes. However, we do believe that some aspects of the FISA standards for obtaining a warrant and some of its procedures could reasonably be applied for obtaining a warrant for national security physical searches, but only where the sole purpose of the search is for intelligence gathering (and not for criminal investigation or prosecution), where the warrant particularly describes the place to be searched and the persons or things to be seized (unlike the FISA or the new recommendation), and where knock, notice, and inventory are required, whether of the home, office, mail, or luggage.

C. CONCLUSION

Accordingly, Congress should pass no law that authorizes a general exception to the knock and notice requirement for national security physical searches, and, therefore, should not use the FISA as a vehicle for authorizing such searches. On the contrary, we urge Congress to pass a separate law prohibiting the Government from engaging in warrantless, unannounced and unnoticed national security physical searches, particularly of the homes and offices of U.S. persons. To do so, it could use aspects of the FISA probable cause standard and its warrant application procedures, but it must insist on knock, notice, and inventory and that the warrant describe the search with particularity.

---

[32] Note that under the FISA, the "warrant" need never be shown to the target if so ordered by the Attorney General. 50 U.S.C. 1806(f).

[33] We note that in a 1990 appeals court opinion, with which we do not entirely agree, the court held that a covert search for the purpose of taking photographs was an "intangible search," much like wiretapping, and therefore could be conducted without prior notice. *U.S.* v. *Villegas*, 899 F.2d 1324 (2d Cir. 1990). But that court ruled that the Government could not "dispense with advance or contemporaneous notice of the search unless they have made a showing of reasonable necessity for the delay," and that, in such cases, subsequent notice must be given within 7 days. *Id.* at 2610.

[34] *See* F.R.Crim.P. 41(e): "A person aggrieved by an unlawful search and seizure or by the deprivation of property may move the district court in which the property was seized for the return of the property on the ground that such person is entitled to lawful possession of the property."

However, if Congress is not prepared to take such action, we believe that it may indeed be better to do nothing and leave the status quo. Notwithstanding the Ames case, we understand that very few warrantless physical searches are currently conducted against U.S. persons. Legislation authorizing searches without knock, notice, and inventory would likely lead to a significant increase in such searches in clear contravention of the constitutional rights of Americans.

TESTIMONY OF KATE MARTIN

Ms. MARTIN. Thank you, Mr. Chairman and Mr. Vice Chairman, for the opportunity to appear today and discuss the civil liberties implications of the proposed counterintelligence reforms. We have prepared an appendix which will discuss in some detail the various bills and would ask that that be included as part of the record, when we submit it.

Vice Chairman WARNER. Without objection.

Ms. MARTIN. The ACLU has long believed that the counterintelligence activities of the United States should be and can be reorganized to deal more effectively with the problem of espionage, while at the same time reducing harm to civil liberties.

In general——

Vice Chairman WARNER. Just to ask personally of you, were you involved at the time we looked at the Jacobs' report? In other words, has there been a continuity on your part personally or your organization or——

Ms. MARTIN. Yes, I was. I was at that time the director of the litigation program of the Center for National Security Studies, but in fact had a fair amount of involvement in drafting the testimony that was given by the former director of the center.

Vice Chairman WARNER. So you personally and professionally have been involved with this issue for some time then?

Ms. MARTIN. Yes, sir.

Vice Chairman WARNER. And can speak with a good deal of experience.

Ms. MARTIN. Well——

Vice Chairman WARNER. And we thank you.

Ms. MARTIN. In general, we do not believe that the answer lies in broadening the investigative powers of the Government at the expense of individual privacy. We note that at the moment there are several reviews being undertaken in both the executive branch and in the Congress of the overall security clearance system, not only with respect to the problem of espionage, but also with respect to the end of the cold war and the changing nature of the threats and problems confronted by the intelligence communities.

We would like to, at the outset, say that we are, in general, quite pleased with the direction of some of the proposals that have been made, specifically the ones—the one submitted by the administration and some of the proposals in the Chairman's and Vice Chairman's proposed legislation.

We believe that the proposal from the administration is in large measure a restrained and appropriate response to the problem. All of the proposals contain measures that would allow the Government to obtain financial and travel records of certain Government employees with access to classified information in limited circumstances as a condition of access to such information. In general we agree that that is the proper approach to take if it is limited

in ways that we think are necessary to deal with privacy and civil liberties problems.

We think that the category of employees subject to such disclosure requirements should be a limited one, in part for the reasons that Senator Boren mentioned this morning—otherwise it is a useless exercise. But the category should also be limted in order to deal with the constitutional issues.

The administration proposal, for example, would require that the Government not gain access to financial and travel records about a specific individual unless it had some specific information that the specific individual was disclosing classified information to a foreign power, or unless there was specific information that the individual had come into unexplained wealth. We believe that kind of limitation is very important and very appropriate.

At the same time, there are two issues with regard to the——

Vice Chairman WARNER. Very important. In a legal framework, would you say it is probable cause or prima facie or just a rumor or where in the spectrum of how the law treats information to trigger things would this criteria fall?

Ms. MARTIN. We would propose the standard of reasonable suspicion.

Vice Chairman WARNER. Reasonable——

Ms. MARTIN. Which is less than probable cause.

Vice Chairman WARNER. Yes. Is that defined anywhere, reasonable?

Ms. MARTIN. It's not that I know of.

Vice Chairman WARNER. Nor do I. It's a new term to me.

[Pause.]

Ms. MARTIN. Oh, I'm sorry. Mr. Stern informs me that it is in fact a term used in FBI guidelines for counterintelligence investigations.

Vice Chairman WARNER. FBI guidelines.

Ms. MARTIN. Yes.

Vice Chairman WARNER. So there is a definition and a practice.

Ms. MARTIN. And a practice. And that that is the standard we believe should be used here.

The two issues that we are still concerned about involve whether or not the employees are entitled to notice that the Government has in fact obtained their financial or travel records. We believe that in general the rules should provide that they are entitled to notice, unless there is some real need to keep the fact that there may be a counterintelligence investigation of that individual a secret. I think that the administration proposal talks about keeping it secret in the course of all security determinations. We think that is too broad. If there is a reasonable suspicion that the individual is in fact providing information to a foreign power and the existence of the counterintelligence investigation is at that moment secret, then we believe that it is appropriate not to give contemporaneous notice to the employee.

Vice Chairman WARNER. Would that be about the same standard as you applied in your earlier case?

Ms. MARTIN. In our earlier testimony?

Vice Chairman WARNER. Which you and I just discussed? Reasonable suspicion.

Ms. MARTIN. Yes, it would be the same standard.

Vice Chairman WARNER. In both instances.

Ms. MARTIN. Yes.

Vice Chairman WARNER. But you said it had to be when you had reasonable suspicion that he was dealing with a foreign government. Suppose this individual were dealing with one of his own colleagues, which he had reason to believe in turn was then diverting it to a foreign government. In other words——

Ms. MARTIN. Oh, we would include that situation. I should have said dealing with either a foreign government or an agent of a foreign government. In either of those situations, we would have no objection.

We do, however, object to applying these requirements to employees after they no longer have current access to classified information. We do not believe that there is any basis for creating an exception to the constitutional requirements governing law enforcement investigations, which requirements include probable cause rather than reasonable suspicion, and a search warrant or a subpoena to obtain the personal and private records of individuals after they no longer have access to classified information.

There are other proposals in the various bills that do not raise civil liberties concerns including, for example, enhanced penalties for espionage, providing rewards for discovering espionage, the provision of venue or extraterritorial offenses, none of those raise civil liberties concerns.

We are, however, extremely concerned about a couple of provisions, one of which is contained in the administration proposal as well as in the other bills, and some of which are only contained in the other bills. The first one is the National Security Letter exception to the Fair Credit Reporting Act. Mr. Kohler discussed some of the reasons why we don't think that is a good idea.

I might only mention that that proposal is not a proposal that was crafted in response to the Ames case, but is in fact a provision that the FBI has sought for the last 4 years, and Congress has not seen fit to provide it. We don't believe it is appropriate to do so. The proposed amendment would provide access to the credit records, not just of Government employees, but of any individual.

The second area of concern is the issue of physical searches and seizures of various records without a warrant, and in secret. The original Jacobs Panel bill and now Senator Boren's and Cohen's bill provide for an expansion of the authorities under the Foreign Intelligence Surveillance Act to certain kinds of physical searches. And there is also a provision for expanding that kind of authority to tax records. We strongly oppose that.

The basis for the provisions in the Foreign Intelligence Surveillance Act, which the ACLU supported, was in part the unique nature of electronic surveillance. If you tell someone you are wiretapping them during the wiretap, you will, of course, be unable to wiretap and capture the conversation.

We know of no basis to say that there is exception to the warrant requirement for seizing an American's personal papers or other kinds of private documents. Indeed, in the Ames case, the Attorney General evidently authorized a warrantless secret search of Mr. Ames' house pursuant to Executive Order 12333, which was signed

by President Reagan. We are extremely disturbed that the new administration chose to carry out such a search of an American citizen, intended to seize evidence to be used against that American citizen in a court of law to convict him. And the administration did so instead of initiating a public dialog about the propriety of such warrantless searches, especially given the end of the cold war.

On that subject I was concerned to hear the Deputy Attorney General this morning answer Senator Warner's question about their position on the provision granting FISA kinds of procedures for tax records, by saying she could only respond in Executive Session. That kind of policy question, raising the issue of a significant civil liberties violation should and must be debated publicly—first, whether it is, constitutional, and second, whether there is any reason for it.

In connection with that, let me add that as a general matter, we support the role of the Congress in legislating on these issues. The administration this morning said that they feared that their litigation position might be jeopardized if the Congress statutorily authorized some provisions and not other provisions of their security program. We believe, however, that where decisions are involved which require striking a balance between national security and civil liberties, as Senator Warner pointed out this morning, and a decision is going to be made to limit civil liberties, such decisions should be made jointly by the Congress and the executive branch. They should be made only after full public debate, and made jointly in order to ensure that both branches have reached a considered judgment that any limitations on civil liberties are in fact necessary and appropriate. We do not believe that such decisions should be made by the executive branch on its own.

There is, of course, a history of doing that in the past, and we are hopeful that this administration will take a different view of it in the future.

In closing, let me note that on the general subject of the difficulties involved in counterintelligence, there are two principles relevant to crafting responses to deal with the problem. Both principles I am sure the Committee is well aware of. First, there are sometimes, and in fact, frequently conflicting objectives involved in intelligence gathering and law enforcement. Counterintelligence, of course, is the area where the two come together, and raise difficult problems, and it is where civil liberties concerns arise, because there is the potential for law enforcement and criminal prosecutions of American citizens.

At the same time, we think that the time has come to recognize that the fact that the threat has changed may indeed mean that the balance has changed between some national security and civil liberties concerns. We do not argue that the world is no longer a dangerous place. We do, however, believe that we no longer face, and the U.S. Government would no longer say that we face an adversary aimed at a military takeover of the United States. We believe that the threat of organized crime, or worldwide narcotics rings, and the threat of economic espionage are quite different kinds of threats which lead to two conclusions.

First, that the procedures and apparatus that were designed to deal with the military defense of the United States may no longer

be appropriate. But even more significantly, that the balance may indeed have shifted, because you are no longer talking about preserving the very existence of the United States—although we do not question the importance of these other matters.

So we would be happy to work with the Committee further on the specifics.

Vice Chairman WARNER. Those last few sentences about preserving the existence of the United States, would you go back over that?

Ms. MARTIN. Yes.

Vice Chairman WARNER. One of the handicaps, I have not seen your statement. It was just given this morning. I am not registering a complaint, but——

Ms. MARTIN. Yes.

Vice Chairman WARNER [continuing]. I would liked to have read it so that I could engage you in a more thorough colloquy here. But nevertheless, go back over that last point again.

Ms. MARTIN. Yes.

During the cold war, I think the national security and civil liberties issues were framed in terms of the United States facing the Soviet Union as an adversary aimed at taking over the United States. It was basically an issue of self preservation, and we were facing an adversary who had the potential military strength to defeat us.

