S. HRG. 101-1293

S. 2726 TO IMPROVE U.S. COUNTERINTELLIGENCE MEASURES

HEARINGS

BEFORE THE

SELECT COMMITTEE ON INTELLIGENCE

OF THE

UNITED STATES SENATE

ONE HUNDRED FIRST CONGRESS

SECOND SESSION

ON

S. 2726 TO AMEND THE NATIONAL SECURITY ACT OF 1947 TO IMPROVE U.S. COUNTERINTELLIGENCE MEASURES

WEDNESDAY, MAY 23, AND THURSDAY, JULY 12, 1990

Printed for the use of the Select Committee on Intelligence

U.S. GOVERNMENT PRINTING OFFICE

37-791 ≈ WASHINGTON : 1991

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0-16-037010-8

SELECT COMMITTEE ON INTELLIGENCE

[Established by S. Res. 400, 94th Cong., 2d Sess.]

DAVID L. BOREN, Oklahoma, *Chairman*
FRANK H. MURKOWSKI, Alaska, *Vice Chairman*

SAM NUNN, Georgia
ERNEST F. HOLLINGS, South Carolina
BILL BRADLEY, New Jersey
ALAN CRANSTON, California
DENNIS DECONCINI, Arizona
HOWARD M. METZENBAUM, Ohio
JOHN GLENN, Ohio

JOHN WARNER, Virginia
ALFONSE D'AMATO, New York
JOHN C. DANFORTH, Missouri
WARREN RUDMAN, New Hampshire
SLADE GORTON, Washington
JOHN CHAFEE, Rhode Island

GEORGE MITCHELL, Maine, *Ex Officio*
ROBERT DOLE, Kansas, *Ex Officio*

GEORGE J. TENET, *Staff Director*
JOHN H. MOSEMAN, *Minority Staff Director*
KATHLEEN P. MCGHEE, *Chief Clerk*

CONTENTS

WEDNESDAY, MAY 23, 1990

THURSDAY, JULY 12, 1990

HEARING ON S. 2726 TO IMPROVE U.S. COUNTERINTELLIGENCE MEASURES

WEDNESDAY, MAY 23, 1990

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

The Select Committee met, pursuant to notice, at 2:11 p.m., in room SH-216, Hart Senate Office Building, the Honorable David L. Boren (chairman), presiding.

Present: Senators Boren, Bradley, Metzenbaum, Cohen, Murkowski, Warner, and Danforth.

Also attending: Representatives Bereuter, Livingston and Dornan.

Also present: George Tenet, Staff Director; James Dykstra, Minority Staff Director; Britt Snider, Chief Counsel; Kathleen McGhee, Chief Clerk; and Keith Hall, David Holliday, Fred Ward, Chris Straub, Don Mitchell, Regina Genton, Blythe Thomas, John Elliff, Andre Pearson, Michele Walters, Eric Lee, Claudia Daley, James Wolfe, Jenny Philipson, Chris Mellon, Marin Strmecki, Gary Sojka, James Martin, Larry Kettlewell, Charles Battaglia, Richard Combs, Marvin Ott, Mary Sturtevant, Paul Joyal, John Despres, Jon Chambers, Connell Sullivan, James Currie and Charlene King, Staff Members.

PROCEEDINGS

Chairman BOREN. I think we will commence. Other Members will be joining us.

I want to welcome Doug Bereuter, a Member of the House of Representatives Intelligence Committee. Others of his colleagues may be joining us from the House Intelligence Committee as well as some Members of the Senate Judiciary Committee. Many had expected to be here, but unfortunately, they have the anti-crime bill on the floor. Members of that Committee are heavily involved in managing that particular piece of legislation. But we will have other Members of the Committee and other guests from the rest of Congress with us in the course of our proceedings today.

Ever since the mid-1970's when this Committee was established, we have faced a series of terribly damaging espionage cases. You can start with the Boyce-Lee and Kampiles cases, go through the Walkers, Pelton, Pollard, Chin, to the more recent examples of Conrad and Hall. Our national security has suffered in ways that simply cannot be quantified as a result of these espionage cases.

This Committee has, since its inception, seen as one of its primary responsibilities the fostering of actions by the government to cope with this problem. In the 1970's, we helped to develop the Foreign Intelligence Surveillance Act. In the early 1980's, the Committee helped to develop the Classified Information Procedures Act. We also helped to pass legislation limiting the size and activities of hostile intelligence services within the United States, a piece of legislation on which the Vice Chairman, Senator Cohen, played a particularly important leadership role. We've supported, and indeed, enhanced the funding requests of our counterintelligence services to cope with the problems. In 1986, the Committee issued a major report, entitled "Meeting the Espionage Challenge," which included over 100 recommendations.

Clearly, progress has been made. But much remains to be done. Espionage cases of serious consequence continue to surface with disturbing frequency. We continue to feel frustrated by our inability to deter, detect, and often even to prosecute suspected misconduct.

While our relationship with the Soviet Union has warmed considerably, and the governments in Eastern Europe have undergone dramatic change, there seems to be no decrease in espionage against the United States. Indeed, these new relationships may provide more opportunities than ever before in terms of gaining access to information by foreign and hostile governments within this country.

I would say that we have seen an increase actually in the level of espionage activity over the last 2 or 3 years. Budget pressures are on the other side as well and it becomes, unfortunately, cost-effective to steal our technology. We've also seen an increase in commercial espionage by foreign governments against private commercial targets.

The espionage priorities of both allies and adversaries are changing and will change more. Military secrets, as I've said, may well be less important. Yet, as a nation we must give careful thought to the protection of technologies and weapons which provide the United States with a clear comparative advantage on the battlefield.

As the prospects of military competition between NATO and the Warsaw Pact fade, the real competition for commercial markets, trade, and technology will escalate.

Vladimir Kryuchkov, the head of the KGB, in attempting to portray a new kinder, gentler, if I can use that term, image for the KGB has publicly stated his intention to have the KGB enhance the competitiveness of Soviet companies. In simple terms, what he was really saying is espionage against commercial targets in the United States could become the great equalizer for the shortcomings of the Soviet economy.

In the changing world in which we live, intelligence services once hostile will be friendly, and those that have been friendly services will in some degree become hostile. We have already seen that happening. The economic competition of the next century will result in government-sponsored espionage against our corporate entities.

We don't have to wait until the next century to see it happening. It has already and it is going to escalate. More and more foreign

governments will be out to steal our private commercial secrets for the benefit of their national economic survival and gain.

So at the same time, it is also clear that a large part of the problem is impervious to political changes abroad. The vast majority of Americans who have committed espionage over the last 15 years have been volunteers. They have not been recruited by foreign services; they have volunteered. Is there any reason to think that they won't continue to be welcomed with open arms? I doubt it.

Faced with the seemingly intractable problem, Senator Cohen and I decided to try a new approach by enlisting the help of a knowledgeable group of people outside of Government to look at this problem. We had initial conversations last summer with Eli Jacobs and Admiral Bobby Inman, both of whom are here today, and asked them if they could put together such a group.

They responded admirably by putting together a group of very distinguished private citizens, well-known to all of us for their contributions both in and out of the government. For the last 6 months, this group has been examining the statutory framework for the conduct of U.S. counterintelligence activities and will report their findings to us today.

Indeed, our Nation has a long tradition of "wisemen", offering their advice to senior policymakers on national security matters. Men and women called together from outside of Government to serve their country. This Panel is the latest statement of this bipartisan tradition.

Before proceeding to their testimony, I would like to just take a moment to recognize the members of the Panel who are here with us today and the others who have served with this group.

Acting as Chairman is Mr. Eli Jacobs, a well-regarded and well-respected industrialist who, over the past 30 years, has developed an exceptional grasp and knowledge of this Nation's national security policy issues. To touch briefly on his experience in this area, he began his education on national security matters as a counterintelligence officer in the United States Army. He has long been a member of the General Advisory Committee on Arms Control and Disarmament. He served for several years and continues to serve on the Defense Policy Board which advises the Secretary of Defense on policy issues. He is also on the Chief of Naval Operations' Executive Panel and was a member of the important Carnegie Endowment for International Peace's Panel on international security.

The Panel has also benefited enormously from the participation of Admiral Bobby Inman, who, of course, has previously served as Director of the National Security Agency, Deputy Director of Central Intelligence and Director of Naval Intelligence. He is certainly an old and trusted friend of this Committee who has appeared before this Committee often in his earlier capacities in Government.

We also are delighted to have with us today Mr. Warren Christopher who has served, of course, both as Deputy Attorney General and Deputy Secretary of State. He is now practicing law in Los Angeles.

In addition, we have another distinguished attorney in Lloyd Cutler who served as Counsel to President Carter in the White House. He has figured prominently in a number of national issues.

We are certainly grateful for his willingness to join in this effort and for the advice that he has provided to this Panel as it has proceeded ahead.

We also, and again in a bipartisan spirit, have another gentleman, A.B. Culvahouse, who has served as Counsel to President Reagan. Now practicing law here in Washington, A.B. is another friend of this Committee, has worked with us on a number of occasions and has certainly had a wonderful and constructive relationship with Members of this Committee on both sides of the aisle.

We have with us Ambassador Sol Linowitz, a distinguished lawyer and diplomat, who served formerly as Ambassador to the Organization of American States. He has served as the United States Negotiator in Middle Eastern issues and on the Panama Canal Treaties. We greatly appreciate his contribution to this Panel.

Professor Harold Edgar, another member of the Panel, is a Professor of Law at Columbia, who co-authored with the now President of Yale University Benno Schmidt in the early 1970's, perhaps the most definitive article on the espionage statutes. Professor Edgar is recognized as a leading authority of the law in the espionage and intelligence field.

Two distinguished members of the Panel could not be with us today. First, Richard Helms, who, as we all know, was the Director of the Central Intelligence Agency in the Johnson and Nixon Administrations as well as a former Ambassador to Iran. And, second, Mr. Seymour Weiss, formerly head of the Bureau of Politico-Military Affairs at the State Department, Ambassador to the Bahamas, as well as a member of the President's Foreign Intelligence Advisory Board and Chairman of the Defense Policy Board.

So it has been an exceptional group of people that have worked on this effort. On behalf of the entire Committee, I simply want to thank all of you for performing what I believe is a critically important public service. You have done so without any compensation, on your own time, and at your own initiative. For busy people to take their precious time and apply their exceptional talents to this task is another example of the spirit of public service that, I would say, has marked the professional careers of all of those who are here to share their thoughts with us today.

And so while thank you is an inadequate way to say what we feel, it is heartfelt. I do want to tell you how much we appreciate your service.

The Panel has made a real contribution, not simply in terms of this Committee, but to the country as a whole. No one can realistically expect that espionage will ever be totally eradicated. But we can take steps to minimize its occurrence and lessen its impact. The first step must be to ensure that we have an adequate legal framework to deal with the problem. Your ideas contribute enormously to that end and we welcome them.

Finally before turning to Senator Cohen for any remarks that he might like to make, let me say a few words to Members of the Committee about our own progress.

There is nothing more important to me and to my colleague and friend, the Vice Chairman, than consensus. The distinguished group of people before us has completed their work and the work of

the Committee is now just beginning. Senator Cohen and I will, as we always do, seek to generate consensus and to see what can be realistically done. We will consult with our colleagues on the Judiciary Committee. As I have indicated, Senator Biden, Senator Thurmond, Senator Leahy and several others indicated they hoped they would be here today. They are following our progress with interest. We have already had some discussions with them as well as with Members of the House Intelligence Committee.

We will make changes. Undoubtedly we will change some of the ideas presented to us. And above all, we will ensure that the Committee's final views preserve and protect the First Amendment Rights of every American including those who choose to work in some of our Nation's most sensitive national security positions.

We understand that our responsibility is not only to guard against espionage, protect against it, deter it, but also to make sure that the legitimate constitutional rights of Americans are not infringed and that we do not take actions that are unnecessarily intrusive into the lives of others. The Panel has shown very great sensitivity to those values and we appreciate that very much.

Let me say also, since we've commenced, our colleagues Congressman Dornan and Congressman Livingston, have arrived from the House of Representatives. We welcome you and are very glad that you could be with us today.

I'll turn now to Senator Cohen for any remarks that he might like to make before we hear from the Panel.

Senator COHEN. Thank you very much, Mr. Chairman.

I want to echo your words of praise. This Panel has taken its charge very seriously. Taking time out of their busy days—and weekends I might add, especially in the case of the Acting Chairman Eli Jacobs, they have come to grips with a complicated subject, and I think have come up with a number of good ideas in an area which needed some fresh thinking. I was privileged to sit in on a number of their weekday and weekend sessions, and was impressed by the seriousness with which they went about their work, and the caliber of the discussion.

I think it demonstrates that it is still possible to draw upon a council of wise men, unencumbered by bureaucracies or partisanship, who can produce results that we would never see emerge from the government itself.

And let me just follow up on a point you alluded to, Mr. Chairman. To those who would say, this is all well and good, but, your timing is off. The Cold War is over. Why now? To which we must respond—if not now, when? After the next Felix Bloch? Or the next Craig Kunkle or Henry Otto Spade?

In the past, people betrayed their country out of ideological zeal. But the days of Philby, Burgess, MacLean, Blount, and the Rosenbergs are over. Now our Nation's secrets are sold at the espionage bazaar to the most generous buyer.

More spies have been named during the last 10 years than ever before in our history. They have been clerks, analysts, counterespionage specialists, cryptanalysts, officers and enlisted personnel from every one of our military services. They are not high-profile, derring-do agents of spy fiction fame, but faceless, unglamorous individuals who have access to our most important secrets. They are

what authors Tom Allen and Norman Polmar call our *Merchants of Treason.* And we seem to be capable of detecting them when some family member turns them in, they surrender or when a Soviet defector discloses their identities.

John Walker, a Navy radioman, operated a spy ring for 17 years before his former wife—no femme fatale out of Robert Ludlum or Len Deighton's novels—but a woman who worked for a time at a local shoe factory in Maine for $2.65 an hour, turned him in. Without Barbara Walker's phone call to the FBI, John Walker would in all probability still be jeopardizing the lives of every American so that he could profit.

I might note parenthetically that Walker equates himself with the skullduggery of certain Wall Street traders. He did no more than Ivan Boesky—trade a little inside information. What Walker, Whitworth, Howard, Pelton and others did was strike a Faustian bargain of sorts—they traded our lives for cash, undermining our deterrent against war, enabling our adversaries to neutralize the very heart of our strength.

And again, it is suggested that this is all behind us. The Cold War is over. John LeCarre has written that the days of George Smiley and Karla are history. It is time to face new enemies—drugs, terrorism, poverty, brush fire wars, and the pollution of our planet. Many spies will indeed come in from the cold, but unfortunately many more will bask and flourish in the warm sun of our new relationship with the USSR and East European nations—not to mention some of our closest allies.

The Era of the Cloak and Dagger may be over, but the cloaks are likely to multiply and become even more pervasive in their effort to procure military, industrial and commercial secrets.

The proposals recommended by the Jacobs Panel will not put an end to espionage. They are designed to do three things. Deter U.S. citizens from spying. Detect those who are not deterred. Help prosecute those who trade our security for their own enrichment.

There are legitimate questions that have been raised about rights of privacy. The subject is not a trivial one and we must always remain sensitive to the fact that we do not want to Stalinize our Intelligence Community in the name of national security. Access to our Nation's secrets is a privilege—one that must be more carefully granted and more carefully guarded. It is our responsibility to seek and strike the appropriate balance between guarding the right of privacy against those who would betray our Nation. I believe that balance has been struck.

And so as I join in commending the Panel. I think you've done an outstanding public service. And I believe that this Committee and other committees who share jurisdiction are going to be very, very indebted to the work product that you have brought before us.

Chairman BOREN. Thank you very much, Senator Cohen.

Let me ask Senator Warner, do you have any opening comments that you would like to make?

Senator WARNER. Mr. Chairman, I compliment the Chair and the Ranking Member for, I think, very accurately characterizing the sentiment of gratitude that this Committee has towards these outstanding men.

Like a great chain, America can be no stronger than its weakest link. And one of those weak links is the ability to cope with espionage.

And as Senator Cohen said, we are fortunate to have seven of the wisest men bring to bear their collective experience and judgment to help the Congress solve this problem.

Thank you, gentlemen.

I have a statement for the record.

[The statement of Senator Warner follows:]

PREPARED STATEMENT OF SENATOR JOHN WARNER

Today, we welcome Mr. Eli Jacobs, Chairman of the Committee's Counterintelligence Advisory Panel, to provide the Panel's recommendations on strengthening our country's counterintelligence laws. Joining Mr. Jacobs at the table are two other distinguished members of the Panel—Admiral Bobby Inman, who needs no introduction, and Professor Harold Edgar, a specialist in counterintelligence law at Columbia University.

I welcome these witnesses and the other distinguished members of the Panel sitting behind them—Lloyd Cutler, Warren Christopher, Sol Linowitz, A.B. Culvahouse, and Seymour Weiss. I thank all of you for the excellent service which you have performed in preparing these 13 recommendations for our consideration.

I also wish to thank my Chairman and Vice Chairman for constituting this Panel. Given the flood of espionage cases we have experienced over the recent years, reviewing the adequacy of current laws is the right thing to do at the right time. As the committee has noted, critical damage has been done by American spies who have sold military, intelligence, and diplomatic information to foreign countries. So much information has been passed to foreign countries it could fill a good size room, and it has covered every conceivable category of information—strategic and tactical reconnaissance systems, human sources, advanced weapon systems, and military war plans.

Simply put, Mr. Chairman, we need to insure that our laws provide for effective counterintelligence, and the Panel's recommendations seek to insure that they do. At the same time, I understand that as they selected and crafted the 13 recommendations, the Panel paid particular attention to insuring that the liberties to which our American citizens who hold government positions are entitled will be protected. This is important, because the vast, vast majority of these people are honest, patriotic Americans who would never dream of betraying their country.

With these opening remarks, I look forward to hearing from the witnesses and working with the members of this committee to draft legislation which meets the twin goals of strengthening our counterintelligence laws while maintaining the basic rights of our government employees.

Chairman BOREN. Thank you very much.

Senator Danforth?

Senator DANFORTH. Mr. Chairman, you and Senator Cohen have spoken very well for me. And I just want to express also my appreciation for the work of these people. We seem to go back to the same wells over and over again for public service. And these are very good wells and we appreciate what you produced. Thank you.

Chairman BOREN. Thank you very much, Senator Danforth.

Well, again, I express my appreciation to the Panel.

Mr. Jacobs, you served as Chairman and coordinator of this Panel for which we are very grateful. We'd welcome your opening remarks and I understand you may want to then turn to Admiral Inman and Professor Edgar to give more of a detailed summary of the recommendations. We welcome you.

TESTIMONY OF ELI JACOBS

Mr. JACOBS. Thank you.

Mr. Chairman it is a pleasure to be with you today.

At the request of Senators Boren and Cohen, our Panel began approximately 6 months ago to review the laws and policies affecting the counterespionage activities of the United States. This effort was motivated by the large number of very serious espionage cases that have damaged virtually every area of our national security over the last 20 years. We sought to determine whether new legislation might improve our ability to deter, detect and prosecute such cases in the future. Today we present to you the initial results of our review.

It is important that the Committee understand at the outset how we defined our role.

First, we addressed the counterintelligence problem within the existing organizational framework. We did not examine the need for changes to that framework.

Second, we determined at the outset that we would not address the problem of unauthorized disclosure of classified information to the media. We do not deny that leaks are a problem, but attempts to deal with them inevitably raise special constitutional concerns that we hoped to avoid by limiting the scope of our efforts to dealing with classical espionage.

Third, our focus has been on legislative remedies, and we have approached that subject cautiously. We recommend no changes to the basic espionage statutes set forth in Title 18, United States Code, Sections 793, 794, and 798. These are now old statutes whose clarity in some respects leaves something to be desired. But given the large amount of existing case law interpreting these statutes, there is no compelling reason to amend them.

Instead, we've taken the approach that such statutes should be supplemented by additional laws that address shortcomings identified by experience. The recommendations we are presenting today are largely based on a study of cases that have occurred since 1970. They are designed to tackle some of the problems in deterrence, detection and prosecution that were identified by our study.

Finally, we have attempted to craft proposals that avoid serious civil liberties concerns. Clearly, there is a balance to be struck in this area between the need of the Government to protect national security information and the need to protect the constitutional rights of all of our citizens, including those who choose to work for the Government in sensitive positions. We believe that it is possible to do so.

The post-World War II security and counterintelligence establishment always assumed that there would be hostile penetration of our national security system, and that Communist ideology was the principal motive for betrayal.

The past 20 years indicate that the main threat is not the ideologically motivated agent but rather the volunteer spy, the insider who betrays his country not from belief, but for money or revenge.

Some of our proposals are aimed at deterring such conduct before it occurs. Others are designed to detect such conduct as it occurs, for example, by identifying employees with access to TOP SECRET data who experience either sudden wealth or face financial ruin. As the world continues to grow more complex, so must our responses in order to meet the espionage challenge.

The question that is raised is why, at this juncture in history, when relations with the Soviet Union are undergoing a significant change and democracy seems to be sweeping across Eastern Europe, must we energize our effort against the counterespionage threat.

First, there is no indication of a decrease in the espionage activities directed against the United States by the Soviets. Second, other traditional intelligence adversaries, such as China and Cuba, will continue to pose serious counterintelligence threats to our national security. Third, there are increasing indications that new forms of economic espionage may be joining classical espionage as a necessary object of our concern. In short, there appears to be no abatement in espionage either now or on the horizon.

Admiral Inman will describe the process our Panel went through in analyzing the post-1970 espionage cases. The cumulative damage assessment demonstrates that intelligence activities against the United States caused grievous damage during this period. Espionage losses have affected a full range of U.S. national security interests, including strategic and tactical reconnaissance programs, human and signals intelligence sources and methods, advanced weapons systems and technology, and military war plans and capabilities. We believe this history provides a compelling set of reasons for the proposed legislation. It is our hope that changes in the legislative framework dealing with counterintelligence will deter such crimes in the future.

Professor Harold Edgar will then explain where the cases have led us and summarize each of the 13 legislative proposals. Upon Professor Edgar's conclusion, we will turn to the Committee's questions and all Panel members are urged to participate in the responses.

Admiral Inman?

Admiral INMAN. Thank you, Mr. Jacobs. And, Mr. Chairman, if I may submit my statement for the record to be included.

[The prepared statement of Admiral Inman follows:]

PREPARED STATEMENT OF ADMIRAL INMAN

Mr. Chairman, the purpose of my statement is to present the results of a review of the major espionage cases which have occurred since 1975. That review was a principal basis for the legislative proposals we are making to the Committee.

Before beginning a discussion of the cases, let me make two introductory points.