That is no longer the situation. The threats and the national——

Vice Chairman WARNER. Ms. Martin, at my juncture in this, I will debate that issue with you very thoroughly. So I'll defer my further comments on that. I don't mean to be argumentative on that, but my gracious, if you have made any study, or have it done, of what weaponry is retained by Russia today, it's basically the strategic arsenal that they had before, minus some in the Ukraine and some in Kazakhstan. They are modernizing their submarine force. They are going into another generation of intercontinental ballistic missile. There has been some downgrading of their air element and some of their ground elements, but I would ask that you get a briefing on that and see whether or not you could make that statement once again.

Ms. MARTIN. Well, I should be clearer, and amend my statement, because the ACLU does not take a position on the actual extent of a threat to the United States.

Our position really is that to the extent that the intelligence community refocuses its efforts on such things as organized crime, economic espionage, international narcotics, those threats are by their nature very different from the threat that the Soviet Union was deemed to pose. And therefore, work that is done to meet those threats has to be re-evaluated.

Now, if the main task of the intelligence and the defense community continues to be to defend ourselves against potential military threats from Russia or China, then that is certainly much more like the situation during the cold war.

My understanding is that both the intelligence community and the Defense communities have now said that the problems facing them are quite different. While those problems are important, they are not, I believe, the kind of fundamental threat to the United

States' existence which would justify restrictions on civil liberties that, in time of war or cold war, might otherwise be acceptable.

Vice Chairman WARNER. Let me add one more element to this, and that is, in this vacuum between—created by the Soviet Union disappearing and the several states, a dozen or more, coming into the Soviet Union, into the vacuum is quickly coming the proliferation of weapons of mass destruction—nuclear, biological, and chemical. And those weapons are now being possessed by much smaller entities than the former monolith of the Soviet Union.

So again, I would urge you to look at those statements with great caution, because I frankly, in my own personal opinion, the world is almost a more troublesome place today than it was when we understood very clearly the bipolar relationship between communism, the Soviet Union, and the Free World. Now it is fractured in so many different ways.

So perhaps you and I some day can have a more detailed colloquy on this, but I would hope you would reexamine such statements as we no longer need to apply the rigid standards we may have had during the cold war period, because that has disappeared. Take into consideration what may have come in its place.

Chairman DECONCINI. Mr. Whipple, if you would summarize your statement, your full statement will be printed in the record.

[The prepared statement of Mr. Whipple follows:]

PREPARED STATEMENT OF DAVID D. WHIPPLE

Today I will concentrate my initial comments on three concepts which were included in one or more of the four bills sent to me. The first relates to background investigations, financial disclosure statements, disclosures of tax returns, bank accounts, investment credit accounts, and assets, special searches based on orders from a Foreign Intelligence Surveillance Court, and amending the Right to Financial Privacy Act. The second addresses what I fear may be a misapprehension of the use and utility of polygraph "examinations". Lastly, I am worried about the prospect of legislation which in effect would put the FBI in charge of all counterintelligence, including overseas operations now run by CIA.

My comments are based on my own personal experiences. I am extremely proud of having been for 35 years an operations officer in the CIA. Most of those years were served on 2- to 4-year postings abroad, in Southeast Asia, Africa, and Europe, and/or shorter postings in Asia, the Middle East, and Europe. Of my 10 more permanent posts, I was the station chief in five countries and deputy station chief in three others. I ended my career in 1985 working directly for the DCI as the first National Intelligence Officer for Counterterrorism. During all those years I regarded my career as important, very educational, and emotionally fulfilling. I described myself as an "on-the-street" intelligence professional. Listeners may suspect that I am strongly prejudiced in favor of what I consider to be the best interests of American intelligence as identical with those of our Nation. Your suspicion would be correct.

When I joined CIA in 1950, I assumed that because I was to occupy positions of great trust somebody was always or occasionally going to be looking over my shoulder with or without my knowledge. I think I would have been disappointed if I believed CIA was less than majorly concerned with my security-related private behavior. I understand that CIA's management today believes that while those working in intelligence organizations freely compromise aspects of their privacy to satisfy security needs, they do so with faith that fundamental rights, including due process, will not be compromised; constitutional guarantees must be considered against the need for intrusion on individual rights in the interest of national security. I think that is all well and good with respect to citizens who are not intelligence people. However, I take a more extreme view. I believe that when one signs on as an intelligence employee he or she should be required to waive several constitutional guarantees and rights. He should expect to be treated differently from ordinary people in the interest of national security broadly or narrowly defined. I do applaud the provisions I see in the draft bills but suggest that those provisions be even more stringent and a bit less concerned with "fairness."

Second, I note that one of the bills (Senator Cohen's and Senator Boren's) refers to periodic polygraph "examinations." The last word suggests to me a misunderstanding, widely shared by the American news media, of what the polygraph process can and cannot do. I have had a good deal of experience with the use of the polygraph and polygraph operators abroad in agent operations. The polygraph can be a very useful investigative tool, but only a tool, in the hands of a truly skilled operator. It should not be regarded as a determinant of guilt or innocence or proof of any person's trustworthiness or untrustworthiness without collateral indications from more through investigations.

When I was the CIA station chief during the final years of the American official presence in Cambodia, we badly needed more penetrations, meaning indigenous spies working for us inside the communist Khmer Rouge. I asked my case officers, a talented lot, to make this their priority. With time, we began to acquire likely looking assets who gave us the mouth-watering intelligence which we eagerly sought. I resisted my own temptations and pressure from our recruiters to immediately disseminate this agent product as valid intelligence. I insisted on waiting until I could arrange to get newly recruited "assets" on the polygraph.

CIA sent out its most skilled operator who questioned the "assets" for as long as an entire night each with the help of the polygraph. In many, but not all cases, the would-be agents eventually were persuaded to admit that they were controlled and had been sent to us by the Khmer Rouge. The details they provided us of their missions, when compared to information we already had and knew to be valid, gave us valuable counterintelligence insight on what the Khmer Rouge thought we wanted and would believe and about their disinformation meant to deceive us. However, I was impressed that the polygraph is only one tool and its results alone were not proof of anything. That is why I am supportive of stringent investigative procedures and controls rather than to continue over-reliance only on polygraph "examinations," while I support continuing use of the polygraph as one investigative tool.

Lastly, I feel obliged to inject a warning, again from my experiences particularly in operations work abroad, concerning the risks involved in effect in taking the foreign counterintelligence function away from CIA. This would damage U.S. spy recruitment abroad. I assert that most leads on treason cases originate from CIA's foreign intelligence operations. Foreign liaison services and defectors give CIA leads or invaluable indications when American secrets have come into hostile hands.

To help make my point, I recall at least a couple of instances involving our cooperation with European liaison services targeted at high priority nuclear and arms proliferators. In both cases our joint efforts were progressing nicely until suddenly our foreign collaborators came to believe our cooperation, by U.S. law, would have to be briefed to U.S. authorities outside of CIA, and that leaks could occur which would severely embarass our foreign friends. I had a devil of a time persuading our friends, for example, that the oversight responsibility in the United States involved only quite small committees, the members of which could be trusted to keep our secrets. In other cases of agent recruitment attempts, potential recruited agents have turned us down because "Americans cannot keep secrets" and "American laws make it difficult for CIA to protect secrets."

Protection of sources is fundamental to CIA operations. CIA collects and analyzes information in order to advise the President and Congress on issues of national security. Protection of sources and methods has always been one of the DCI's primary responsibilities. Naturally, the FBI, as a law enforcement service, is determined to detect criminal behavior and to prosecute individuals. Protection of sources is necessarily secondary. When an effective prosecution requires the use of evidence that may have been collected by covert sources, and that evidence becomes public from courtroom or other use, those covert sources are at risk as is their utility as future sources of important information. That then damages CIA's ability to recruit and keep agents, and to obtain cooperation from foreign liaison sources.

CIA must maintain its ability to keep entirely secret its sources and methods for collecting counterintelligence abroad, whereas it can safely share the product of its counterintelligence operations only if sources or methods are not compromised by so doing. In cases when there is doubt about this it seems wise that CIA conduct the counterintelligence investigations without risking valuable sources by being forced to disclose them outside CIA. Sources must be carefully protected lest they dry up.

TESTIMONY OF DAVID D. WHIPPLE

Mr. WHIPPLE. I am afraid that I am going to find myself way out of step with my colleagues in things I have to say to you this afternoon.

My comments are based on my own personal experiences. I was, for 35 years, an operations officer in the CIA. Most of those years were served on 2- to 4-year postings abroad in Southeast Asia, Africa, and Europe, or shorter postings in Asia and the Middle East and Europe.

Of my 10 more permanent posts, I was station chief in five countries and deputy chief in three others. I ended my career in 1985, working directly for the DCI as the first National Intelligence Officer for Counterterrorism.

When I joined CIA in 1950, I assumed that because I was to occupy positions of great trust, somebody was always, or occasionally, going to be looking over my shoulder, with or without my knowledge. I think I would have been disappointed if I believed CIA was less than majorly concerned with my security-related behavior. I understand that CIA's management today believes that while those working in intelligence organizations freely compromise aspects of their privacy to satisfy security needs, they do so with faith that fundamental rights, including due process, will not be compromised. Constitutional guarantees must be considered against the need for intrusion on individual rights in the interests of national security.

I think that is all well and good with respect to citizens who are not intelligence people. However, I take a more extreme view. I believe that once one signs on as an intelligence employee, he or she should be required to waive certain constitutional guarantees and rights. He should expect to be treated differently from ordinary people in the interests of national security broadly or narrowly defined.

I do applaud the provisions I see in the draft bills, but suggest that these provisions be even more stringent, and a lot less concerned with, "fairness."

Second, I note that one of the bills—Senator Cohen's and Senator Boren's—refers to periodic polygraph examinations. The last word, examinations, suggests to me a misunderstanding, widely shared by the American news media, of what the polygraph process can and cannot do. I have had a good deal of experience with the use of the polygraph and polygraph operators abroad, in agent operations. The polygraph can be a very useful investigative tool, but only a tool, in the hands of a truly skilled operator. It should not be regarded as a determinant of guilt or innocence or proof of any person's trustworthiness or untrustworthiness, without collateral indications from more thorough investigations.

When I was a CIA station chief during the final years of the American official presence in Cambodia, we badly needed more penetrations, including indigenous spies working for us inside the communist Khmer Rouge. I asked my case officers, who were a talented lot, to make this their priority. With time, we began to acquire likely looking assets who gave us the mouth-watering intelligence which we eagerly sought.

I resisted my own temptations and pressures from our recruiters to immediately disseminate this agent product as valid intelligence. I insisted instead on waiting until I could get newly recruited, "assets," on the polygraph. CIA sent out its most skilled operator who questioned the assets for as long as an entire night, each with the

help of the polygraph. In many, but not all cases, the would-be agents eventually were persuaded to admit that they were controlled and had been sent to us by the Khmer Rouge.

The details they provided us of their missions, when compared to information we already had and knew to be valid, gave us valuable counterintelligence insight on what the Khmer Rouge thought we wanted and would beiieve, and about their disinformation meant to deceive us. However, I was impressed that the polygraph is only one tool and its results alone are not proof of anything. That is why I am supportive of stringent investigative procedures and controls rather than to continue over-reliance only on polygraph examinations., while I support continuing use of the polygraph as one investigative tool.

Lastly, I feel obliged to inject a warning, again from my own experiences, particularly in operations work abroad, concerning the risks involved in effect in taking the foreign counterintelligence function away from CIA. I am talking about the foreign counterintelligence function. This would damage U.S. spy recruitment abroad. I assert that most leads on treason cases originate from CIA's foreign intelligence operations. Foreign liaison services and defectors give CIA leads or invaluable indications when American secrets have come into hostile hands.

To help me make my point, I recall at least a couple of instances during—involving our cooperation with European liaison services targeted at high-priority nuclear and arms proliferators. In both cases, our joint efforts were progressing nicely until suddenly our foreign collaborators came to believe our cooperation by U.S. law would have to be briefed to U.S. authorities outside of the CIA, and that leaks could occur which would severely embarrass our foreign friends. I had a devil of a time persuading our friends, for example, that the oversight responsibility in the United States involved only quite small committees, the members of which could be trusted to keep our secrets. In other cases of agent recruitment attempts, potential recruited agents have turned us down because Americans cannot keep secrets and because American laws make it difficult for CIA to protect secrets.

Protection of sources is fundamental to CIA operations. CIA collects and analyzes information in order to advise the President and Congress on issues of national security. Protection of sources and methods has always been one of the DCI's primary responsibilities. Naturally, the FBI, as a law enforcement service, is determined to detect criminal activity, and to prosecute individuals. Protection of sources is necessarily secondary. When effective prosecution requires the use of evidence which may have been collected by covert sources, and that evidence becomes public from courtroom or other use, these covert sources are at risk, as is their utility as future sources of important information. That then damages CIA's ability to recruit and keep agents and to obtain cooperation from foreign liaison services.

CIA must maintain its ability to keep entirely secret its sources and methods for collecting counterintelligence abroad, whereas it can safely share the product of its counterintelligence operations only if sources and methods are not compromised by so doing. In cases where there is doubt about this, it seems wise that CIA con-

duct the counterintelligence investigations without risking valuable sources by being forced to disclose them outside CIA. Sources must be carefully protected lest they dry up.

Chairman DECONCINI. Thank you, Mr. Whipple.

I have just a couple of questions. I would like to ask Mr. Kohler, you raised some very good points on the amount of bureaucracy and paperwork. What if legislation did one of two things, or maybe both. One is made available your records of your employees to the investigative branch here of the CIA, or for that matter—I mean the FBI, or for that matter if the CIA wanted to come look at the employees that had top secret or secret clearance, and you didn't have to do anything but whatever you keep there, just make it available to them. Would that be too much of an interference.

Mr. KOHLER. Let's see. I think that employees of companies like mine who already have clearances already go through intensive investigations.

Chairman DECONCINI. Yes, I know.

Mr. KOHLER. And in many cases, investigations are the same as Government employees go through. Forms that are some 40 pages long that have to be filled out. Many of us, the 7,000 or so that I talked about at my company, take polygraph examinations.

Chairman DECONCINI. Well, that's not my point. My point is what if the law said that upon a proper certification from the Agency, CIA or FBI, to you, that they wanted to look at employee X's financial reports that they file with you, and to look at it without advising that employee. Would that be a——

Mr. KOHLER. It would be inadequate for you, because companies do not maintain detailed financial records of their employees. We know what we pay them, but that's about all. They don't know about stock transactions or anything like that.

Chairman DECONCINI. But what if the request for you to fill out all of this by the employees or the employees, if that was filled out or if—let me put it this way, if when an employee who is going to work on a Government contract, if they signed a statement that said, I am waiving my right during this period of time that I am going to be employed in this sensitive contract area, from the standpoint of the Government investigating and pursuing economic interests they may have, would that pose any problem to you, just by that alone?

Mr. KOHLER. Senator, Mr. Chairman, this is an extraordinarily complex situation. I—what I was trying to say in my testimony is first of all, there's a lot of us contractors out there.

Chairman DECONCINI. Yes.

Mr. KOHLER. And we don't need to overwhelm the Government with any more information. It already takes an incredible long period of time to get clearances through the contractor world, and it costs you a lot of money in this Committee to do that, because of the investigative process.

What bothers me, I guess, more than anything else, is two things. One, a really good spy is going to hide the financial data anyway. That's one observation.

Chairman DECONCINI. But my point is, yeah, and you may be right, but if you have 7,000 employees working on classified information with the Government——

Mr. KOHLER. Yes.

Chairman DECONCINI [continuing]. Consented, if the Government wanted to, as part of their clearance process, they signed a waiver or whatever you want to call it, would that pose a problem in and of itself? It may not catch the spies. I am not sure it does. It may not even be a deterrent.

Mr. KOHLER. In and of itself——

Chairman DECONCINI. My question is, does it pose a problem for industry?

Mr. KOHLER. In and of itself it doesn't pose a problem. I would only—I think anything that you ask people to do for something as sensitive as intelligence, where they get a chance to decide ahead of time, that I will do it or I won't do it, is a reasonable request. I don't have any problem with that.

Chairman DECONCINI. Well, thank you.

Now, Ms. Martin, you have a problem with that. If, as a precondition of employment or a precondition in this case of being—your being certified for classified information, that you would agree that your financial records may be disclosed and looked at without your knowledge.

Ms. MARTIN. We think that some employees can be asked to waive their rights in advance.

Chairman DECONCINI. And how do you distinguish that? Where do you draw that line?

Ms. MARTIN. One of the ways is according to what kind of information they have access to, either top secret or critically sensitive——

Chairman DECONCINI. Yes. Critically sensitive, top secret material. If people in Mr. Kohler's organization, those that are dealing with a very classified, top secret program, if they had presented to them such a waiver, or they would not be granted permission to work on this contract or be given the status necessary, how does that come out to you?

Ms. MARTIN. That is acceptable to us as long as the Government only looks at those records without giving notice to the employee when it has a reasonable suspicion that that employee is——

Chairman DECONCINI. From your standpoint, giving the waiver is OK as long as there is another step that the Government would go to to reasonable suspicion or something.

Ms. MARTIN. Yes.

Chairman DECONCINI. So that they would do that before they just perhaps willy nilly go look at 7,000 employee's records.

Ms. MARTIN. Yes. Which I assume would help the administrative problem as well.

Chairman DECONCINI. Sure. That's a good point.

Mr. KOHLER. Mr. Chairman, could I just help here just a minute.

Chairman DECONCINI. Yes.

Mr. KOHLER. There are things that the Government does, the intelligence agencies do, and there are things that we, as contractors help them do, where people's lives are at risk, and if the operation fails, somebody dies. Those things, I have absolutely no problem.

Chairman DECONCINI. Well, yes, but the problem, Mr. Kohler, it seems to me, you can't tell, see, you don't know whether or——

Mr. KOHLER. No. We know what those programs are.

Chairman DECONCINI. I mean, do you really know what those programs are, that somebody is going to die if they let them——

Mr. KOHLER. No, I didn't say they were going to, but I am saying—I make a distinction——

Chairman DECONCINI. They could die or something.

Mr. KOHLER [continuing]. Where you put somebody's life at risk versus somebody reading a report in Washington. I think there is a way to come to grips with what are the truly classified, sensitive intelligence operations and information of the U.S. Government.

Chairman DECONCINI. Mr. Whipple, let me just pursue one thing with you. You said you were opposed to turning over the foreign part of counterespionage to the FBI.

Mr. WHIPPLE. Yes. Which seemed to me——

Chairman DECONCINI. Now, that's not the intent of the legislation that Senator Warner and I, in S. 1948, put in. Let me read it to you. It says, the Director of the Federal Bureau of Investigation shall have overall responsibility for the conduct of counterintelligence and law enforcement investigations involving persons in critical intelligence positions.

Maybe that does say they take it over. But what it is meant to say is that somebody is going to have overall responsibility, not that they are going to take it away from the CIA or invade those sources or something, but when it comes down to an Ames case, they are going to be able to get in earlier if they want to, and in fact, the CIA would be required to get them in earlier than they did in this case that we know now.

Is that offensive or is that going too far?

Mr. WHIPPLE. I don't—it's apples and oranges. Because the Ames case would be domestic counterintelligence, which is clearly an FBI thing. What I am talking about is the exploitation of sources abroad under the control of——

Chairman DECONCINI. All right, fair enough. Let's stick to the overseas area. But in the case of Ames, he was in Rome and some publications that indicated he may have disclosed some information then, he may have had some contacts then. Having overall responsibility with the FBI, is that a problem?

Mr. WHIPPLE. No, it wouldn't be a problem.

Chairman DECONCINI. Wouldn't be a problem.

Mr. WHIPPLE. Because he—there should have been other indications that he was under suspicion, or he should have been under suspicion.

Chairman DECONCINI. Sooner?

Mr. WHIPPLE. Therefore, it would have been a domestic——

Chairman DECONCINI. My purpose for this 807 is to get the Agency, as you may have heard this morning, particularly the operations people that this information first comes into play usually, I am told, to get them to turn it over sooner to the FBI, either through the CI or directly or what have you. And I am not wedded to this. What I am trying to do is establish some way to get that done. You know better than I do, and correct me, that there is often a reluctance to bring in the FBI until you really have a target, until you're really sure.

Just the fact that Mr. Redmond may have made—and I use this hypothetically because it is only from the Post that I have picked

it up—may have made a statement to his superiors that wherever Ames went, there was a problem. To me, that's enough for somebody to say, my God, let's have somebody look at this from an investigative point of view, perhaps outside the Agency. We've got a problem that this superior of Ames thinks that every place he has been there has been a problem.

Had that happened, they would have turned that over to the FBI in 1989. They didn't do it. Now, my question to you is, do you know how to get that accomplished within the CIA?

Mr. WHIPPLE. Yes, I think so.

Chairman DECONCINI. And do you need legislation to do it?

Mr. WHIPPLE. I am going to dodge that, because that isn't my particular province. I think that Executive order that they talked about this morning would do it, given good will on both sides. And I know you are reluctant to say that you depend on good will.

Chairman DECONCINI. Well, I agree with you. Good will, you know, really is how it happens, even if you have a law, it takes good will. But given good will and an Executive order and then given non-good will and an Executive order, and non-compliance, are we better off with legislation and non-compliance, or are we better off with an Executive order and non-compliance, if in fact it is not going to happen. Do you think that makes any difference?

Mr. WHIPPLE. I would like to think we didn't have to have non-compliance.

Chairman DECONCINI. Well, I would, too. But in fact, it is so clearly pointed out in the 1988 MOU, the last one, as well as 10 other efforts during the period of time certainly didn't bring this cooperation to what the good will, as expressed by Mr. Freeh and Mr. Woolsey, is today.

Mr. WHIPPLE. Well, I don't have to remind you that the problem is that you have got FBI concerned with prosecution, you have CIA concerned with collection. And you are always going to have a sometimes healthy little conflict there.

No, I don't have any difficulty in the things you have said.

Also, as pertains to the Ames case, I don't see that this is—I am looking at the whole thing from the outside looking in, whereas you are looking from the inside looking out.

Chairman DECONCINI. Well, I appreciate your effort and comments on the suggestions here, and I don't want to overkill this thing and drive it into the ground, but I sure hate to miss an opportunity, because I'm concerned it is going to take another crisis for us to once again be here. And it is easy for the Ames case to be bled out and now we move on to something else, and then the next big spy case, pretty soon there'll be other legislation, there may be another administration come in and they'll say, well, let's just try another MOU or another Executive order.

I yield to the Senator.

Vice Chairman WARNER. Mr. Whipple, let me just pick up on the line of questioning of the Chairman. And your participation here today is very important to this hearing. We thank you for coming. And also you have been on a number of the media discussions on this and I have followed those with great interest and I think you have handled yourself very well.

Your historical perspective of this great Agency—and the CIA has been a tremendous Agency throughout its lifetime, and 99.9 percent of the people who have given their lives and careers for that great Agency deserve enormous gratitude from the American people.

Mr. WHIPPLE. Thank you, Senator.

Vice Chairman WARNER. But let us—this phrase comes up from time to time, particularly in this debate on whether FBI should have the authority, CIA retain it, now the dual horse concept of the administration, let's, you know, give them both co-equal, but rotate the chairs and so forth and so on, what about this phrase, it's a different culture in these two agencies. What do they mean by that, in your judgment? Or do you agree with it?

Mr. WHIPPLE. I don't really agree, but I realize that there is a slightly different culture. Traditionally there was a very different culture. That difference is disappearing in the modern day to my knowledge. And I——

Vice Chairman WARNER. Describe the culture difference as you knew it in the early part of your career, and how it has given away today.

Mr. WHIPPLE. FBI were more apt to be, "blue collar, down-to-earth, practical," directly spoken people. In the early days of CIA, CIA was apt to be a little more intellectual, a little more——

Vice Chairman WARNER. Ivy League?

Mr. WHIPPLE. I hesitate to say that. In the beginning, I think that would be quite fair.