First, as we looked at how the government has dealt with counterintelligence, we found a process that was oriented toward trying to detect individuals who were either ideologically sympathetic with our principal adversaries or who were susceptible to being blackmailed into committing espionage. We set out to go through the cases and determine whether that was, in fact, the basis upon which people became involved in espionage.

Second, we looked at how the government tried to deal with each of the cases in four specific areas—deterrence of individuals who might be inclined to engage in espionage, detection of them if they did become engaged, assessment of the damage done from their espionage, and finally prosecution.

As we approached the agencies, we received truly great cooperation and candor. It turned out that they had not gone through all the past cases in this systematic way with the objective of trying to understand the lessons to be learned and detecting patterns of activity where legislation might have made a difference. The agencies did a first-rate job in working with us, and they will tell you that they have now begun thinking about these problems in a very different way. In analyzing the cases we tried to concentrate on the largest problems. The question was not how to detect

every case, but where could legislation really make a difference in the way the government goes about its counterintelligence work.

We ended up with nineteen cases of people who actually delivered classified information at some point to a foreign power, and we prepared a matrix that should help you track those cases. We also had prepared for us an unclassified summary of the cases since 1975. It is based on the media accounts of the espionage cases that have been publicized. The matrix and summary should be part of the record of our presentation.

The matrix presents what we found when we looked at the individuals who committed espionage. Was there anything in their background that should have caused people to worry? Once they were in office, were there things that might have been detected earlier in the process by better performance? What kind of information did the people who did the most damage have access to? How were they contacted, or how did they get drawn into espionage? What did they get from being in the espionage business? How damaging was the information they provided, and how well did the government come to understand that?

What you find in looking at the 19 cases is that the overwhelming proportion of truly serious damage came from people who had access to TOP SECRET information or cryptographic information. So we made a judgment early to try to get this problem down to size by focusing, not on the four million people in government who have some access to classified information, but on those who have access to TOP SECRET or cryptographic information. This would deal with the vast majority of cases that actually did substantial damage over time.

In the overwhelming percentage of the cases, the individuals went through a clearance process, including a background investigation and clearance approval, and were given access to classified information *before* they had done anything that would cause you to believe they would turn out to provide classified information to foreign governments. They were not ideologically sympathetic, and they were not blackmailed into the process.

What we found was that overwhelmingly they were volunteers. As you go through the matrix, you will find that individuals were recruited in about six cases, but they were recruited after it had become apparent to foreign governments that they were prime targets, not because they were ideologically sympathetic, but because they wanted money. They were demonstrating in their behavior that they would be approachable and likely to respond to an offer of money. For example, some were complaining they were underpaid.

There was no clear pattern of where the individuals ranked. They were neither the most senior people nor the most junior people. They had often been in government for several years, in some cases a good many years, and then decided to take a chance. In only two of the most serious cases had they left the government. Most were still in government with continuing access when they began their espionage activities.

The next question was how they made contact, if they were volunteers. And we found there were a variety of ways. Frequently it was telephone calls. In some cases, it was mail. The individual making the approach generally believed that it was a way that would not be likely to be detected. To repeat, in the overwhelming percentage of the cases that were the most damaging, the first contact was by a U.S. citizen, cleared for TOP SECRET, making the initial approach.

In two of the cases that were particularly damaging, Pelton and Howard, the individuals had left government service. Howard was very disgruntled. Pelton got into deep financial difficulty.

Turning to the detection side of the problem, we spent some time trying to understand whether, if we had a process that would let us understand either economic distress or sudden unexplained wealth, it would have helped us uncover the case. The answer is that in some cases it would have, but not in all. We looked at foreign travel. In a great many of the cases, after the individuals became directly involved in espionage, they traveled outside the United States to make contacts with case officers. This did not happen in a few cases. Some were handled entirely in the United States.

The point is that no single action would have detected all the cases. As we gradually winnowed our way through the evidence, we identified a series of areas where legislation would make a difference. Our aim was to produce a different approach by those government organizations that are responsible for counterintelligence, including both prevention and detection of espionage. We wanted to improve the prospects for detecting problems when individuals entered into service, but more importantly to deter those who were already cleared for access from initiating a contact designed to lead to espionage.

We sought to do this by raising the risk that if they undertook espionage activities, first, they would be caught and, second, there would be at least some laws they would violate in the process for which they would end up paying a penalty, serving time in jail. With respect to criminal laws, we looked beyond the ability to prosecute for espionage in the classic sense that we have considered in the past.

In our discussions of these cases, we spent a great deal of time going through the individual circumstances. Some of the details remain classified. Each of the legislative proposals can be traced back to specific cases where we believe that, if the legislation had been on the books, we would have had a better chance—not certainty—of deterring, detecting, or prosecuting the individuals involved. For example, we have a recommendation on consent to access to financial records. The first objective is deterrence. The fact that the individuals know there will be access to financial records raises the specter that they might be caught if they engage in espionage. In addition, we are aiming at the individual who has already been through the initial clearance investigation. The main concern is re-investigations, after they have already had access, because we found that that is where the heart of our problem is.

Another thing that emerged from looking at the cases was the wide variation on security clearance standards and the different application of standards among various departments and agencies. We have taken the view that you need a solid legislative-base to ensure uniform acceptance and application of rigorous standards.

To sum up: While we have considered other issues, our decision was to focus at this time on how we make sure that anyone who engages in selling the country's secrets ends up paying at least some penalty, instead of walking free with no penalty at all.

There are many who could reasonably ask whether our work has been overtaken by events. Have the changes in eastern Europe made the espionage threat less significant than it was even a year ago? It is true that those who are offering money for secrets may include some different countries in the years ahead. But the problem we have to deal with, as demonstrated over the last 15 years, is that Americans who have access to very sensitive information will sometimes look for ways to make a profit from that access. That is the issue we are trying to address, not which country is offering to pay.

In closing, I would like to add two personal comments. The first is about our decision to recommend legislative actions. I became engaged in this effort and supported it because of my own experience with the congressional Intelligence Committees some years ago, and particularly with the Foreign Intelligence Surveillance Act. I was persuaded that once we put in place legislation that clearly defined the rules and a process, we achieved substantially enhanced professionalism in pursuing intelligence objectives and reduced the ambiguity about how you deal with the rules. That experience applies to the effort we are making again here. As one looks at all of the past problems, and says how do we get greater professionalism, the first and most important thing to be done is to consider legislating as many tools as we believe are sound. Lastly, I would simply like to report that from this six-month effort, I am encouraged by what I see in the quality of the people being assigned to pursue this problem in the agencies. There is some very good talent working on these problems. And that was not always the experience in the past. Indeed, honesty requires that I note that I avoided any assignment in counterintelligence during my career, because that was not the road for career progress. That is changing, and I hope that one of the things we can help do, and one that the committee should pursue after legislation, is the encouragement for some of the best professionals to be assigned to counterintelligence duties in the future.

TESTIMONY OF ADMIRAL BOBBY R. INMAN

Admiral INMAN. When the Panel began its efforts, some research had been done that helped get us on our way. And one of the things that jumped out was the reality that through the 1950's, a relatively small number of espionage cases occurred. And where they had occurred, more than half of the individuals involved had been recruited.

Ideological sympathy had been the basis, or, in some cases, blackmail. Relatively small numbers of cases of blackmail. The last blackmail cases we find are in the late 50's, early 60's.

From that time on, there is a very dramatic shift. Not only do the number of cases go up, particularly in the 1980's, some of them

began in the 70's, were detected in the 80's. But there is an overwhelming shift from recruitment to volunteer status.

We set about trying to do a very concentrated, very thorough examination of the evidence. We were assisted ably, both by the staff of the Committee and by the Departments and agencies in the Executive branch. They were truly helpful in every way. They opened all the doors. And they helped us assemble a matrix of the cases over these last 20 years to let us try to understand when we looked at the volunteers, and those who had become subject to a different kind of recruitment for cash, could we begin to understand ways that they had become engaged? And, more importantly, could we try to focus on four specific issues.

Deterrence of those who now had access to classified information from becoming engaged in espionage.

If they were not deterred, to detect them and to ensure that we did that as early as possible.

Third, to be able to do an accurate and timely assessment of damage that had been done to this country's security.

And fourth, to ensure that we could prosecute them, i.e., maybe not under the full extent of the espionage laws, but to the best of our abilities to ensure that if an individual sold the secrets of this country, they would spend some time in jail.

In going through this process, we found 19 cases that had occurred from which we have drawn our judgments. And a point I would like to underline is that for each of the proposed elements of legislation, there was a specific challenge we found where we believed the legislation, had it been in place, would have offered a significant prospect of our being able to deter, detect or hopefully prosecute if the espionage had taken place.

In the overwhelming percentage of the cases, the individuals had gone through a full clearance process, had entered into active engagement in their duties where they had access to classified information, and then had decided to become involved in espionage. They were not ideologically sympathetic and they had not been blackmailed in the process.

With very substantial help from the staff and the Community, we have assembled an unclassified matrix which is before you on a very large chart. Unfortunately, we couldn't boil that down to the size that would be very convenient for everyone.

There are a great many more details that are available in a highly classified version which I am sure would be available to the Members of both bodies under the standard rules that govern protection of classified information, should any Member wish to pursue the full classified details. But I believe the summary that is before you, much of it from open source material, will make it easy for anyone to understand where these facts apply.

Two of the most damaging cases, Pelton and Howard, occurred after the individuals left Government. So it became clear that our problems do not end when an individual ends their access. Indeed, in both those cases, substantial damage to our interests took place well after they had left Government service.

There is no clear pattern among these 19 cases that would cover—that would tie them all together that any single law would offer the prospect of detecting or deterring. They are not neither

the most senior nor the most junior employees. Most have been in Government several years. Most still had continuing access when they began their espionage activities. Some were paid relatively small sums of money. Others were paid a great deal.

Even those who were recruited had clearly indicated their willingness to accept money and they did accept financial rewards in almost all cases.

In fact, the only ones where they really didn't profit was where it got preempted very early in the process.

In turning to the detection side, we spent some time trying to understand if we had had a process that let us understand economic distress or unexplained sudden wealth, whether it would have helped us uncover the cases. The answer is that in some cases it would but not in all.

We looked at foreign travel. In a great many of the cases, after the individuals became directly involved in espionage, they traveled outside the United States to make contacts with their case officers and they did not declare that travel. This did not happen in all cases. There are a few cases that were handled entirely in the United States.

There was no single pattern on how contact was established. In some cases, it was by direct telephone call to an embassy, to a consulate, or by a visit. On other occasions, it was by mail. And other rare occasions, outside official premises.

As we winnowed our way through the evidence, and began to narrow in on specific legislation, we found that we needed to take different approaches to deal with detection and the ability to do damage assessment and indeed to do prosecution itself. What we have tried to do here is to improve the prospects for detecting problems when individuals entered the service. And, as I have said before, to deter those already cleared from initiating the contact that might lead to espionage.

We hope this legislation would raise the risk that individuals would run if they undertook espionage activities. First, that they would be caught. Second, that there were at least some laws that they would violate in the process for which they would end up paying a penalty, serving time in jail.

With respect to the criminal laws, we looked beyond the ability to prosecute for espionage in the classic sense that has been considered in the past. As one looks at these legislative proposals, it is clear that access to financial information is a particularly important element. It's also clear—that much of our focus has to be on individuals who have already been cleared. It isn't the initial step but rather, the follow-up investigations, the process for those who already have a clearance.

In trying to come to grips with the vast numbers of people who are cleared, about which we know this Committee has worried in the past, we found that more than four million people have access to classified information. But the bulk of the damage was done by a vastly smaller group that had access to TOP SECRET information or cryptographic information. So the recommendations have focused not on the vast group but on the areas where most damage has been created and where we believe workable rules can be applied.