Vice Chairman WARNER. I remember it well in the 1950's. I date back to your time getting started with our first job, mine 1949, your's, 1950. I remember the former days of the CIA very well, and the young, my generation that came to join that agency. They were predominately out of the Northeast schools of the larger universities and colleges, in sharp contrast to those who went into the FBI. I don't mean to denigrate certainly the FBI—they have superb people—but they were different, from different backgrounds and oftentimes in the old days the FBI hired really only two categories, accountants and lawyers. Whereas the Agency, a broad spectrum, history, all kinds of backgrounds.

Mr. WHIPPLE. But later on—later on it became a little bit of a detriment to have been Ivy League. I found myself——

Vice Chairman WARNER. Well, in other words, I think we agree on that, but you are coming down to the important point, does that difference of culture, in your opinion, exist today?

Mr. WHIPPLE. No, I don't think to the same extent at all. I find in my dealings—I am dealing with ex-FBI people and sometimes with active FBI people all the time, and I find them almost completely, totally understandable, that they are like me, they are like us.

Vice Chairman WARNER. Good.

Mr. WHIPPLE. There isn't that much difference now.

So I think there is usually——

Vice Chairman WARNER. And I share that view.

How do you feel that the consent approach that we have been discussing—and I will shortly bring up again with Ms. Martin—do you think the young persons coming into the Agency today or the

careerists presently serving would be reluctant to sign a consent form?

Mr. WHIPPLE. I was astonished to hear you discussing that this morning. I don't think that's an issue at all. I agree with what I believe Director Woolsey said. I don't think that is going to affect—people are very anxious, youngsters are very anxious to join CIA right now, for instance. And if you had stringent rules like I recommended and they had to sign away some of their civil rights, which would be very offensive to a lot of people I think here, but if they had to, I think the people would readily do that. And I think they would understand the reason for that.

Vice Chairman WARNER. And I share your view on that also.

Mr. Kohler, let's turn for a minute, let's assume this simple pad of paper is a set of drawings for the latest satellite for the United States, and your company, with which I have had association for practically a quarter of a century now, is known preeminently worldwide for its building of satellite systems, so that here is a set of plans. They are in the possession of the Federal Government, say the Department of Defense, they are in the possession of TRW. Should the rules and regulations regarding the handling of these sets of plans be any different in private industry versus the Government?

Mr. KOHLER. Absolutely not.

Vice Chairman WARNER. Therefore, should the treatment of the people in Government with respect to the rules and regulations governing their personal conduct, which we're now considering in this bill, be any different?

Mr. KOHLER. Yes.

Vice Chairman WARNER. Why?

Mr. KOHLER. Because people in Government have access to more classified information than we do in the private sector. When I was the—you know, Senator, I was in the satellite building business when I was in CIA, and as an office director I knew a lot about what went on in the Operations Directorate, I knew a lot what went on in the Intelligence Directorate. We interacted daily with the people in the Intelligence Directorate.

Vice Chairman WARNER. I'll concede that you probably had a broader knowledge.

Mr. KOHLER. Industry doesn't have that kind of insight. It simply does not have that kind of insight.

Vice Chairman WARNER. All right. But if I am a Russian spy and I want these plans, it makes no difference to me whether I get that set of plans from the Government or TRW, because they're identical.

Mr. KOHLER. Absolutely right.

Vice Chairman WARNER. So then why should I consider that the—or I, or I should say the Senate, consider the rules and regulations regarding the private sector be any different, because the end product is what the Russians or other countries want.

Mr. KOHLER. If the Government decided that those plans were of very high national importance to national security, then I would have no trouble with the contractors being treated the same as the Government people.

I just—I really resonate, however, with Senator Boren, when he says be careful about casting a net over millions, which there are elements of that in the bill which I was trying to address. I would rather see us truly protect stuff which is important.

And in that context, I have no problem with—when I went to work for CIA, I gave up a bunch of my civil rights. I signed a whole bunch of pieces of paper that gave up civil rights. I have no problem with that, as long as people get to make that decision.

And I think in industry, most of our people who work on these programs, if they understood it was truly important, would agree to the kinds of things you are talking about. I just urge you not to blanket us and make it apply to millions of people.

Vice Chairman WARNER. I think that's a fair contribution, yes, not to blanket. But as far as this set of plans are concerned, they are just as vital to those who want them, and they don't care from which source they get them.

Mr. KOHLER. Sure; that's correct.

Vice Chairman WARNER. And therefore, in my judgment, you have to have equality of treatment, Government and private sector.

Ms. Martin, this consent the Chairman started on this line of questioning and I want to pick up on it, because it—I must say that I am very much taken with your concept of having some reasonable standard, and I am going back to that one. But let's talk about the consent.

If employees, by virtue of a condition of their employment, signed a very comprehensive consent statement, would that not be a basis for eliminating a number of the concerns you have raised today as to the invasion of their personal rights or constitutional rights or however you want to characterize it?

Ms. MARTIN. If it was coupled with a requirement that the circumstances under which the documents are going to be looked at is limited, it would. Although, I must say that I think it is a legal fiction to talk about employees consenting when they are waiving their rights. There are certainly situations where people feel that the only place that they can pursue their chosen professions is in the intelligence community, and so in order to do what they want to do, they have to give up their civil liberties.

Vice Chairman WARNER. I operate on the premise—it's been my experience, and I have dealt, as I say, with this community for a quarter of a century—an individual who is qualified to work at the Central Intelligence Agency or NSA or whatever, believe me, that individual can go out and find comparable or perhaps more remunerative employment elsewhere. They are very highly-qualified individuals and highly-skilled. So they are making a determination that they wish to serve their country and they recognize that what they do has to be protected, not only in terms of the security of the country, but the lives of men and women of the armed forces, of men and women of their respective agencies, on the front line around the world.

So I think they can approach the question of consent, as I characterize it, or if you wish to have the term waiver, in a very intelligent and informed way. And if they give, it and it seems to me it just about removes many of the concerns that you raise here today.

Ms. MARTIN. One of the reasons why we think that it is acceptable, actually, is that we believe that the focus on financial and travel information in security clearance determinations is the correct focus.

As you are aware, I am sure, in the past there has been a focus on a lot of extraneous and private information—ideological bents, for example. There is still, I believe, in some of the agencies, a practice of asking questions about extremely private kinds of things like divorce counseling or other kinds of consultations with mental health professionals, having nothing to do with any kind of mental illness, which questions are over broad and completely unrelated to any legitimate security concerns.

The kind of information that is being talked about in these bills is the most relevant information that exists as to whether or not a person is liable to engage in espionage.

Vice Chairman WARNER. Fine. But let's come back to my question, if I may politely ask you to address it once again. If we were to put in a requirement to give waiver or consent, would that not then meet your concerns on almost every point you've raised today?

Ms. MARTIN. If it was coupled with two things.

Vice Chairman WARNER. All right, let's—go ahead, coupled with?

Ms. MARTIN. With first, the reasonable suspicion standard for looking at the documents.

Vice Chairman WARNER. Right.

Ms. MARTIN. And second, if it was limited to the period of time in which the employee had access to classified information.

Vice Chairman WARNER. I think those are valid points.

Let's take first this reasonable basis doctrine that you have.

You raised your hand, Mr. Whipple? Let me finish with this line and I will certainly invite you to respond.

We have this doctrine firmly imbedded in the law with regard to search warrants. And there they have to be issued by a recognized judicial authority—judge, magistrate, or whatever the case may be. I am not sure what we could institute within these intelligence agencies that give the same measure of protection as this third party, presumably totally objective judicial or quasi-judicial person out here rendering that judgment. How do we meet that?

Ms. MARTIN. Well, we wouldn't require a third——

Vice Chairman WARNER. You what?

Ms. MARTIN. We would not require a third party outside the executive branch. What we would require would be a written certification by an executive branch official that the reasonable basis existed, so that somebody has the responsibility for writing down we have a reasonable suspicion.

Vice Chairman WARNER. OK, you're going to have to refine that, I think, because the executive branch is everybody from the person who is down in the cafeteria all the way up to the head of the CIA, so that won't do it. It has got to be a certain grade or a certain position. In other words, it seems to me you have got to define those individuals who would be entrusted with making this decision. How would you describe them? Because if there is an investigator in the counterintelligence division who is on an investigation, he or she is bound to be somewhat prejudiced, say let's go ahead and sign it, we've got to sign a little form, let's sign it.

Ms. MARTIN. Well——

Vice Chairman WARNER. I don't see how we're going to bring the objectivity in to add some stature to this procedural step.

Ms. MARTIN. I think that one——

Vice Chairman WARNER. You may have to think through it and come back to the Committee.

Ms. MARTIN. Although I might mention, the administration's bill I think provides that the department or agency head or deputy department or agency head has to make the certification. I am not completely certain that is what the bill——

Vice Chairman WARNER. Well, why don't you examine that, because——

Ms. MARTIN. And that would certainly be a sufficient certification by someone at that level.

Vice Chairman WARNER. I see your colleague in the back might have an idea.

VOICE. That's right, the head of the Agency.

Ms. MARTIN. Or the deputy head.

Vice Chairman WARNER. Or someone designed in a position to give it some objectivity, I would presume.

Ms. MARTIN. It's really a question of accountability as well, that there be a person who is accountable for having made that decision.

Vice Chairman WARNER. Yes.

Now, your concerns—and it's a very good presentation that you had today—are they based more on philosophical approaches to this balance between one's personal or constitutional rights, or is it based upon an interpretation of existing law or the likely interpretation of, say, one of our provisions by a court of law?

Ms. MARTIN. Well, it is based on two things. It is based on our view of what the Constitution and the Bill of Rights requires. That view, as I am sure the Senator knows, is not always the view that is accepted by the courts. And second, it is based on our experience in looking at national security and civil liberties problems over the past 20 years, and trying to come up with solutions which address real national security concerns and are the least restrictive means for—with regards to civil liberties problems.

Vice Chairman WARNER. Well, your organization has had a very long and distinguished record trying to balance these rights in many, many areas of law. And therefore, your contribution to this Committee today will be carefully considered. I think I understand your answer now. It is based on experience in other areas that you bring to this particular area.

How widespread, within your organization, was this discussed, this testimony today?

Ms. MARTIN. It was discussed and reviewed by the persons who work specifically on national security and civil liberties, and the other people in the Washington office of the ACLU. Most of the positions that we have talked about here today are positions that we have taken over the past 5 or 10 years, and grow out of those positions. So there was in fact, no position that was especially difficult for us to adopt in terms of presenting a new policy problem.

Vice Chairman WARNER. Let me go back then to your response on the question of consent. You said, if we have consent, it is likely

to meet our objectives with two conditions. Condition number one is reasonable test. Condition number two is no post employment restrictions whatsoever. And that would cover everything? In other words, once an employee departs the Agency, it totally severs all the relationships in terms of investigation, absent the existing body of criminal law?

Ms. MARTIN. Once the employee departs the Agency, then the FBI can conduct an investigation of him or her in the same way——

Vice Chairman WARNER. Through existing law?

Ms. MARTIN. Yes. In the same way that it conducts an investigation of anyone else for any other possible crime.

Vice Chairman WARNER. Supposing we incorporated in the consent, then, a reasonable period of time. And I am not sure whether it is 1 year, 10 years—someone who is in the enforcement business will have to give us the expert advice—a period of time in the consent. Would that be agreeable?

Ms. MARTIN. A period of time after they leave the——

Vice Chairman WARNER. That's correct.

Ms. MARTIN. We basically object to that. We think that once you are no longer talking about investigating a person who is currently working inside an agency—so that you have this problem of dealing with somebody who may not be a spy, and somehow you want to investigate them but not let them know that they are the target and not compromise their work—you have the kind of a criminal investigation that you have with regard to all crimes, and that the fourth amendment should apply in that situation.

Vice Chairman WARNER. All right. We'll have to study this further.

I want to return to my last questions to Mr. Kohler.

Mr. Kohler, your testimony today, if you said it I missed it, but do you speak for the industry or just TRW or yourself?

Mr. KOHLER. I was asked to come today as a representative of the Security Affairs Support Association——

Vice Chairman WARNER. Wait a minute, hold it, go slowly. As a representative of?

Mr. KOHLER. Security Affairs Support Association, which is an association which consists of both industry that supports the intelligence community as well as active members of the intelligence community.

Vice Chairman WARNER. Were your views circulated beforehand so——

Mr. KOHLER. Yes; yes.

Vice Chairman WARNER [continuing]. It does represent a consensus of those persons entrusted——

Mr. KOHLER. Yes.

Vice Chairman WARNER [continuing]. With trying to communicate with the Congress.

Mr. KOHLER. Yes, sir.

Vice Chairman WARNER. Well, that's very helpful.

Therefore, if we need to get further views, we would come back to you and you would then circulate our questions amongst your peer group and come back and respond?

Mr. KOHLER. Yes, sir. I am a member of the board of directors of that organization, so I can easily do that.

Vice Chairman WARNER. Mr. Whipple, in your group, are there other groups comparable to yours that you suggest we try and get their views?

Mr. WHIPPLE. Yes. There are many, many groups similar to ours. There is a military organization, NMIA. There is the—there is a fraternal organization from CIA which is purely fraternal, social, called CIAR, Central Intelligence Agency Retirees, and you might want to talk to them. They are all, admittedly, CIA people, whereas the association I represent——

Vice Chairman WARNER. Well, I wonder if you would be helpful to the Committee by just making some contacts yourself and then informing the Committee if you know of a person who wants to speak on behalf of an organizational point of view, and then subject to our time, or perhaps we could take it in written form, we could avail ourselves of their contribution.

Mr. WHIPPLE. All right, and I will do that through Britt Snider.

Vice Chairman WARNER. Indeed. That would be fine.

Mr. KOHLER. Senator——

Vice Chairman WARNER. Yes.

Mr. KOHLER. Can I make one more comment on who I represent? The comments I made about TRW and the credit business, we also coordinated those with the Credit Industry Association, so those were also comments that were from the industry, not from TRW.

Vice Chairman WARNER. Mr. Whipple, was there further testimony you wanted to provide on a point?

Mr. WHIPPLE. I wanted to make one point, if I might.

Vice Chairman WARNER. You've made several, and we're glad to have an additional.

Mr. WHIPPLE. Well, this is—it seems to me that this hearing and your efforts to devise legislation is all based on one objective, and that is to prevent or to make it unlikely that we will not have another Ames-like penetration of one of our sensitive intelligence services. If that's true, then it seems to me that the most important thing that people ought to be focusing on, it seems to me, is monitoring the ability, the legislative right of intelligence organizations without—these are the things—without any notification of the individual, without reason to monitor their behavior, so that we prevent people getting into trouble, being tempted to be getting into trouble before they do. If the agencies had the right, in effect, to watch carefully, short of investigation, or to continue with an investigation if they saw a little bit of evidence, we would have avoided an awful lot of the difficulties we ran into on the Ames case.

I don't think it is any secret to the outside world that when a CIA station chief goes abroad, he is instructed—and we all have experience in this—to in effect, pay particular attention to the private, family, and every other form of life of all of our people. We are, in effect, responsible for the behavior, personal, private and everything else, of all the people in our stations. This prevents things happening in many stations.

This is where you got—you referred, I think you, sir, referred today to Mr. Redmond in the Rome station. That was a good point

well taken, because he, in effect, did notice these things and did pay—now whether they paid attention to him or not, no, they were not. It seems to me that if the legislation allowed the intelligence agencies then to pay attention to their people, and then on a spot basis or on a comprehensive basis, whatever is practical, and then go after an investigation if such a thing were called upon, you wouldn't need a justification, you wouldn't need to have a reason why you are picking up this bit of suspicion going on. But this way we would be in better shape to know what we are up against.

Vice Chairman WARNER. I thank you very much.

I thank each of you. This has been an excellent hearing, throughout the day, and all three panels have made substantial contributions. The Chairman and I have had our own private discussion. The bottom line is we have really cut out the work for the two of us for the future. We have learned much, we still have much to learn, and we thank you very much.

[Thereupon, at 3:47 p.m., the hearing was concluded:]

UNITED STATES SENATE,
Washington, DC, May 13, 1994.

Hon. DENNIS DECONCINI,
Chairman, Select Committee on Intelligence,
United States Senate, Washington, DC.

DEAR MR. CHAIRMAN: Enclosed is a letter I recently sent to David Whipple regarding his testimony last week to the Intelligence Committee.

Because it clarifies a point he focused on in his testimony, I would ask that my letter and the accompanying enclosure be incorporated into the record of the hearing following his testimony.

Thank you for your consideration.

With best wishes, I am

Sincerely,

WILLIAM S. COHEN,
United States Senator.

Enclosure

UNITED STATES SENATE,
Washington, DC, May 12, 1994.

Mr. DAVID D. WHIPPLE,
Association of Former Intelligence Officers,
McLean, Virginia.

DEAR MR. WHIPPLE: I have just had an opportunity to review your prepared testimony for last week's Intelligence Committee hearing.

In discussing section 3 of S. 1869, you raise an important matter regarding the degree to which reliance should be placed on polygraph results. I wholeheartedly share your view that we should not over-rely upon polygraph results, which should be used as only one of many tools employed in tandem.

That is, in fact, one reason that Senator Boren and I chose to use the term "polygraph examination" in our bill. The commonly used term "polygraph test" can convey the impression that a person either fails or passes a "test." This being quite misleading, we chose instead to use the more neutral term "examination," which refers to detailed observation or questioning without implying a simple pass or failure.

We also took pains to ensure that our bill would not lead to action against a person based solely on the results of a polygraph examination. Section 3 of S. 1869 clearly states:

> No person shall be removed from access to cryptographic information or spaces based solely upon the interpretation of the results produced by a polygraph instrument, unless, after further investigation, the head of the department or agency concerned determines the risk to the national secu-

rity in permitting such access to be so potentially grave that access must nonetheless be denied.

In addition, the detailed section-by-section analysis of our bill, which has been associated with it as legislative history since it was first introduced in 1990, explicitly states that:

> . . . interpretation of polygraph results should not be the sole basis for denial of access to classified cryptographic information or spaces. (The Congress) intends that where the results of such examinations do indicate lying or deception to key counterintelligence questions, that these discrepancies be resolved, where possible, through interviews with the subject and such further investigation as may be warranted. If such further investigation does not provide an independent basis for removal from access, such access should be granted or maintained unless the head of the department or agency concerned determines, in view of all the circumstances involved and the potentially grave threat to the national security, that access should not be permitted.

A copy of the relevant excerpt from this section-by-section analysis is attached.

I believe that this is fully consistent with your testimony that the results of a polygraph examination "should not be regarded as a determinant of guilt or innocence or proof of any person's trustworthiness or untrustworthiness without collateral indications from more thorough investigations."

I appreciate having the benefit of your testimony to the Intelligence Committee.

With best wishes, I am

Sincerely,

WILLIAM S. COHEN,
United States Senator.

Enclosure

SECTION 3

Section 3 of the bill adds a new title IX to the National Security Act of 1947 (50 U.S.C. 401 et seq.) to provide special requirements for the protection of cryptographic information. Persons with access to such information necessarily have the capability of inflicting grave damage upon the national security by enabling unauthorized persons to read or understand an unlimited number of U.S. communications at all levels of classification. In view of the peculiar sensitivity of such information, the Congress believes that special security measures should be imposed on persons who have access to this information.

It is the intent of the Congress, however, that only those executive branch employees or contractors who have extensive involvement with, or in-depth knowledge of, classified cryptographic information need to be covered by the proposed title. This would include persons who develop U.S. codes or ciphers, persons who build or install devices or equipment which contain such codes or ciphers, and persons who are employed in locations where large volumes of classified information are processed by such devices or equipment, such as communications centers. It is not intended that persons who have access to cryptographic devices or equipment designed for personal use or office use should be covered by this title.

SECTION 901 establishes minimum uniform security requirements for executive branch employees who are granted access to classified cryptographic information or routine, recurring access to any space in which classified cryptographic key is produced or processed, or is assigned responsibilities as a custodian of classified cryptographic key. The President may provide latitude in the regulations implementing this title for departments and agencies to impose additional, more stringent security measures upon such persons where circumstances may warrant.

Two basic requirements are imposed upon persons covered by the title. Subsection (a)(1)(A) requires that they meet the security requirements established by section 802 of the Act, as persons with access to particularly sensitive information. Thus, persons covered by this title would also be subject to initial background investigations, reinvestigations not less than every 5 years, and unscheduled investigations as appropriate, to ensure they continue to meet the standards for access to classified cryptographic information, regardless of the level of security clearance such persons may otherwise have. They would also be required to provide their consent to the authorized governmental investigative authorities having access to the categories of records set forth in section 802.

Subsection (a)(1)(B) requires that persons covered by this title also be subject to periodic polygraph examinations conducted by appropriate governmental authorities, limited in scope to questions of a counterintelligence nature, during the period of their access to classified cryptographic information. This provision does not require such polygraph examinations for all such persons, but it does make such persons, regardless of the department or agency where they may be employed, subject to such examinations on an unscheduled basis while such access is maintained. In accordance with the implementing regulations required by section 902, it is anticipated that departments and agencies with employees or contractors covered by this title would establish or acquire a sufficient capability to conduct such examinations to maintain a credible deterrent to persons with access to such information.

The Congress also reemphasizes that this section provides for minimum standards. It is not the intent of the provision to restrict the use of the polygraph at the Central Intelligence Agency and National Security Agency, where polygraph examinations are routinely required of all employees and are not limited to questions of a counterintelligence nature.

Subsection 901(a)(2) provides that any refusal to submit to a counterintelligence-scope polygraph examination shall constitute grounds to remove such person from access to classified cryptographic information. It is not intended, however, that such person be subjected to any additional personnel or administrative action, including any adverse action on his or her security clearance, as a result of such refusal.

Moreover, subsection 901(a)(2) goes on to provide that no person shall be removed from access to classified cryptographic information or spaces based solely upon the interpretation of the machine results of a polygraph examination, which measure physiological responses, unless the head of the department or agency concerned determines, after further investigation, that the risk to the national security under the circumstances is so potentially grave that access cannot safely be permitted.

The Congress recognizes that a polygraph examination in essence measures certain physiological responses produced by answers to questions posed to the subject. Such responses might reflect deception on the part of the subject, but they might also reflect other, wholly innocent stimuli, both mental and physical. Indeed, while expert opinion varies in terms of how often the interpretation of polygraph results can be relied upon to show lying or deception, the Congress is aware of no expert who contends that interpretation of polygraph results provides an infallible indication of lying or deception. Accordingly, the Congress believes that an interpretation of polygraph results should not be the sole basis for denial of access to classified cryptographic information or spaces. It intends that where the results of such examinations do indicate lying or deception to key counterintelligence questions, that these discrepancies be resolved, where possible, through interviews with the subject and such further investigation as may be warranted. If such further investigation does not provide an independent basis for removal from access, such access should be granted or maintained unless the head of the department or agency concerned determines, in view of all the circumstances involved and the potentially grave risk to the national security, that access should not be permitted.

Subsection 901(b) sets forth the definitions of the terms used in this section.

Subsection (b)(1) defines the term "classified cryptographic information" as any information classified pursuant to law or Executive order which concerns the details of (A) the nature, preparation, or use of any code, cipher, or cryptographic system of the United States; or (B) the design, construction, use, maintenance, or repair of any cryptographic equipment. The proviso to this definition specifically excludes information concerning the use of cryptographic systems or equipment required for personal or office use.

This term is thus intended to cover classified information which reveals or contains detailed information concerning U.S. codes and cryptographic equipment, to include information concerning the nature and development of such codes or equipment, and the design, construction, use, maintenance or repair of such equipment. ("Cryptographic equipment" is defined in subsection (b)(4) as any device, apparatus, or appliance used by the United States for authenticating communications, or disguising or concealing communications or their meaning.) The definition of "classified cryptographic information" is not intended, however, to cover persons who use cryptographic equipment that has been developed for personal or office use, such as a secure telephone, where such person is not also exposed to detailed information concerning the design, construction, use, maintenance or repair of such equipment. The term is intended to cover individuals, however, who require access to detailed information concerning the use of encoding equipment for other than personal or office use. For example, persons employed at Government communications centers which process large volumes of classified information would be persons who fall within this definition.