There are many who could reasonably ask whether our work has been overtaken by events. Indeed, both the Chairman and Vice Chairman have already dealt with this issue. But as we look at what's occurred over the last 15 years, it's clear that the volunteer will look for whomever might pay for the information. It isn't tied to an ideological factor. And clearly in the world out ahead of us, those who are inclined to want to find someone to whom they can sell secrets will continue seeking that opportunity and they are likely to find them, in some cases in countries that have not been involved in the past.

We could spend substantial time going over the chart, but since it's sufficiently far removed from you, I decided not to go through my dog and pony show of trying to point out each single element. We will be happy to come back to them in questions.

But if I may make two personal points in closing that aren't contained in the matrix.

When I first agreed to join this effort, it was based on the experience I had in working with the Select Committees in enactment of legislation, first, the Foreign Intelligence Surveillance Act, then later the Classified Information Procedures Act. I am persuaded that putting in place the legislation contained in the Foreign Intelligence Surveillance Act was a major step not only in clarifying the rules, and ensuring that we went forward in important collection within the law, but it also very substantially increased the professionalism of those who were engaged in that area of collection.

My second point is closely tied. I am very encouraged from this 6 month effort in the quality of individuals that we saw at work now in the various agencies on counterintelligence matters. This was not always the case in earlier years. In fact, honesty compels me to note that I carefully avoided any assignment in counterintelligence duties during my career. It was not a career enhancing route. That says as we go forward, the legislation we are recommending is really only the beginning. The Executive branch has to put in place the regulations. There are other issues they need to address. But areas where I hope the Committee will watch closely will be both the question of resources and pursuing the professionalism of those who are engaged in undertaking the counterintelligence duties.

Thank you very much.

Chairman BOREN. Thank you very much, Admiral Inman.

I believe we will now turn to Professor Edgar to give some detail of the recommendations.

TESTIMONY OF PROFESSOR HAROLD EDGAR

Mr. EDGAR. Thank you, Mr. Chairman.

You have heard about the process the Panel has gone through in making its recommendations. Let me take a moment to make a few general comments about the proposals, and then summarize each of them very briefly.

First, we recognize that most of these proposals require further technical refinement. We would expect this to occur in the legislative process, if, indeed, the Committee chooses to pursue them.

Second, while I believe that all members of the Panel are in agreement with the general thrust of the recommendations, I can't

say that each member agrees with the precise wording of each and every proposal. And I think it is our collective judgment that many of them are capable of further substantive improvement.

Senator METZENBAUM. Is that spelled out for us? Is that spelled out in the Panel's report so we know who dissents at what point?

Mr. EDGAR. No, I don't think it is, Senator Metzenbaum.

Senator METZENBAUM. I think that would be helpful to us.

Mr. EDGAR. We can do that.

Senator METZENBAUM. Thank you.

Mr. EDGAR. Third, these proposals by no means exhaust the possibilities for legislative reform. There are other ideas worthy of pursuit. Those that are presented today primarily respond to specific problems raised by executive agencies that have responsibilities in the counterintelligence area. These agencies have told the Panel that such proposals, if enacted, would make a difference in their ability to deter, detect, and prosecute espionage.

Finally, the Panel, as Eli Jacobs has suggested, has sought a balanced approach. We have tried to avoid recommendations that raise serious civil liberties concerns. Some may quarrel with how well we have achieved this objective, but it was our intent so to act.

Now, if I may proceed, I will provide a short description of each of the Panel's recommendations.

As you will note, there are 13 proposals in all. We've grouped the recommendations in three categories: The first four proposals are intended to improve the personnel security system; the second five proposals are intended to provide additional penalties for activities related to espionage; last four proposals are intended as enhancements to our counterintelligence investigative capabilities.

The first statutory proposal is to establish by statute uniform minimum requirements for everyone granted a TOP SECRET security clearance. The proposal is applicable to all three branches of Government. There is at present no law on the books which establishes such requirements, and, indeed, the Panel found that these requirements vary from agency to agency.

The Panel thought it was important to deal here with only the highest category of security clearance, and with the people who were, by definition, being placed in a position to cause "exceptionally grave" damage to the national security of the United States. So these recommendations are tied to TOP SECRET information.

The Panel's proposal, as the Committee will note, establishes a number of requirements. Among them that persons who receive such a clearance consent to the Government's being able to access certain types of their financial records as well as travel records. Reports of foreign travel would be required of these Government employees, as would reports by them of efforts by foreign nationals to improperly solicit classified information.

The proposal would exempt elected officials and Federal judges from the investigative requirements and would permit the President wide discretion in terms of how the system was implemented.

The second statutory proposal would amend the Right to Financial Privacy Act to permit persons with TOP SECRET clearances to provide their consent to the appropriate governmental authorities obtaining access to certain of their financial records. This proposal complements the provision in the first proposal requiring consent

to provide financial records as a condition of access to TOP SECRET information. It is necessary because the Right to Financial Privacy Act as it is written now permits an individual to consent to access to his financial records for a period of only 3 months.

The third proposal is intended to strengthen the protection of cryptographic information, which, in plain English, means codes and coding machines. The key element of the proposal is to require that all Government communicators, in whatever agency they may be employed, be subject to the possibility of a limited, counterintelligence-scope polygraph examination during the period of their employment as communicators. Basically, they would be asked simply if they were a spy. The Panel's intent is to reach that population of Government employees who run communications centers processing classified information, those who build coding machines, and those who devise codes. The Panel believes the consequence to the United States of the loss of this kind of information justified this requirement. We further believe that the possibility of periodic polygraph examinations will deter people in this category from contemplating espionage.

The fourth proposed new statute would give the Director of the National Security Agency discretionary authority to provide assistance to employees for up to 5 years after they leave the National Security Agency to help them cope with problems. Experience shows that post-employment problems can jeopardize the classified information to which employees have become privy during the period of their employment. The CIA now exercises this authority under existing law, and it has proven useful on occasion to the CIA. While the authority might well be needed in other agencies which handle sensitive information, the Panel was persuaded that the need was particularly acute in the NSA inasmuch as their employees normally spend their careers in positions of unique sensitivity.

Turning to the second group of recommendations, those bearing on criminal espionage, the fifth statutory proposal would make it a crime to possess espionage devices if the intent to violate the espionage statutes can be shown. This proposal is similar to a statute already in place that criminalizes the possession of electronic surveillance equipment, and it is similar as well as to many State statutes making possession of burglary tools a crime where the intent to use them in a burglary can be established. A law such as this would make it possible to prosecute someone found in the possession of such devices as burst transmitters, sophisticated concealed cameras and such, where the intent to commit espionage can be shown. It permits prosecution without the necessity of proving the passage of classified information, and without proving a conspiracy by showing an agreement with another person. This situation is not a common one, but the proposal occasionally can come into play.

The sixth proposed statute would make it a crime to sell to a person representing a foreign power documents or materials that are marked or otherwise identified as TOP SECRET without the Government having to prove as an element of the offense that the classification marking had been properly applied. The Panel's intent in recommending this is to allow the Government to pros-

ecute such conduct without having to reveal the TOP SECRET information in question. The Panel accepts fully the notion that much information is classified that should not be classified. It believes such concern is lessened however insofar as information designated TOP SECRET is involved, and moreover and importantly, that no one can possibly justify selling such materials to known representatives of foreign powers. In these circumstances, we believe the Government should not have to disclose the TOP SECRET information in order to prove its proper classification.

The seventh statutory proposal would add a new provision to that part of the criminal code that deals with the responsibilities of Government employees. It creates a new misdemeanor offense for any Government employee who knowingly removes TOP SECRET documents without authority and retains them at an unauthorized location. The Panel's intent here is to provide the Government with a lesser criminal sanction to deal with Government employees stockpiling highly classified documents with the thought that later they may wish to convert them to personal use. This provision includes both civil and criminal sanctions that might be applied by a court to such cases. The Panel believes the potential seriousness of this kind of behavior, where TOP SECRET information is involved, warrants a special sanction, such as termination of Federal employment. If Government employees must take information which is classified home and keep it for a period of time, they should obtain appropriate authority to do so.

The eighth proposal extends an existing statute which provides for the forfeiture of profits associated with the violation of one of the principle espionage statutes, 18 U.S.C. 794. The proposal would extend that, the so-called "Son of Sam" law to other kinds of espionage convictions.

The ninth proposed statute also amends an existing statute. It would permit the Government to deny retirement pay to United States retirees in the Civil Service Retirement System who are convicted of espionage in foreign courts where the offense concerned United States national defense information. The Attorney General would have to certify that the procedures pursuant to which the conviction had been obtained provided due process rights comparable to those in the United States.

Turning to the last category of recommendations—enhancements of investigative capabilities—our 10th statutory proposal amends or would amend the Fair Credit Reporting Act to permit the FBI to obtain consumer credit reports on persons who are certified by the Director of the FBI as suspected of being agents of foreign powers, as that term has been defined by the Foreign Intelligence Surveillance Act of 1978. Limited identifying information could also be obtained when certified as necessary in other cases. Consumer credit agencies who provide such report would be prohibited from disclosing the request to the consumer involved and this tracks the similar authority the FBI already has with respect to bank records under the Right to Financial Privacy Act of 1979.

The 11th statutory proposal would amend the Electronic Communications Privacy Act of 1986 in order to permit the FBI to obtain subscriber information about persons with unlisted telephone numbers who are called by foreign powers or agents of foreign powers.

Under existing law, the FBI can obtain the toll records of foreign powers and agents of foreign pursuant to a certification process from the Director. These records—in other words, whom the foreign power or agent of foreign power has called—are useless in the instance where the FBI cannot get the names and addresses of the persons whose unlisted telephone numbers were called. Therefore this proposal would authorize the FBI to obtain from the phone company that limited information, namely the information identifying the person whose unlisted telephone number is called by a foreign power or an agent of a foreign power. It does not authorize any other investigative activity on the part of the FBI concerning such a person. Any additional activity would have to be authorized in accordance with other FBI authority.

The 12th statutory proposal would amend the existing statute which provides discretionary authority to the Attorney General to pay rewards for information concerning terrorism, to permit such rewards to be paid for information leading to an arrest or conviction for espionage or for information which had prevented the commission of espionage. The Panel would authorize payments of up to a million dollars for this purpose.

Last but hardly least, the Panel proposes extending the court order procedure now used for electronic surveillances, established by the Foreign Intelligence Surveillance Act, to physical searches done for national security purposes. These are undertaken without a court order under a claim of inherent presidential authority. We think subjecting such searches to a court order process not only would be an important safeguard for the civil liberties of Americans, but would serve also as a protection for the employees of the executive agencies who are asked to engage in such conduct. The Panel believes that the FISA has worked exceedingly well over the last 10 years where electronic surveillances are concerned and we are persuaded that it should be applied to physical searches as well.

Mr. Chairman that concludes my summary of these statutory proposals, and we collectively stand ready to answer your questions.

Chairman BOREN. Thank you very much. Without objection I will enter into our record the text of the Panel's recommendations and any additional comments that members of the Panel might wish to make.

[The document referred to follows:]

May 23, 1990.

THE HONORABLE DAVID L. BOREN,
Chairman.

THE HONORABLE WILLIAM S. COHEN,
Vice Chairman,
Select Committee on Intelligence,
United States Senate,
Washington, DC 20510.

DEAR MR. CHAIRMAN AND VICE CHAIRMAN: As you requested, I am today transmitting on behalf of my colleagues on the Panel thirteen legislative proposals to improve the counterintelligence posture of the United States. These proposals are the product of our review, conducted over the last six months, of the existing statutory framework.

While clearly these proposals can be refined and improved, we believe that the enactment of this or similar legislation would significantly strengthen the ability of the United States to deter, detect, and prosecute persons who turn to espionage. As you will note, the proposals primarily address persons with access to the most sensitive classified information who necessarily possess the capability of doing the greatest harm. We have, on the other hand, attempted to avoid recommendations that would place undue burdens upon the rights and privacy of those who might be affected. The Committee, of course, must decide for itself whether the appropriate balance has been struck.

Our Panel remains ready to assist in any way we can should the Committee decide to pursue these recommendations in the legislative process.

Sincerely,

ELI S. JACOBS.

JACOBS' PANEL—PROPOSED LEGISLATIVE ITEMS

1. AMENDMENT TO THE NATIONAL SECURITY ACT OF 1947 (to provide uniform requirements for persons granted TOP SECRET security clearances)

The National Security Act of 1947 (50 U.S.C. 401 et seq) is amended by inserting at the end thereof the following new title:

"TITLE VIII. UNIFORM REQUIREMENTS FOR ACCESS TO TOP SECRET INFORMATION

Sec. 801. *Minimum Requirements for a TOP SECRET Security Clearance.* Except as provided by section 804 of this title and in accordance with the procedures required by section 805, no person shall be given a security clearance after the effective date of this title by any department, agency, or entity of the United States Government, providing such person access to TOP SECRET information owned, originated, or possessed by the United States, unless such person is a citizen of the United States and has, at a minimum:

(1) Been the subject of a completed background investigation by competent investigative authority;

(2) Agreed to provide consent to appropriate investigative authorities permitting such authorities, during the initial background investigation and for such time as the clearance remains in effect, and for five years thereafter access to:

(a) financial records concerning the subject pursuant to section 1104 of the Right to Financial Privacy Act of 1978;

(b) consumer reports concerning the subject pursuant to section 1681b of the Consumer Credit Protection Act; and

(c) records maintained by commercial entities within the United States pertaining to any travel by the subject outside the United States.

(3) Agreed for such period as such clearance may be in effect, to report to the department, agency, or entity granting the security clearance any travel to foreign countries which has not been authorized as part of the subject's official duties; and

(4) Agreed to report to the Federal Bureau of Investigation or other appropriate investigative authorities any unauthorized contacts with persons known to be foreign nationals or persons representing, or purporting to represent, foreign nationals, where an effort to acquire classified information is made by the foreign national or persons representing a foreign national, or or where such contacts appear intended for this purpose.

Failure by the subject to comply with any of the requirements of this section shall constitute grounds for denial or termination of a security clearance permitting access to TOP SECRET information.

Sec. 802. *Requirements for Additional Investigations.* In accordance with the regulations issued pursuant to section 804 of this title, persons who are granted TOP SECRET security clearances shall, at a minimum:

(1) Be subject to additional background investigations by appropriate governmental authorities during the period such clearance is maintained at no less frequent interval than every five years", *provided* that any failure to satisfy this requirement that is not attributable to the subject of such investigation shall not result in loss or denial of the security clearance concerned; and

(2) Be subject to investigation by appropriate governmental authority at any time to ascertain whether such persons continue to meet the standards for access to TOP SECRET information.

Sec. 803. *Definitions.* As used in this title—

(1) The term "security clearance" means a determination by competent governmental authority to permit a person routine access to information that has been marked or designated as requiring protection in the interests of national security.

(2) The phrase "department, agency, or entity of the United States Government" includes the Executive, Legislative and Judicial Branches of the United States Government, and encompasses all elements thereof.

(3) The term "TOP SECRET information" means information that has been marked or otherwise designated pursuant to law or Executive Order 12356, or successive Executive Orders, as information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security.

Sec. 804. *Exceptions and Waiver Authority.*

(1) Notwithstanding section 801 of this title, persons holding elected positions in the Executive and Legislative branches, or who are judges of courts established pursuant to Article III of the Constitution of the United States, shall, by virtue of their positions, be entitled to access to such TOP SECRET information as may be necessary to carry out their official duties without obtaining a security clearance based upon compliance with section 801.

(2) The President, or his designee, may waive the requirements imposed in section 801, either for particular categories of cases or as they apply to particular departments, agencies, or entities within the United States Government, whenever he deems it necessary in the interests of national security; *provided, however,* that all such waivers are recorded and all waivers that apply to particular departments, agencies, or entities within the Executive Branch are reported within thirty days to the Select Committee on Intelligence of the Senate and to the Permanent Select Committee on Intelligence of the House of Representatives.

Sec. 805. *Implementing Procedures.*

Within 180 days of the effective date of this Act, and after appropriate consultation with the Congress and the Administrative Office of the U.S. Courts, the President shall issue regulations to implement this title which shall be binding upon the Executive, Legislative, and Judicial branches of Government, and incorporated into appropriate policy instruments within each branch of Government. In addition, such regulations shall provide for a central office to monitor the implementation and operation of this title, to include the establishment of a single registry to maintain accountability of all TOP SECRET clearances issued pursuant to this title.

Sec. 806. *Effective Date.* The requirements of this title shall go into effect 180 days after enactment.

EXPLANATION: This would amend the National Security Act of 1947 by creating a new title which establishes certain uniform, minimum requirements in order to obtain a TOP SECRET security clearance.

Currently, there is no statute that establishes the requirements for security clearances at any level. Nor is there an Executive Order that sets such standards for all employees and contractors of the Executive branch. These requirements are largely left to agency-by-agency determination.

The Legislative and Judicial branches acquiesce to Executive agency requirements in terms of clearing their employees, but are not legally bound to do so.

These institutional shortcomings are especially critical as they pertain to access to the most sensitive category of classified information. There is a need to ensure that minimum levels of investigation are performed for all persons with TOP SECRET access, regardless of where they are employed.

There is also a need to ensure that sufficient attention is given by the Government to those categories of information which are the most likely to indicate possible security problems, particularly financial information and information relating to travel outside the United States. While access to such records does not mean some loss of privacy in terms of the individuals affected, where such persons are being given the capability of doing "exceptionally grave damage" to the nation's security, it does not seem unreasonable to ask them to relinquish a measure of their personal privacy. Persons who object to providing access to the government to such information need not seek positions which require TOP SECRET clearances.

The proposed legislation would require initial background investigations, and reinvestigations every five years thereafter during the period of access.

The proposal would require persons who are given TOP SECRET clearances to consent to government access to their financial and consumer records, and to records pertaining to their travel outside the United States, during the period the clearance is in effect and for five years thereafter. Although no affirmative report-

ing obligation is imposed on the employee concerned, the agency which granted the clearance would be able to assess situations which may arise that indicate a security problem involving an employee with a high-level-clearance.

The proposal also requires reporting of all foreign travel during the period of access, as well as any contacts with foreign nationals which occur during the period of access or thereafter, where an attempt to obtain classified information without authority is made or suspected.

The proposal exempts elected officials and federal judges from the clearance requirements, and provides general authority for the President to waive the statute where necessary, so long as such waivers are reported to the Congressional intelligence committees.

The proposal would require implementing procedures to be issued by the President after appropriate consultation with the other branches of Government.

The Act itself would take effect 180 days after enactment, and would apply only to TOP SECRET clearances granted after such date.

2. AMENDMENT TO RIGHT TO FINANCIAL PRIVACY ACT (to permit access for purposes of security clearance investigations)

Section 1104 of the Right to Financial Privacy Act of 1978 (12 U.S.C. 3404) is amended by adding at the end thereof the following new subsection (d):

"(d) *Consent by customers with high-level security clearances.* Notwithstanding the provisions of subsection (a), above, a customer who is the subject of a personnel security investigation by an authorized Government authority, as a condition of receiving or maintaining a security clearance at the level of TOP SECRET, pursuant to applicable Executive order or statute, may authorize nonrevokable disclosure of all financial records maintained by financial institutions for the period of the customer's access to TOP SECRET information and for up to five years after access to such information has been terminated, by the Government authority responsible for the conduct of such investigation for an authorized security purpose. Such authority shall be contained in a signed and dated statement of the customer, which identifies the financial records which are authorized to be disclosed. Such statement also may authorize the disclosure of financial records of accounts opened during the period covered by the consent agreement which are not identifiable at the time such consent is provided. A copy of such statement shall be provided by the Government authority concerned to the financial institution from which disclosure is sought, together with the certification required pursuant to section 1103(b) [12 U.S.C. 3403(b) of this title."

EXPLANATION: Under the existing statute, a customer can only consent to access for a period not to exceed three months, and such consent is revocable. The existing law also gives the customer the right to ask if his financial records have been disclosed. The statute also has special provisions that permit access by the FBI for counterintelligence purposes based upon the certification of the FBI Director that the person involved is an agent of a foreign power. In this circumstance, the financial institution is precluded from advising its customer.

The purpose of this provision would be to give Government agencies responsible for assessing cleared personnel the ability to obtain access to financial records to ascertain vulnerabilities or problems of persons cleared for access to highly sensitive information. For persons cleared for TOP SECRET, they might be asked to consent to Government access for a period of five years after access has been terminated.

Given the large population affected and in the absence of any information indicating an "agent of a foreign power" or a violation of law, this proposed statutory change does *not* include a waiver of the customer's right to find out if his financial records have been disclosed to the investigating authority.

It is also to be noted that the Act already limits any dissemination of financial records outside the requesting agency except where the agency certifies that it is needed for a law enforcement purpose within the jurisdiction of another agency.

Finally, to explain the reference to the certification requirement in 3404(b). The existing law requires the Government authority seeking the records to certify to the financial institution that it has complied with the applicable provisions of the statute. This should be retained here, and would encompass a requirement to certify that the subject of the investigation currently maintains a TOP SECRET clearance or has held such clearance in the last five years.

A copy of the section of the Act being amended is attached.

§ 3403. Customer authorizations.

(a) Statement furnished by customer to financial institution and Government authority; contents. A customer may authorize disclosure under section 1102(1) [12

USCS § 3402(1)] if he furnishes to the financial institution and to the Government authority seeking to obtain such disclosure a signed and dated statement which—

(1) authorizes such disclosure for a period not in excess of three months;

(2) states that the customer may revoke such authorization at any time before the financial records are disclosed;

(3) identifies the financial records which are authorized to be disclosed;

(4) specifies the purposes for which, and the Government authority to which, such records may be disclosed; and

(5) states the customer's rights under this title.

(b) Authorization as condition of doing business prohibited. No such authorization shall be required as a condition of doing business with any financial institution.

(c) Right of customer to access to financial institution's record of disclosures. The customer has the right, unless the Government authority obtains a court order as provided in section 1109 [12 USCS § 3409], to obtain a copy of the record which the financial institution shall keep of all instances in which the customer's record is disclosed to a Government authority pursuant to this section, including the identity of the Government authority to which such disclosure is made.

3. AMENDMENT TO THE NATIONAL SECURITY ACT OF 1947 (50 U.S.C. 401 et seq.) (to provide protection to cryptographic information)

The National Security Act of 1947 (50 U.S.C. 401 et seq.) is amended by inserting at the end the following new title:

"TITLE VIII—PROTECTION OF CRYPTOGRAPHIC INFORMATION

Sec. 801(a). *Requirements for Access to Cryptographic Information.* Any person who is granted access to classified cryptographic information or routine, recurring access to spaces in which classified cryptographic key is produced or processed, or is assigned responsibilities as a custodian of classified cryptographic key, shall, as a condition of receiving such access, or being assigned such responsibilities, and at a minimum:

(1) Meet the requirements to TOP SECRET information pursuant to [proposal 1]; and

(2) Be subject to a periodic polygraph examinations conducted by appropriate governmental authorities, limited in scope to questions of a counterintelligence nature, during the period of such access. Failure to submit to such examinations shall be grounds for removal from access to cryptographic information or spaces.