Subsection b(2) defines the term "custodian of classified crytographic key" as meaning positions that require access to classified cryptologic key beyond that required to use or operate cryptographic equipment for personal or office use, future editions of such key, or such key used for multiple cryptographic devices. The term "classified cryptographic key", as defined in subsection (b)(3), refers to the information, which may take several forms, needed to set up and periodically change the operations of cryptographic equipment or devices to enable them to communicate in a secure manner.

Similar to the definition of "classified cryptographic information," it is not the intent of the Congress to cover by this definition persons who are custodians of, or otherwise have access to, "classified cryptographic key" for personal or office use. Thus, persons who have access to such key in order to operate a secure telephone located in a single office are not covered by this definition. On the other hand, it is intended that persons who have access to such key in order to operate multiple cryptographic devices or who operate cryptographic devices which are used to process large volumes of classified information originating in multiple locations, such as Government communications centers, would be covered by this definition.

Subsection (b)(5) defines the term "employee" to mean any person who receives a salary or compensation of any kind from a department or agency of the executive branch, or is a contractor or unpaid consultant of such department or agency.

Subsection (b)(6) makes clear that the term "head of a department or agency" refers to the highest official who exercises supervisory control of the employee concerned, and does not include any intermediate supervisory officials who may otherwise qualify as heads of agencies within departments. For example, the Secretary of Defense would constitute the "head of the department" for all employees of the Department of Defense, and not the secretary of a military department or the director of a Defense agency.

Subsection (b)(7) defines the phrase "questions of a counterintelligence nature" as meaning questions specified to the subject of a polygraph examination in advance limited solely to ascertain whether such person is engaged in, or planning, espionage against the United States or knows persons who are so engaged. It is not intended that this definition encompass any question relating to the life-style of the subject, such as his or her sexual orientation, prior or present use of drugs or alcohol, etc. The sole thrust of such questions must be to ascertain whether the subject is acting on behalf of a foreign government, is involved in planning such activities, or knows others who are so engaged.

SECTION 902 of the bill requires the President to issue regulations to implement this title within 180 days of its enactment, and to provide copies of such regulations to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives.

Select Committee on Intelligence,
United States Senate, April 12, 1994.

DEAR COLLEAGUE: Recently, we introduced S. 1948, "The Counterintelligence and Security Enhancements Act of 1994." Joining us as cosponsors of this measure are Senators Graham, Murkowski, D'Amato, Kerrey, Gorton, Bryan, Chafee, Johnston, Boren, and Baucus—all past or current members of the Senate Select Committee on Intelligence (SSCI). We are writing to request your cosponsorship of this important legislation, which we believe will go a long way toward improving the counterintelligence and security posture of the U.S. intelligence community.

Our Committee is particularly concerned about counterintelligence matters in the wake of the Ames espionage case—which could well turn out to be one of the most significant spy cases since the end of World War II. We are determined to address what were obviously serious deficiencies in the security and counterintelligence procedures that led to this incident. For Mr. Ames' alleged espionage activities to have gone on as long as reported represents a serious breakdown in the process.

In the weeks since the arrest of Mr. and Mrs. Ames, the SSCI has been exploring what went wrong and how best to fix it. While the Committee has not completed its inquiry into the Ames case—and the extent to which it is symptomatic of the apparent deficiencies in our nation's counterintelligence capabilities, several points are clear:

First, the CIA and other intelligence agencies actually require little information from their employees which could provide tip-offs to espionage activities. Background investigations are periodically updated, and at the CIA and the NSA, polygraph examinations are required for employees. Once an individual has been hired by the intelligence community, however, there is little additional employee scrutiny.

Second, it is apparent that security elements at the intelligence agencies—as well as the FBI itself—lack the legal authority needed to obtain records from private institutions relating to intelligence community employees. Moreover, some of the authorities the FBI does have—for example, to see tax returns—cannot be exercised until late in the investigative process.

Third, there has been a problem between the CIA and the PBI in terms of their cooperation on counterintelligence investigations. There must be complete cooperation and coordination between these two important agencies at all times—where investigations of counterintelligence problems are concerned, the stakes are simply too high.

S. 1948 addresses each of these problem areas:

- it would require all employees of intelligence agencies, as a condition of their employment, to consent to access by the Government to their tax returns, financial records, and travel records;
- it would further require that all employees who are in "critical intelligence positions," as defined by the bill, must make detailed financial disclosures and continuously update them for so long as they hold such positions, and for 10 years thereafter (or until they leave Government service);
- it would provide additional legal authority needed by the intelligence agencies and by the FBI to obtain access to records needed for counterintelligence investigations, and to prohibit private entities from notifying the subject of an investigation that a request for records had been made by the Government; and
- it would establish clear requirements to improve the relationship between the FBI and the CIA and other intelligence agencies.

Clearly, no legislation can stop an individual determined to betray the United States—but we can make it far more difficult for that person to do so without detection. We can and must take action to improve the ability of our counterintelligence and security agencies to identify individuals engaged in espionage activities and facilitate their prosecution. This is what S. 1948 attempts to do.

Our bill builds upon legislation that was introduced by former SSCI Chairman Boren and Vice Chairman Cohen in 1990 (and based on the work of the so-called Jacobs Panel)—which unfortunately was never reported out of the Committee. We thought it desirable to develop a new bill to address more directly the problems apparent in the Ames case and to reflect developments since 1990 when the original legislation was introduced.

Next month, the SSCI will hold a series of public hearings on S. 1948 and other legislative proposals which attempt to deal with the counterintelligence problem. As Chairman and Vice Chairman of the Senate Select Committee on Intelligence, our objective is to find the most reasonable and responsible solution to this issue—striking the appropriate balance between national security needs and the privacy rights of the Federal Government employees who would be affected by the enactment of this legislation. We intend to work closely with the administration in developing this legislation. And we are determined to enact into law this year meaningful counterintelligence and security reforms.

If you would like to co-sponsor this legislation or have any questions, please feel free to contact us or have your staff contact Britt Snider, the Committee's General Counsel at 224–1729.

Best regards.

Sincerely,

DENNIS DECONCINI,
Chairman,

JOHN W. WARNER,
Vice Chairman.

Enclosures

KEY FEATURES OF S. 1948: THE COUNTERINTELLIGENCE AND SECURITY ENHANCEMENTS ACT OF 1994

Current Co-Sponsors: Graham, Murkowski, D'Amato, Kerrey, Gorton, Bryan, Chafee, Johnston, Boren, and Baucus

Section 2: Establishes certain requirements for employees of intelligence agencies to improve their security posture. All employees of intelligence agencies would, as

a condition of employment, provide written consent for authorized representatives to inspect or obtain copies of their Federal tax returns, financial records, and records relating to unofficial foreign travel.

Those employees who hold "critical intelligence positions" would, in addition, have to file disclosure reports regarding their bank, investment and credit accounts, and identify assets valued at more than $10,000. They would also have to promptly report any changes in these categories for so long as they occupy such positions and for 10 years thereafter, or whenever they leave Federal employment, whichever comes first.

The bill requires agency heads to identify positions that meet the criteria of the statute. It gives primary responsibility to the FBI in investigations involving persons in critical intelligence positions, and requires intelligence agencies to provide access to employees and records involved in such investigations.

The bill also mandates cooperation from governmental and private entities in providing access to, or copies of, documents requested by authorized investigative agencies in the course of an authorized counterintelligence and security investigation and precludes them from telling the subject or anyone else of the request.

Section 3: The FBI consumer credit amendment that passed the Senate in last year's intelligence authorization bill, giving the FBI authority to obtain consumer credit reports based upon a letter from the Director certifying that the person to whom the reports pertain (whether an employee or not) is the subject of a counterintelligence investigation. (This provision was dropped in the intelligence authorization conference last year, due to objections from the House Banking Committee.)

Section 4: Amends the Internal Revenue Code, giving the FBI authority to seek a court order from the Foreign Intelligence Surveillance Court (which currently issues orders permitting electronic surveillances for intelligence purposes) to see tax returns in counterintelligence cases. (This would apply to non-employees as well. Currently, the FBI must meet a criminal standard before non-consensual access can be obtained to tax records.)

Section 5: A modified Jacobs Panel recommendation giving the Attorney General authority to provide rewards for information leading to espionage arrests (similar to what the Attorney General can do in the terrorism area).

Section 6: A modified Jacobs Panel recommendation to give U.S. courts jurisdiction over espionage cases where the offending conduct occurred overseas. This is not a problem in the Ames case, but has been a problem for Justice in other situations (leaving the case to foreign courts).

Section 7: A modified Jacobs Panel recommendation establishing a new misdemeanor offense (up to $1,000 fine and 1 year in jail) for persons who remove classified information and retain it in an unauthorized location, whether it has been disclosed to an unauthorized person or not. (The Jacobs Panel limited this to the removal of TOP SECRET information.) Such conduct currently violates agency regulations, but does not violate any law.

Section 8: Extends the forfeiture provisions of the drug enforcement statute to the property of persons convicted of espionage. Thus, where the proceeds of espionage activities were moved outside the United States or commingled with other funds, the Government could use other assets of a person convicted of espionage to recover the proceeds of espionage activity. The proceeds resulting from the sale of such assets would be deposited in the Victims of Crime Fund of the Department of Justice.

II

103D CONGRESS
2D SESSION

S. 1948

To amend the National Security Act of 1947 to improve the counterintelligence and security posture of the United States intelligence community and to enhance the investigative authority of the Federal Bureau of Investigation in counterintelligence matters, and for other purposes.

IN THE SENATE OF THE UNITED STATES

MARCH 17 (legislative day, FEBRUARY 22), 1994

Mr. DECONCINI (for himself, Mr. WARNER, Mr. GRAHAM, Mr. MURKOWSKI, Mr. D'AMATO, Mr. KERREY, Mr. GORTON, Mr. BRYAN, Mr. CHAFEE, Mr. JOHNSTON, Mr. BOREN, and Mr. BAUCUS) introduced the following bill; which was read twice and referred to the Select Committee on Intelligence

---

A BILL

To amend the National Security Act of 1947 to improve the counterintelligence and security posture of the United States intelligence community and to enhance the investigative authority of the Federal Bureau of Investigation in counterintelligence matters, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Counterintelligence and Security Enhancements Act of 1994".

SEC. 2. COUNTERINTELLIGENCE FOR EMPLOYEES OF AGENCIES IN THE INTELLIGENCE COMMUNITY.

(a) IN GENERAL.—The National Security Act of 1947 (50 U.S.C. 401 et seq.) is amended by adding at the end the following new title:

"TITLE VIII—COUNTERINTELLIGENCE FOR EMPLOYEES OF AGENCIES IN THE INTELLIGENCE COMMUNITY

"DEFINITIONS

"SEC. 801. As used in this title:

"(1) The term 'head of an agency within the intelligence community' includes the following:

"(A) The Director of Central Intelligence in the case of the Central Intelligence Agency and the Office of the Director of Central Intelligence.

"(B) The Director of the National Security Agency in the case of such agency.

"(C) The Director of the Defense Intelligence Agency in the case of such agency.

"(D) The head of the central imagery authority of the Department of Defense in the case of such authority.

"(E) The Director of the National Reconnaissance Office in the case of such office.

"(F) The Secretaries of the military departments in the case of offices within such departments for the collection of specialized national intelligence through reconnaissance program and in the case of intelligence elements of the Army, Navy, Air Force, and Marine Corps.

"(G) The Director of the Federal Bureau of Investigation in the case of the intelligence elements of such bureau.

"(H) The Secretary of State, the Secretary of Treasury, and the Secretary of Energy in the case of the intelligence elements within the departments of each such Secretary, respectively.

"(2) The term 'critical intelligence position' means any position within the intelligence community, the holder of which requires access to critical intelligence information.

"(3) The term 'critical intelligence information' means—

"(A) classified information which reveals the identities of covert agents of the intelligence community and the disclosure of which to unauthorized persons would reasonably jeopardize the lives or safety of such agents;

"(B) classified information concerning a technical collection system of the intelligence community, the disclosure of which to unauthorized persons would substantially negate or impair the effectiveness of the system; or

"(C) classified information relating to a cryptographic system for the protection of classified information of the United States, the disclosure of which to unauthorized persons would substantially negate or impair the effectiveness of the system.