(b) For purposes of this section—

(1) the term "classified cryptographic information" means any information classified by the United States Government pursuant to law or Executive Order concerning the details of (i) the nature, preparation, or use of any code, cipher, or cryptographic system of the United States; or (ii) the design, construction, use, maintenance, or repair of any cryptographic equipment;

(2) "custodian of classified cryptographic key" means positions that require access to classified cryptographic key beyond that required to operate cryptographic equipment designed for personal or office use, future editions of classified cryptographic key, or classified cryptographic key used for multiple devices.

(3) the term "classified cryptographic key" means any information (usually a sequence of random binary digits), in any form, classified by the United States Government pursuant to law or Executive Order that is used to set up and periodically change the operations performed by any cryptographic equipment;

(4) the term "cryptographic equipment" means any device, apparatus or appliance used, or prepared, or planned for use by the United States for the purpose of authenticating communications or disguising or concealing the contents, significance, or meanings of communications;

(5) the phrase "questions of a counterintelligence nature" means specified questions to ascertain whether the subject is engaged in espionage against the United States on behalf of a foreign government or knows persons who are so engaged.

Sec. 802. *Implementing Regulations.* The President shall, within 180 days of enactment of this section, promulgate regulations to implement the provisions of this title. Copies of such regulations shall be provided to the Armed Services Committees of the Senate and House of Representatives, the Select Committee on Intelligence of the Senate, and the Permanent Select Committee on Intelligence of the House of Representatives."

EXPLANATION: This amendment would carve out by statute Government employees and contractors who develop, build, and operate cryptographic equipment, or who operate communications centers with access to large amounts of keying ma-

terial, and subject them to certain specified security requirements. In addition to requiring such persons meet the same standards as persons with TOP SECRET clearances, the proposal would subject such persons to the possibility of having to take a limited polygraph examination during their period of access to cryptographic information.

Inasmuch as it would be extremely difficult to place all of the nuances involved into the statute itself, this draft would leave the details to implementing regulations issued by the President to cover all departments and agencies. It is anticipated that such regulations would provide safeguards similar to those now in effect at the Department of Defense, in terms of limiting the use and effect of the results of such examinations.

4. AMENDMENT TO THE NATIONAL SECURITY AGENCY ACT OF 1959 (50 U.S.C. 402 note) (to authorize the Director of NSA to take certain actions to deal with problem employees after termination of employment)

The National Security Agency Act of 1959 (50 U.S.C. 402 note) is amended by inserting at the end thereof the following new section:

"Sec. 17. (a) The Director of the National Security Agency may, in his discretion and notwithstanding any other law, use appropriated funds to assist employees who have been in sensitive positions who are found to be ineligible for continued access to Sensitive Compartmented Information and employment with the Agency, or whose employment with the Agency has been terminated in finding and qualifying for subsequent employment, in receiving treatment of medical or psychological disabilities, and in providing necessary financial support during periods of unemployment, if, in the judgment of the Director, such assistance is essential to maintain the judgment and emotional stability of such employee and avoid circumstances that might lead to the disclosure of classified information to which such employee had had access. Assistance provided under this section shall not be provided any longer than five years after the termination of the employment of the employee concerned.

(b) The Director of the National Security Agency shall report annually to the Appropriations Committees of the Senate and House of Representatives, the Select Committee on Intelligence of the Senate, and to the Permanent Select Committee on Intelligence of the House of Representatives with respect to any expenditure made pursuant to this section."

EXPLANATION: NSA now lacks the legal authority to assist employees who have personal problems which may lead them to turn to espionage. CIA does have such authority and it has proved useful from time to time.

This amendment would provide authority for NSA to assist problem employees for a period of five years after their employment in the areas which NSA cites are its greatest need.

5. AMENDMENT TO CHAPTER 37 OF TITLE 18, U.S.C. (to create a new criminal offense for the possession of espionage devices)

Chapter 37 of title 18, United States Code, is amended by inserting at the end thereof the following new section:

"Section 800. *Possession of Espionage Devices.* Whoever knowingly maintains possession of any electronic, mechanical, or other device or equipment within the United States, or in areas within the jurisdiction of the United States, knowing or having reason to know that the design and capability of such device or equipment renders it primarily useful for the purpose of surreptitiously collecting or communicating information, with the intent of utilizing such device or equipment to undertake actions in violation of sections 793, 794 or 798 of this title, shall be fined not more than $10,000 or imprisoned not more than five years, or both."

EXPLANATION: This proposed amendment would add a new offense to the espionage laws, making possession of espionage paraphernalia with the intent to use such paraphernalia to commit espionage a crime in and of itself.

This amendment is similar to "burglary equipment" statutes in many states, as well as to 18 U.S.C. 2512, which, among other things, criminalizes the possession of wire or oral communication interception devices.

This provision would provide prosecutors in certain circumstances with an option that would not be available under existing law, i.e. the ability to prosecute persons who can be shown to possess equipment to carry out espionage and have the intent to do so, without having to prove that espionage itself was actually committed, or that such persons were involved in a conspiracy to commit espionage.

Although it might be desirable from the point of view of a prosecutor only to prove possession of such paraphernalia, because most of the devices or equipment at issue could be used for surreptitious purposes other than espionage, it appears that

proof of intent to commit espionage is constitutionally necessary. Such intent might be shown, however, by other available evidence in a given set of circumstance: for example, proof of meetings with known hostile intelligence officers, or notes showing names and address of such contacts, or the discovery of a radio transmitter with capabilities to communicate only with satellites operated by foreign governments. In short, proof of intent should be possible in certain circumstances.

6. AMENDMENT OF CHAPTER 37 OF TITLE 18, UNITED STATES CODE (to create a new offense for selling to foreign governments documents and other materials designated as TOP SECRET)

Chapter 37 of title 18, United States Code, is amended by inserting after section 794 the following new subsection:

"Section 794a. *Sale or Transfer of Documents or Materials Marked as TOP SECRET.*

(1) No person shall knowingly sell or otherwise transfer for any valuable consideration to a person or persons representing a foreign power, as defined in 50 U.S.C. 1801, or their intermediaries, (1) any document, writing, code book, sketch, photograph, map, model, instrument, equipment, electronic storage media, or other material, or portion thereof, that is marked or otherwise designated in any manner, pursuant to applicable law and Executive order, as TOP SECRET, or (2); any such document, writing, code book, sketch, photograph, map, model, instrument, equipment, electronic storage media, or other material, or portion thereof, which has had such marking or designation removed without authority and the person making the sale or transfer is aware of such removal. This section is not violated by a person who makes such sale or transfer pursuant to applicable law or Executive branch authority.

(2) In any prosecution under this section, whether or not the information or material marked or designated as TOP SECRET has been properly marked or designated pursuant to applicable law or Executive Order shall not be an element of the offense.

(3) Violation of this section shall be punishable by imprisonment for a maximum of 15 years.

EXPLANATION: This proposed amendment would substantially overlap present espionage laws. Existing law prohibits any communication, whether by sale or not, of information related to the national defense in circumstances where the information is to be used to injure the United States or advantage a foreign nation. The term "national defense" has been defined broadly by the courts, and properly classified defense information is national defense information protected by the espionage laws.

Similarly, the kind of "advantage" to a foreign nation necessary to sustain an espionage prosecution is *de minimus.* Case law suggests that it is enough simply that the information is of a kind that a foreign government wants to know.

In a conventional espionage prosecution, however, the Government must reveal in open court the information that was transferred as part of its obligation to prove the information's national defense character; moreover, the Government must present testimony establishing that the information's compromise might injure the United States or advantage the foreign nation that receives it. The prosecution itself has the potential of widening the security breach.

With respect to one category of intelligence information, communications intelligence, a more particular law, 18 U.S.C. 798, has been construed to make the fact of classification dispositive, thus freeing the prosecution from explaining why the document or information is important.

The proposed amendment is much narrower than present espionage laws in that it reaches only TOP SECRET documents and materials, rather than the umbrella concept of national defense information. Moreover, it does not reach any and all unauthorized communications of such materials, but only their sale or transfer for valuable consideration to "foreign powers"—a term defined in the Foreign Intelligence Surveillance Act to include foreign governments and factions thereof. Thus, the statute has no application to the general problems of leaks of government information.

What is new about the statute is that in cases that it reaches, the government will have the option of proceeding with no obligation to reveal the contents of the TOP SECRET document or material at issue, or to explain why the information contained in it was important to the national defense. Plainly this limits no important individual interest. A person has no right to sell foreign governments documents or materials marked or otherwise designated as TOP SECRET, even if one takes the view that the system for classifying information produces massive overclassification.

Moreover, because the national defense significance of the information is not a material element of this crime, the Government, if it proceeds pursuant to its provisions, can investigate the damage of information transfer caused with no fear that those impact assessments are discovered by the defense, (on the theory that the impact assessments tend to prove that no injury or advantage occurred).

In most espionage prosecutions, the Government will probably prefer to proceed in a conventional way, and disclose the seriousness of the security breach in order to justify the extremely strict penalties the espionage laws provide. Still, legal authority to proceed without heightening security losses should be established to provide an additional option in appropriate cases.

7. AMENDMENT TO CHAPTER 93 OF TITLE 18, UNITED STATES CODE (to provide a lesser criminal offense for the removal of TOP SECRET documents by government employees and contractors)

Chapter 93 of title 18. U.S.C., is amended by inserting at the end thereof the following new section:

"Section 1924. *Removal of TOP SECRET documents or material.* Whoever, being an officer, employee or person acting for or on behalf of the United States or any department or agency thereof, and having, by virtue of his office, employment or position, become possessed of documents or materials classified at the level of TOP SECRET pursuant to applicable law or Executive Order, willfully and knowingly removes such documents or materials without authority and retains such documents or materials at an unauthorized location, shall be fined not more than $10,000, or imprisoned for not more than one year, or be removed from office or employment, or be subjected to any combination of such sanctions."

EXPLANATION:

—The espionage statutes (18 U.S.C. 793(f)) make it a crime for someone entrusted with classified material to fail to report "to his superior officer" that such material has been "illegally removed from its proper place of custody". Persons found guilty of this crime are to be fined not more than $10,000 or imprisoned for not more than ten years, or both.

—Although theoretically available to address cases where classified information is removed without authority by government officials either while in government or when they leave government, the nature of the offense (espionage) and the gravity of the charge (a felony) has not offered prosecutors a very palatable alternative in these circumstances. If the information was not compromised, the punishment seemed more severe than the offense.

—It has become a relatively common phenomenon for persons with high-level clearances to remove copies of classified documents to their residences and "stockpile" them for possible future use, where an intent to sell them to hostile intelligence services cannot be established.

—The proposed amendment would create a new offense for government employees and contractors that would not be part of the espionage statutes but rather part of the criminal code dealing with the responsibilities of public officers and employees. It would apply only to TOP SECRET information rather than classified information as a whole. It would not require proof of compromise but proof that the document had been (1) willfully and knowingly removed without authority (2) with the intent to retain it at an unauthorized location.

—The proposed amendment would also provide for removal of the individual from office or employment, an option that is not available under the espionage statute.

8. AMENDMENT TO 18 U.S.C. 3681 (to expand existing statute regarding forfeiture of collateral profits of crime to additional espionage offenses)

Section 3681(a) of title 18, United States Code, is amended by:

(1) striking "section 794" and inserting in lieu thereof "sections 793, 794, and 798"; and

(2) by adding at the end of the section the following new sentence: "For purposes of this section, convictions pursuant to military courts-martial for offenses comparable to violations of section 793, 794, and 798 of this title, or convictions by foreign courts for offenses which, if perpetrated within the United States, would constitute offenses under sections 793, 794, and 798 of this title, shall be considered as convictions for which actions may be ordered Pursuant to this section."

EXPLANATION: Congress amended the existing "son of Sam" statute in 1986 to provide for the forfeiture of collateral profits arising from crimes under 18 U.S.C. 794. The amendment did not reach similar criminal misconduct under other provisions of the espionage laws: 18 U.S.C. 793 (gathering, transmitting or losing defense information) and 18 U.S.C. 798 (the disclosure of classified information relating to

communications intelligence). The proposed amendment would broaden the application of the forfeiture provision to cover these categories of criminal misconduct. Although there is some question as to whether all that section 793 criminalizes (e.g. negligent loss of national defense information) should necessarily justify action under this special forfeiture statute, it is believed that such decision should be left to the determination of the Justice Department and the courts in enforcing this provision.

The amendment would also provide that convictions of similar offense by military courts martial, or convictions by foreign courts for offenses which, if undertaken within the United States, would constitute violations of the statutes that are covered, would permit similar actions by a court.

Under—this statute, the Attorney General must institute a civil proceeding to recover the proceeds at issue. The legislative history of this amendment might indicate that where the conviction occurred in a foreign court, the Attorney General should take into account whether the individual concerned received basic rights of due process, in terms of whether to invoke this provision.

A copy of 18 U.S.C. 3681 and 3682 is attached.

§ 3681. Order of special forfeiture.

(a) Upon the motion of the United States attorney made at any time after conviction of a defendant for an offense under section 794 of this title or for an offense against the United States resulting in physical harm to an individual, and after notice to any interested party, the court shall, if the court determines that the interest of justice or an order of restitution under this title so requires order such defendant to forfeit all or any part of proceeds received or to be received by that defendant, or a transferee of that defendant, from a contract relating to a depiction of such crime in a movie, book, newspaper, magazine, radio or television production, or live entertainment of any kind, or an expression of that defendant's thoughts, opinions, or emotions regarding such crime.

(b) An order issued under subsection (a) of this section shall require that the person with whom the defendant contracts pay to the Attorney General any proceeds due the defendant under such contract.

(c)(1) Proceeds paid to the Attorney General under this section shall be retained in escrow in the Crime Victims Fund in the Treasury by the Attorney General for five years after the date of an order under this section, but during that five year period may—

(A) be levied upon to satisfy—

(i) a money judgment rendered by a United States district court in favor of a victim of an offense for which such defendant has been convicted, or a legal representative of such victim; and

(ii) a fine imposed by a court of the United States, and

(B) if ordered by the court in the interest of justice, be used to—

(i) satisfy a money judgment rendered in any court in favor of a victim of any offense for which such defendant has been convicted, or a legal representative of such victim; and

(ii) pay for legal representation of the defendant in matters arising from the offense for which such defendant has been convicted, but no more than 20 percent of the total proceeds may be so used.

(2) The court shall direct the disposition of all such proceeds in the possession of the Attorney General at the end of such five years and may require that all or any part of such proceeds be released from escrow and paid into the Crime Victims Fund in the Treasury.

(d) As used in this section, the term "interested party" includes the defendant and any transferee of proceeds due the defendant under the contract, the person with whom the defendant has contracted, and any person physically harmed as a result of the offense for which the defendant has been convicted.

§ 3682. Notice to victims of order of special forfeiture.

The United States attorney shall, within thirty days after the imposition of an order under this chapter and at such other times as the Attorney General may require, publish in a newspaper of general circulation in the district in which the offense for which a defendant was convicted occurred, a notice that states—

(1) the name of, and other identifying information about, the defendant;

(2) the offense for which the defendant was convicted,; and

(3) that the court has ordered a special forfeiture of certain proceeds that may be used to satisfy a judgment obtained against the defendant by a victim of an offense for which the defendant has been convicted.

9. AMENDMENT TO FEDERAL RETIREMENT STATUTE (5 U.S.C. 8312) (To permit the U.S. to deny annuities or retired pay to persons convicted of espionage in foreign courts involving U.S. information)

Section 8312 of title 5, United States Code, is amended by inserting at the end thereof the following new subsection:

"(d) For purposes of subsections (b) (1) and (c) (1) of this section, an offense within the purview of such subsections is established if the Attorney General certifies (1) that an individual subject to this chapter has been convicted by a court within a foreign country in circumstances in which the conduct violates the statutes enumerated in subsections (b) (1) and (c) (1), or would violate such statutes, had such conduct taken place within the United States, and that such conviction is not being appealed; (2) that such conviction was obtained in accordance with procedures that provided the defendant due process rights comparable to such rights provided by the U.S. Constitution, and such conviction was based upon evidence which would have been admissible in the Courts of the United States; and (3) that such convictions occurred after the date of enactment of this subsection."

EXPLANATION: Under existing law, the U.S. can deny annuities or retired pay to persons (civilian and military) who have been convicted of espionage and related crimes. The law also provides that the U.S. may deny such annuities and retired pay to anyone who is indicted in the U.S. on such charges and—who willfully remains outside the U.S. for more than a year with knowledge of the indictment.

There is no provision in existing law, however, to deny annuities or retired pay to U.S. retirees who may be convicted in a foreign court of similar offenses involving U.S. classified information.

This situation has, in fact, occurred over the last year. A U.S. citizen and retiree of the Army, Zoltan Szabo, was convicted of espionage in Austria for his cooperation with the Hungarian intelligence service, as part of the Clyde Conrad case. Even after conviction, he continues to draw a U.S. pension.

The amendment would provide that U.S. retirees could be denied a pension if the Attorney General certified: (1) that such retiree has been convicted in a foreign court for conduct that violates the enumerated statutes, or would violate such statutes had it occurred in the United States; (2) that the conviction was obtained in accordance with procedures that provided the defendant with due process and was based upon evidence admissible in United States courts; and (3) occurred after the dates of enactment of this provision.

As drafted, this amendment applies only to the Civil Service Retirement System. Retirees under other federal retirement programs should be covered by similar amendments.

§ 8312. Conviction of certain offenses

(a) An individual, or his survivor or beneficiary, may not be paid annuity or retired pay on the basis of the service of the individual which is creditable toward the annuity or retired pay, subject to the exceptions in section 8311(2) and (3) of this title [5 USCS § 8311(2) and (3)], if the individual—

(1) was convicted, before, on, or after September 1, 1954, of an offense named by subsection (b) of this section, to the extent provided by that subsection or

(2) was convicted, before, on, or after September 26, 1961, of an offense named by subsection (c) of this section, to the extent provided by that subsection.

The prohibition on payment of annuity or retired pay applies—

(A) with respect to the offenses named by subsection (b) of this section, to the period after the date of the conviction or after September 1, 1954, whichever is later; and

(B) with respect to the offenses named by subsection (c) of this section, to the period after the date of conviction or after September 26, 1961, whichever is later.

(b) The following are the offenses to which subsection (a) of this section applies if the individual was convicted before, on, or after September 1, 1954:

(1) An offense within the purview of—

(A) section 792 (harboring or concealing persons), 793 (gathering, transmitting, or losing defense information), 794 (gathering or delivering defense information to aid foreign government), or 798 (disclosure of classified information), of chapter 37 (relating to espionage and censorship) of title 18 [18 USCS §§ 792-794, 798];

(B) chapter 105 (relating to sabotage) of title 18 [18 USCS § 2151 et seq.];

(C) section 2381 (treason), 2382 (misprision of treason), 2383 (rebellion or insurrection), 2384 (seditious conspiracy), 2385 (advocating overthrow of government), 2387 (activities affecting armed forces generally), 2388 (activities

affecting armed forces during war), 2389 (recruiting for service against United States), or 2390 (enlistment to serve against United States), of chapter 115 (relating to treason, sedition, and subversive activities) of title 18 [18 Uscs §§ 2381-2385, 2387-2390];

(D) section 10(b)(2), (3), or (4) of the Atomic Energy Act of 1946 (60 Stat. 766. 767),as in effect before August 30, 1954;

(E) section 16(a) or (b) of the Atomic Energy Act of 1946 (60 Stat. 773), as in effect before August 30, 1954, insofar as the offense is committed with intent to injure the United States or with intent to secure an advantage to a foreign nation; or

(F) an earlier statute on which a statute named by subparagraph (A), (B), or (C) of this paragraph (1) is based.

(2) An offense within the purview of—

(A) article 104 (aiding the enemy) or article 106 (spies) of the Uniform Code of Military Justice (chapter 47, of title 10) [10 USCS §§ 904, 906] or an earlier article on which article 104 or article 106, as the case may be, is based; or

(B) a current article of the Uniform Code of Military Justice (or an earlier article on which the current article is based) [10 USCS §§ 801 et seq.] not named by subparagraph (A) of this paragraph (2) on the basis of charges and specifications describing a violation of a statute named by paragraph (1), (3), or (4) of this subsection, if the executed sentence includes death, dishonorable discharge, or dismissal from the service, or if the defendant dies before execution of that sentence as finally approved.

(3) Perjury committed under the statutes of the United States or the District of Columbia—

(A) in falsely denying the commission of an act which constitutes an offense within the purview of—

(i) a statute named by paragraph (1) of this subsection; or

(ii)an article or statute named by paragraph (2) of this subsection insofar as the offense is within the purview of an article or statute named by paragraph (1) or (2) (A) of this subsection;

(B) in falsely testifying before a Federal grand jury, court of the United States, or court-martial with respect to his service as an employee in connection with a matter involving or relating to an interference with or endangerment of, or involving or relating to a plan or attempt to interfere with or endanger, the national security or defense of the United States; or

(C) in falsely testifying before a congressional committee in connection with a matter under inquiry before the congressional committee involving or relating to an interference with or endangerment of, or involving or relating to a plan or attempt to interfere with or endanger, the national security or defense of the United States.

(4) Subornation of perjury committed in connection with the false denial or false testimony of another individual as specified by paragraph (3) of this subsection.

(c) following are the offenses to which subsection (a) of this section applies if the individual was convicted before, on, or after September 26, 1961:

(1) An offense within the purview of—

(A) section 2272 (violation of specific sections) or 2273 (violation of sections generally of chapter 23 of title 42) of title 42 [42 USCS § 2272 or § 2273] insofar as the offense is committed with intent to injure the United States or with intent to secure an advantage to a foreign nation;

(B) section 2274 (communication of restricted data), 2275 (receipt of restricted data), or 2276 (tampering with restricted data) of title 42 [42 USCS § 2274, § 2275 or § 2276]; or

(C) section 783 (conspiracy and communication or receipt of classified information) of title 50 [50 USCS § 783] or section 601 of the National Security Act of 1947 (50 U.S.C. 421) (relating to intelligence identities) [50 USCS § 421].

(2) An offense within the purview of a current article of the Uniform Code of Military Justice (chapter 47 of title 10) [10 USCS §§ 801 et seq.] or an earlier article on which the current article is based, as the case may be, on the basis of charges and specifications describing a violation of a statute named by paragraph (1), (3), or (4) of this subsection, if the executed sentence includes death, dishonorable discharge, or dismissal from the service, or if the defendant dies before execution of that sentence as finally approved.