"(4) The term 'covert agent' has the meaning given such term in section 606(4).

"(5) The term 'technical collection system' means a system for the collection, transmission, or exploitation of electronic signals, emanations, or images by means that are not commercially available.

"(6) The term 'information relating to a cryptographic system' means information relating to (i) the nature, preparation, content, or use of any code, cipher, or other method of protecting communications of classified information of the United States from interception by unauthorized persons, or (ii) the design, construction, use, maintenance, or repair of any equipment used to protect such communica-

tions from such interception. Such term does not include information on the use of such equipment for personal or office use.

"(7) The term 'authorized investigative agency' means an agency, office, or element of the Federal Government authorized by law or regulation to conduct investigations of employees of the intelligence community for counterintelligence or security purposes.

"(8) The term 'employee' means any person who—

"(A) receives a salary or compensation of any kind from an agency of the intelligence community;

"(B) is a contractor or unpaid consultant of such an agency; or

"(C) otherwise acts for or on behalf of such an agency.

"REQUIREMENTS FOR EMPLOYEES OF AGENCIES IN THE INTELLIGENCE COMMUNITY

"SEC. 802. A person may not become an employee of an agency within the intelligence community unless, before becoming such an employee, the person—

"(1) authorizes, in writing, the Secretary of the Treasury to disclose the tax returns of the person, or information from such tax returns, to a rep-

resentative of an authorized investigative agency specified in the document evidencing such authority during the period in which the person is employed by the agency;

"(2) agrees, in writing, to permit a representative of such an authorized investigative agency to inspect or obtain for purposes authorized under this title copies of all records relating to bank accounts, investment accounts, credit accounts, and assets having a value of more than $10,000 in which the person, or any member of the immediate family of the person, has a beneficial interest during such period; and

"(3) agrees, in writing, to permit a representative of such an authorized investigative agency to inspect or obtain copies of all records maintained by a governmental entity or a private entity relating to the travel of the person to a foreign country.

"DESIGNATION OF CRITICAL INTELLIGENCE POSITIONS

"SEC. 803. Consistent with this title and in accordance with section 808, the head of each agency within the intelligence community shall by regulation designate each position within the agency which qualifies as a critical intelligence position.

"REQUIREMENTS FOR EMPLOYEES IN CRITICAL INTELLIGENCE POSITIONS

"SEC. 804. (a) An employee of an agency within the intelligence community may not hold a critical intelligence position unless, before holding such position, such employee—

"(1) provides the authority and agreements referred to in paragraphs (1), (2), and (3) of section 802; and

"(2) in accordance with the regulations prescribed under section 808—

"(A) provides the agency employing the employee with an appropriate statement disclosing the nature and location of all bank accounts, investment accounts, credit accounts, and assets valued at more than $10,000 in which the employee, or any immediate member of the family of the employee, has a beneficial interest;

"(B) agrees, in writing, to advise promptly the agency of any changes which occur with respect to the nature or location of the accounts or assets disclosed pursuant to subparagraph (A); and

"(C) agrees, in writing, to advise the agency employing the employee, in advance, of any travel of the employee to a foreign country if the travel is not authorized as part of the employee's official duties in such position.

"(b) An employee providing an authorization and agreements under subsection (a) shall agree that the authorization and agreement continue in effect—

"(1) during the period in which the employee holds the critical intelligence position for which the employee provides the authorization and agreements; and

"(2) if the employee ceases holding such position, until the earlier of—

"(A) the date 10 years after the date on which the employee ceases holding such position; or

"(B) the date on which the employee ceases employment with the Federal Government.

"RESPONSIBILITIES OF AUTHORIZED INVESTIGATIVE AGENCIES

"SEC. 805. (a) An appropriate authorized investigative agency shall, in accordance with the regulations prescribed under section 808—

"(1) periodically review and verify the information provided and disclosed under section 804 by persons holding critical intelligence positions; and

"(2) if such review indicates the failure of any such person to comply fully and completely with the requirements of such section, conduct an appropriate inquiry with respect to such failure.

"(b)(1) If circumstances indicate the loss or compromise of critical intelligence information, the head of the agency concerned shall immediately advise the Federal Bureau of Investigation of such loss or compromise.

"(2) Upon notification under paragraph (1), the Federal Bureau of Investigation, or any other appropriate authorized investigative agency with the concurrence with the Federal Bureau of Investigation, may conduct appropriate inquiries with respect to such loss or compromise.

"(c) Any inquiry under this section may include requests for information from a governmental entity or from private entities. Such requests shall be made in accordance with section 806.

"REQUESTS BY AUTHORIZED INVESTIGATIVE AGENCIES

"SEC. 806. (a)(1) Any authorized investigative agency may request from any governmental entity, or from any private entity, such records or other information as are necessary in order to conduct any authorized counterintel-

ligence inquiry or security inquiry, including inquiries under section 805.

"(2) Each such request—

"(A) shall be accompanied by a written certification signed by the head of the intelligence agency concerned, or the designee of the head of the agency, and shall certify that—

"(i) the person concerned is an employee of the intelligence agency;

"(ii) the request is being made pursuant to an authorized inquiry or investigation; and

"(iii) the records or information to be reviewed are records or information which the employee has previously agreed to make available to the authorized investigative agency for review;

"(B) shall contain a copy of the agreement referred to in subparagraph (A)(iii);

"(C) shall identify the records or information to be reviewed; and

"(D) shall inform the recipient of the request of the prohibition described in subsection (b).

"(b) No governmental or private entity, or officer, employee, or agent of such entity, may disclose to any person, other than those officers, employees, or agents of such

entity necessary to satisfy a request made under this section, that such entity has received or satisfied a request made by an authorized investigative agency under this section.

"(c)(1) Notwithstanding any other provision of law, an entity receiving a request for records or information under subsection (a) shall, if the request satisfies the requirements of this section, make available such records or information for inspection or copying, as may be appropriate, by the agency requesting such records or information.

"(2) Any entity (including any officer, employee or agent thereof) that discloses records or information for inspection or copying pursuant to this section in good faith reliance upon the certifications made by an agency of the intelligence community pursuant to this section shall not be liable for any such disclosure to any person under this title, the constitution of any State, or any law or regulation of any State or any political subdivision of any State.

"(d) Subject to the availability of appropriations therefor, any agency requesting records or information under this section may reimburse a private entity for any cost reasonably incurred by such entity in responding to such request, including the cost of identifying, reproducing, or transporting records or other data.

"(e)(1) Except as provided in paragraph (2), an agency receiving records or information pursuant to a request under this section may not disseminate the records or information obtained pursuant to such request outside such agency.

"(2) An agency may disseminate records or information referred to in paragraph (1) only to the agency employing the employee who is the subject of the records or information or to the Department of Justice for law enforcement or counterintelligence purposes.

"(f) Any authorized investigative agency that discloses records or information received pursuant to a request under this section in violation of subsection (e)(1) shall be liable to the employee to whom the records relate in an amount equal to the sum of—

"(1) $100, without regard to the volume of records involved;

"(2) any actual damages sustained by the employee as a result of the disclosure;

"(3) if the violation is found to have been willful or intentional, such punitive damages as the court may allow; and

"(4) in the case of any successful action to enforce liability, the costs of the action, together with reasonable attorney fees, as determined by the court.

"RESPONSIBILITIES OF THE FEDERAL BUREAU OF INVESTIGATION

"SEC. 807. (a) The Director of the Federal Bureau of Investigation shall have overall responsibility for the conduct of counterintelligence and law enforcement investigations involving persons in critical intelligence positions. The Director shall coordinate all investigative activities (other than routine inquiries for security purposes) undertaken with respect to such persons by authorized investigative agencies.

"(b) The head of each agency within the intelligence community shall ensure that the Director of the Federal Bureau of Investigation is provided appropriate access to the employees and the records of the agency as may be necessary to carry out authorized counterintelligence or law enforcement investigations.

"IMPLEMENTING REGULATIONS

"SEC. 808. Not later than 6 months after the date of the enactment of this Act, the Director of Central Intelligence shall issue regulations applicable to all agencies of the intelligence community to implement the provisions of this Act. Such regulations shall take effect not later than 6 months after the date of their issuance by the Director.

"OVERSIGHT

"SEC. 809. The Director of Central Intelligence shall submit to the Select Committee on Intelligence of the Sen-

ate and the Permanent Select Committee on Intelligence of the House of Representatives a report on the activities carried out under this title and the effectiveness of this title in facilitating counterintelligence activities. The Director shall submit the report on an annual basis.".

(b) TREATMENT OF INCUMBENTS OF COVERED POSITIONS.—(1) Each employee of an agency within the intelligence community shall carry out the requirements of section 802 of the National Security Act of 1947, as added by subsection (a), not later than 60 days after the issuance of the regulations required under section 808 of such Act, as so added.

(2) The head of each agency within the intelligence community shall, upon designating a position within the agency as a critical intelligence position under section 803 of such Act, as so added, promptly inform the incumbent, if any, of such position, and any persons being considered for such position, of such designation.

(3) The head of each such agency shall require that each person who holds a position in the agency so designated shall carry out the requirements of section 804 of such Act, as so added, not later than 60 days after the date of such designation.

(4) Notwithstanding any other provision of law, the head of each such agency shall—

(A) terminate the employment of any employee of the agency, or any incumbent in a critical intelligence position in the agency, who fails to comply with the requirements set forth in paragraph (1) or (3), as the case may be; and

(B) to the extent feasible—

(i) reassign such incumbent to a position of equal grade and status within the agency that is not a critical intelligence position; or

(ii) facilitate the reemployment of such employee in an agency that is not an agency within the intelligence community.

(c) TREATMENT OF CONGRESSIONAL STAFF HAVING ACCESS TO CRITICAL INTELLIGENCE INFORMATION.—(1) Notwithstanding any other provision of law and subject to paragraph (2), sections 802 and 804 of the National Security Act of 1947, as added by subsection (a), shall apply to employees of Congress whose positions of employment require access to critical intelligence information.

(2) The leaders of each House of Congress shall jointly determine with respect to such House—

(A) the employees of such House whose positions of employment require access to critical intelligence information; and

(B) appropriate means of applying such sections to such employees.

(3) In this subsection:

(A) The term "critical intelligence information" has the meaning given such term in section 801(3) of such Act, as so added.

(B) The term "leaders of each House of Congress" means the following:

(i) In the case of the Senate, the Majority Leader of the Senate and the Minority Leader of the Senate.

(ii) In the case of the House of Representative, the Speaker of the House of Representatives and the Minority Leader of the House of Representatives.

SEC. 3. DISCLOSURE OF CONSUMER CREDIT REPORTS FOR COUNTERINTELLIGENCE PURPOSES.

Section 608 of the Fair Credit Reporting Act (15 U.S.C. 1681f) is amended—

(1) by striking "Notwithstanding" and inserting "(a) DISCLOSURE OF CERTAIN IDENTIFYING INFORMATION.—Notwithstanding"; and

(2) by adding at the end the following new subsection:

"(b) DISCLOSURES TO THE FBI FOR COUNTERINTELLIGENCE PURPOSES.—

"(1) CONSUMER REPORTS.—Notwithstanding the provisions of section 604, a consumer reporting agency shall furnish a consumer report to the Federal Bureau of Investigation when presented with a written request for a consumer report, signed by the Director of the Federal Bureau of Investigation, or the Director's designee, who certifies compliance with this subsection. The Director or the Director's designee may make such a certification only if the Director or the Director's designee has determined in writing that—

"(A) such records are necessary for the conduct of an authorized foreign counterintelligence investigation; and

"(B) there are specific and articulable facts giving reason to believe that the consumer whose consumer report is sought is a foreign power or an agent of a foreign power, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

"(2) IDENTIFYING INFORMATION.—Notwithstanding the provisions of section 604, a consumer reporting agency shall furnish identifying informa-

tion respecting a consumer, limited to name, address, former addresses, places of employment, or former places of employment, to the Federal Bureau of Investigation when presented with a written request, signed by the Director or the Director's designee, which certifies compliance with this subsection. The Director or the Director's designee may make such a certification only if the Director or the Director's designee has determined in writing that—

"(A) such information is necessary to the conduct of an authorized counterintelligence investigation; and

"(B) there is information giving reason to believe that the consumer has been, or is about to be, in contact with a foreign power or an agent of a foreign power, as so defined.

"(3) CONFIDENTIALITY.—No consumer reporting agency or officer, employee, or agent of such consumer reporting agency may disclose to any person, other than those officers, employees, or agents of such agency necessary to fulfill the requirement to disclose information to the Federal Bureau of Investigation under this subsection, that the Federal Bureau of Investigation has sought or obtained a consumer report or identifying information respect-

ing any consumer under paragraph (1) or (2), nor shall such agency, officer, employee, or agent include in any consumer report any information that would indicate that the Federal Bureau of Investigation has sought or obtained such a consumer report or identifying information.

"(4) PAYMENT OF FEES.—The Federal Bureau of Investigation shall, subject to the availability of appropriations, pay to the consumer reporting agency assembling or providing credit reports or identifying information in accordance with procedures established under this title, a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in searching, reproducing, or transporting books, papers, records, or other data required or requested to be produced under this subsection.

"(5) LIMIT ON DISSEMINATION.—The Federal Bureau of Investigation may not disseminate information obtained pursuant to this subsection outside of the Federal Bureau of Investigation, except to the Department of Justice as may be necessary for the approval or conduct of a foreign counterintelligence investigation.

"(6) RULES OF CONSTRUCTION.—Nothing in this subsection shall be construed to prohibit information from being furnished by the Federal Bureau of Investigation pursuant to a subpoena or court order, or in connection with a judicial or administrative proceeding to enforce the provisions of this Act. Nothing in this subsection shall be construed to authorize or permit the withholding of information from Congress.

"(7) REPORTS TO CONGRESS.—On a semi-annual basis, the Attorney General of the United States shall fully inform the Permanent Select Committee on Intelligence and the Committee on Banking, Finance and Urban Affairs of the House of Representatives, and the Select Committee on Intelligence and the Committee on Banking, Housing, and Urban Affairs of the Senate concerning all requests made pursuant to paragraphs (1) and (2).

"(8) DAMAGES.—Any agency or department of the United States obtaining or disclosing credit reports, records, or information contained therein in violation of this subsection is liable to the consumer to whom such records relate in an amount equal to the sum of—

"(A) $100, without regard to the volume of records involved;

"(B) any actual damages sustained by the consumer as a result of the disclosure;

"(C) if the violation is found to have been willful or intentional, such punitive damages as a court may allow; and

"(D) in the case of any successful action to enforce liability under this subsection, the costs of the action, together with reasonable attorney fees, as determined by the court.

"(9) DISCIPLINARY ACTIONS FOR VIOLATIONS.—If a court determines that any agency or department of the United States has violated any provision of this subsection and the court finds that the circumstances surrounding the violation raise questions of whether or not an officer or employee of the agency or department acted willfully or intentionally with respect to the violation, the agency or department shall promptly initiate a proceeding to determine whether or not disciplinary action is warranted against the officer or employee who was responsible for the violation.

"(10) GOOD-FAITH EXCEPTION.—Any credit reporting agency or agent or employee thereof making

disclosure of credit reports or identifying information pursuant to this subsection in good-faith reliance upon a certificate of the Federal Bureau of Investigation pursuant to provisions of this subsection shall not be liable to any person for such disclosure under this title, the constitution of any State, or any law or regulation of any State or any political subdivision of any State.

"(11) LIMITATION OF REMEDIES.—The remedies and sanction set forth in this subsection shall be the only judicial remedies and sanctions for violation of this subsection.

"(12) INJUNCTIVE RELIEF.—In addition to any other remedy contained in this subsection, injunctive relief shall be available to require compliance with the procedures of this subsection. In the event of any successful action under this subsection, costs together with reasonable attorney fees, as determined by the court, may be recovered.".

SEC. 4. FBI ACCESS TO TAX RETURNS FOR COUNTERINTELLIGENCE PURPOSES.

Section 6103(i) of the Internal Revenue Code of 1986 is amended by adding at the end the following new paragraph:

"(9) DISCLOSURE FOR COUNTERINTELLIGENCE PURPOSES.—

"(A) IN GENERAL.—Except as provided in paragraph (6), any return or return information with respect to any specified taxable period or periods shall, pursuant to and upon the grant of an ex parte order by a district court judge issued pursuant to section 103 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803), be open (but only to the extent necessary as provided in such order) to inspection by, or disclosure to, officers and employees of the Department of Justice who are personally and directly engaged in an authorized counterintelligence investigation solely for the use of such officers and employees in such investigation.

"(B) APPLICATION FOR ORDER.—The Attorney General or the Deputy Attorney General may authorize an application to a judge referred to in subparagraph (A). Upon such application, such judge may grant such an order if the judge determines on the basis of the facts submitted by the applicant that—

"(i) there are specific and articulable facts giving reason to believe that the person whose returns or return information is sought is a foreign power or an agent of a foreign power, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801);

"(ii) there is reasonable cause to believe that the return or return information is or may be relevant to an authorized counterintelligence investigation;

"(iii) the return or return information is sought exclusively for use in an authorized counterintelligence investigation; and

"(iv) the information sought to be disclosed cannot reasonably be obtained, under the circumstances, from another source.".

SEC. 5. REWARDS FOR INFORMATION CONCERNING ESPIONAGE.

(a) REWARDS.—Section 3071 of title 18, United States Code, is amended—

(1) by inserting "(a)" before "With respect to"; and

(2) by adding at the end the following new subsection:

"(b) With respect to acts of espionage involving or directed at classified information of the United States, the Attorney General may reward any individual who furnishes information—

"(1) leading to the arrest or conviction, in any country, of any individual or individuals for commission of an act of espionage with respect to such information against the United States;

"(2) leading to the arrest or conviction, in any country, of any individual or individuals for conspiring or attempting to commit an act of espionage with respect to such information against the United States; or

"(3) leading to the prevention or frustration of an act of espionage with respect to such information against the United States.".

(b) DEFINITIONS.—Section 3077 of such title is amended by inserting at the end thereof the following new paragraphs:

"(8) 'act of espionage' means an activity that is a violation of—

"(A) section 794 or 798 of title 18, United States Code; or

"(B) section 4 of the Subversive Activities Control Act of 1950 (50 U.S.C. 783).

"(9) 'classified information of the United States' means information originated, owned, or possessed by the United States Government concerning the national defense or foreign relations of the United States that has been determined pursuant to law or Executive order to require protection against unauthorized disclosure in the interests of national security.".

(c) CLERICAL AMENDMENTS.—The items relating to chapter 204 in the table of chapters at the beginning of such title, and in the table of chapters at the beginning of part II of such title, are each amended by adding at the end the following: "**AND ESPIONAGE**".

SEC. 6. JURISDICTION OF UNITED STATES COURTS TO TRY CASES INVOLVING ESPIONAGE OUTSIDE THE UNITED STATES.

(a) IN GENERAL.—Chapter 211 of title 18, United States Code, is amended by inserting after section 3238 the following new section 3239:

"§ 3239. Jurisdiction of espionage outside the United States and related offenses

"The trial for any offense involving a violation of—

"(1) section 793, 794, 798, or 1030(a)(1) of this title;

"(2) section 601 of the National Security Act of 1947 (50 U.S.C. 421); or

"(3) subsection (b) or (c) of section 4 of the Subversive Activities Control Act of 1950 (50 U.S.C. 783 (b) or (c)),

begun or committed upon the high seas or elsewhere out of the jurisdiction of any particular State or district, may be prosecuted in the District of Columbia, or in the Eastern District of Virginia, or in any other district authorized by law.".

(b) CLERICAL AMENDMENT.—The table of sections at the beginning of chapter 211 of such title is amended by inserting after the item relating to section 3238 the following:

"3239. Jurisdiction of espionage outside the United States and related offenses".

SEC. 7. LESSER CRIMINAL OFFENSE FOR THE UNAUTHORIZED REMOVAL OF CLASSIFIED DOCUMENTS.

(a) IN GENERAL.—Chapter 93 of title 18, United States Code, is amended by adding at the end the following new section:

"§ 1924. Unauthorized removal and retention of classified documents or material

"(a) IN GENERAL.—Whoever, being an officer, employee, contractor, or consultant of the United States, and, by virtue of his office, employment, position, or contract, becomes possessed of documents or materials containing classified information of the United States, knowingly removes such documents or materials without authority and with the intent to retain such documents or materials at an unauthorized location shall be fined not more than $1,000, or imprisoned for not more than 1 year, or both.

"(b) DEFINITION.—In this section, the term 'classified information of the United States' means information originated, owned, or possessed by the United States Government concerning the national defense or foreign relations of the United States that has been determined pursuant to law or Executive order to require protection against unauthorized disclosure in the interests of national security.".

(b) CLERICAL AMENDMENT.—The table of sections at the beginning of such chapter is amended by adding at the end the following:

"1924. Unauthorized removal and retention of classified documents or material".

SEC. 8. CRIMINAL FORFEITURE FOR VIOLATION OF CERTAIN ESPIONAGE LAWS.

(a) TITLE 18.—Section 798 of title 18, United States Code, is amended by adding at the end the following new subsection:

"(d)(1) Any person convicted of a violation of this section shall forfeit to the United States irrespective of any provision of State law—

"(A) any property constituting, or derived from, any proceeds the person obtained, directly or indirectly, as the result of such violation; and

"(B) any of the person's property used, or intended to be used, in any manner or part, to commit, or to facilitate the commission of, such violation.

"(2) The court, in imposing sentence on a defendant for a conviction of a violation of this section, shall order that the defendant forfeit to the United States all property described in paragraph (1).

"(3) Except as provided in paragraph (4), the provisions of subsections (b), (c), and (e) through (p) of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853 (b), (c), and (e)–(p)) shall apply to—

"(A) property subject to forfeiture under this subsection;

"(B) any seizure or disposition of such property; and

"(C) any administrative or judicial proceeding in relation to such property, if not inconsistent with this subsection.

"(4) Notwithstanding section 524(c) of title 28, there shall be deposited in the Crime Victims Fund established under section 1402 of the Victims of Crime Act of 1984 (42 U.S.C. 10601) all amounts from the forfeiture of property under this subsection remaining after the payment of expenses for forfeiture and sale authorized by law.".

(b) AMENDMENTS FOR CONSISTENCY IN APPLICATION OF FORFEITURE UNDER TITLE 18.—(1) Section 793(h)(3) of such title is amended in the matter above subparagraph (A) by striking out "(*o*)" each place it appears and inserting in lieu thereof "(p)".

(2) Section 794(d)(3) of such title is amended in the matter above subparagraph (A) by striking out "(*o*)" each place it appears and inserting in lieu thereof "(p)".

(c) SUBVERSIVE ACTIVITIES CONTROL ACT.—Section 4 of the Subversive Activities Control Act of 1950 (50 U.S.C. 783) is amended by adding at the end the following new subsection:

"(g)(1) Any person convicted of a violation of this section shall forfeit to the United States irrespective of any provision of State law—

"(A) any property constituting, or derived from, any proceeds the person obtained, directly or indirectly, as the result of such violation; and

"(B) any of the person's property used, or intended to be used, in any manner or part, to commit, or to facilitate the commission of, such violation.

"(2) The court, in imposing sentence on a defendant for a conviction of a violation of this section, shall order that the defendant forfeit to the United States all property described in paragraph (1).

"(3) Except as provided in paragraph (4), the provisions of subsections (b), (c), and (e) through (p) of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853 (b), (c), and (e)–(p)) shall apply to—

"(A) property subject to forfeiture under this subsection;

"(B) any seizure or disposition of such property; and

"(C) any administrative or judicial proceeding in relation to such property, if not inconsistent with this subsection.

"(4) Notwithstanding section 524(c) of title 28, United States Code, there shall be deposited in the Crime Victims Fund established under section 1402 of the Victims of Crime Act of 1984 (42 U.S.C. 10601) all amounts from the forfeiture of property under this subsection remaining after the payment of expenses for forfeiture and sale authorized by law.".