(3) Perjury committed under the statutes of the United States or the District of Columbia in falsely denying the commission of an act which constitutes an offense within the purview of a statute named by paragraph (1) of this subsection.

(4) Subornation of perjury committed in connection with the false denial, of another individual as specified by paragraph (3) of this subsection.

10. AMENDMENT TO THE CONSUMER CREDIT PROTECTION ACT (to permit the FBI to obtain consumer reports on persons believed to be agents of foreign powers)

Sec. 1681(f) of title 15, United States Code, is amended by inserting "(1)" before the text of this section, and by inserting at the end thereof the following new subsection:

"(2). *Disclosures to the Federal Bureau of Investigation.*

(a) Notwithstanding the provisions of section 1681b of this title, a consumer reporting agency shall furnish a consumer report to the Federal Bureau of Investigation when presented with a request for a consumer report made pursuant to this subsection by the Federal Bureau of Investigation, provided that the Director of the Federal Bureau of Investigation, or his designee, certifies in writing to the consumer reporting agency that such records are sought in connection with an authorized foreign counterintelligence investigation and that there are specific and articulable facts giving reason to believe the person to whom the requested consumer report relates is an agent of a foreign power as defined in Section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801). Notwithstanding section 1681g of this title, no consumer credit reporting agency, officer, employee or agent of such institution shall disclose to any person that the Federal Bureau of Investigation has sought or obtained a consumer report respecting any consumer pursuant to this subsection.

(b) A consumer reporting agency shall also furnish to a representative of the Federal Bureau of Investigation identifying information respecting any consumer, as specified in section (1), above, when presented with a written request signed by the Director of the Federal Bureau of Investigation, or the Director's designee, stating that such information is necessary to the conduct of an authorized foreign counterintelligence investigation. Notwithstanding section 1681g of this title, no consumer credit reporting agency, officer, employee or agent of such institution shall disclose to any person that the Federal Bureau of Investigation has sought or obtained identifying information respecting any consumer pursuant to this subsection.

EXPLANATION: This amendment would provide the FBI with new authority to request consumer reports and identifying information from consumer reporting agencies on persons who are subject of foreign counterintelligence investigations without having such reports being made known to the subject. It is similar to authority contained in section 3414 of the Right to Financial Privacy Act of 1979, giving the FBI authority to access financial records covered by that statute for foreign counterintelligence purposes.

The existing statute authorizes consumer reporting agencies to provide consumer reports only with the written consent of the consumer, or to persons who intend to use the information for a variety of specified purposes (e.g. for employment, in connection with a credit transaction, eligibility for a license or government benefit, or otherwise the requestor "has a legitimate business need"). In other words, while use in a foreign counterintelligence investigation is not a specified use, the uses that are specified are quite broad, suggesting a rather marginal guarantee of privacy. The proposed amendment would, however, prohibit a consumer reporting agency from advising a consumer (as it is otherwise required to do) of requests made for such reports within the preceding six-month period.

A copy of the two relevant sections of the Consumer Credit protection Act is attached.

§ 1681b. Permissible purposes of consumer reports

A consumer reporting agency may furnish a consumer report under the following circumstances and no other:

(1) In response to the order of a court having jurisdiction to issue such an order.

(2) In accordance with the written instructions of the consumer to whom it relates.

(3) To a person which it has reason to believe—

(A) intends to use the information in connection with a credit transaction involving the consumer on whom the information is to be fur-

nished and involving the extension of credit to, or review or collection of an account of, the consumer; or

(B) intends to use the information for employment purposes; or

(C) intends to use the information in connection with the underwriting of insurance involving the consumer; or

(D) intends to use the information in connection with a determination of the consumer's eligibility for a license or other benefit granted by a governmental instrumentality required by law to consider an applicant's financial responsibility or status; or

(E) otherwise has a legitimate business need for the information in connection with a business transaction involving the consumer.

§ 1681g. Disclosures to consumers

(a) Every consumer reporting agency shall, upon request and proper identification of any consumer, clearly and accurately disclose to the consumer:

(1) The nature and substance of all information (except medical information) in its files on the consumer at the time of the request.

(2) The sources of the information: except that the sources of information acquired solely for use in preparing an investigative consumer report and actually used for no other purpose need not be disclosed: Provided, that in the event an action is brought under this title [15 USCS §§ 1681 et seq.], such sources shall be available to the plaintiff under appropriate discovery procedures in the court in which the action is brought.

(3) The recipients of any consumer report on the consumer which it has furnished—

(A) for employment purposes within the two-year period preceding the request, and

(B) for any other purpose within the six-month period preceding the request.

(b) The requirements of subsection (a) respecting the disclosure of sources of information and the recipients of consumer reports to not apply to information received or consumer reports furnished prior to the effective date of this title [180 days following Oct. 26, 1970; see effective date note to 15 USCS § 1681] except to the extent that the matter involved is contained in the files of the consumer reporting agency on that date.

11. AMENDMENT TO THE ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986 (18 U.S.C. 2709) (to permit FBI access to subscriber information of persons with unlisted numbers who are called by "foreign powers" or "agents of foreign powers")

Section 2709 of title 18, United States Code, is amended by striking subsection (b) and inserting in lieu thereof the following:

"(b) *Required certification.* The Director of the Federal Bureau of Investigation (or an individual within the Federal Bureau of Investigation designated for this purpose by the Director) may:

(1) request such information and records if the Director (or the Director's designee) certifies in writing to the wire or electronic communication service provider to which the request is made that—

(A) the information sought is relevant to an authorized foreign counterintelligence investigation; and

(B) there are specific and articulable facts giving reason to believe that the person or entity to whom the information sought pertains is a foreign power or an agent of a foreign power as defined in Section 101 of the Foreign Surveillance Act of 1978 (50 U.S.C. 1801); and

(2) request subscriber information regarding a person or entity if the Director certifies in writing to the wire or electronic communications service provider to which the request is made that—

(A) the information sought is relevant to an authorized foreign counterintelligence investigation; and

(B) that information available to the Federal Bureau of Investigation indicates there is reason to believe that communications facilities registered in the name of the person or entity have been used, through the services of such provider, in communication with a foreign power or an agent of a foreign power as defined by Section 101 of the Foreign Intelligence Act of 1978 (50 U.S.C. 1801).

EXPLANATION: The problem to be addressed here is the failure of the existing statute (18 U.S.C. 2709), as interpreted by the Justice Department, to permit the FBI to obtain identifying data from the telephone company on persons with unlisted

telephone numbers who are called by foreign powers (e.g. diplomatic establishments) or agents of foreign powers (e.g. spies). The FBI can obtain toll records and other information on foreign powers and agents of foreign powers under the Act, but under the Justice Department interpretation, is precluded from ascertaining the identity of persons who are called whose numbers are unlisted. This amendment would provide the FBI with the authority to get "subscriber information" only—not the toll records—of such persons. The FBI would have to rely on other information to which it had access before proceeding with further investigative inquiries of the person who called in, once identified.

Subsection (1) is essentially a slight non-substantive revision of existing law.

Subsection (2) contains the new authority referred to above.

A copy of the section being amended is attached.

§ 2709. Counterintelligence access to telephone toll and transactional records

(a) DUTY TO PROVIDE.—A wire or electronic communications service provider shall comply with a request for subscriber information and toll billing records information, or electronic communication transactional records in its custody or possession made by the Director of the Federal Bureau of Investigation under subsection (b) of this section.

(b) REQUIRED CERTIFICATION.—The Director of the Federal Bureau of Investigation (or an individual within the Federal Bureau of Investigation designated for this purpose by the Director) may request such information and records if the Director (or the Director's designee) certifies in writing to the wire or electronic communication service provider to which the request is made that—

(1) the information sought is relevant to an authorized foreign counterintelligence investigation; and

(2) there are specific and articulable facts giving reason to believe that the person or entity to whom the information sought pertains 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); and

(c) PROHIBITION OF CERTAIN DISCLOSURE.—No wire or electronic communication provider, or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.

(d) DISSEMINATION BY BUREAU.—The Federal Bureau of Investigation may disseminate information and records obtained under this section only as provided in guidelines approved by the Attorney General for foreign intelligence collection and foreign counterintelligence investigations conducted by the Federal Bureau of Investigation, and, with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency.

(e) REQUIREMENT THAT CERTAIN CONGRESSIONAL BODIES BE INFORMED.—On a semi-annual basis the Director of the Federal Bureau of Investigation shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate concerning all requests made under subsection (b) of this section.

12. AMENDMENT TO CHAPTER 204 OF TITLE 18 (to provide for rewards for information concerning espionage)

Chapter 204 of title 18, United States Code, is amended:

(1) by inserting at the end of the title of the chapter "and Espionage;"

(2) by designating all the language of section 3071 after the title of the section as subsection (1) and renumbering subsections (1), (2), and (3) as subsections (A), (B), and (C), respectively; and by inserting a new subsection (2) as follows:

"(2) With respect to acts of espionage involving or directed at U.S. information classified in the interests of national security, 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 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 against the United States; or

(3) leading to the prevention or frustration of an act of espionage against the United States."

(3) by striking "$500,000" in section 3072, and inserting in lieu thereof "$1,000,000"; and

(4) by inserting at the end of section 3077 the following new subsections:

"(8) 'act of espionage' means an activity that is a violation of section 794 or section 798 of this title; and

(9) 'U.S. information classified in the interests of national security' means information originated by or on behalf of the United States Government concerning the national defense and foreign relations of the United States that has been determined pursuant to law or Executive order to require protection against unauthorized disclosure and that has been so designated."

EXPLANATION: This amendment would provide discretionary authority for the Attorney General to pay rewards for information leading to the arrest or conviction of an individual for espionage, or to the prevention of espionage, similar to authority that exists for the Attorney General to pay rewards for information leading to arrests or convictions for acts of terrorism. Indeed, the proposed amendment would modify the chapter in Title 18 that authorizes such rewards, incorporating the same conditions and safeguards as the reward system for reports on terrorism.

A copy of chapter 204 is attached.

§ 3071. Information for which rewards authorized

With respect to acts of terrorism primarily within the territorial jurisdiction 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 the commission of an act of terrorism against a Unites States person or United States property; or

(2) leading to the arrest or conviction, in any country, of any individual or individuals for conspiring or attempting to commit an act of terrorism against a United States person or property; or

(3) leading to the prevention, frustration, or favorable resolution of an act of terrorism against a United States person or property.

§ 3072. Determination of entitlement; maximum amount; Presidential approval; conclusiveness

The Attorney General shall determine whether an individual furnishing information described in section 3017 [18 USCS § 3071] is entitled to a reward and the amount to be paid. A reward under this section may be in an amount not to exceed $500,000. A reward of $100,000 or more may not be made without the approval of the President or the Attorney General personally. A determination made by the Attorney General or the President under this chapter [18 USCS §§ 3071 et seq.] shall be final and conclusive, and no court shall have power or jurisdiction to review it.

§ 3073. Protection of identity

Any reward granted under this chapter [18 USCS §§ 3071 et seq.] shall be certified for payment by the Attorney General. If it is determined that the identity of the recipient of a reward or of the members of the recipients immediate family must be protected, the Attorney General may take such measures in connection with the payment of the reward as deemed necessary to effect such protection.

§ 3074. Exception of governmental officials

No officer or employee of any governmental entity who, while in the performance of his or her official duties, furnishes the information described in section 3071 [18 USCS § 3071] shall be eligible for any monetary reward under this chapter [18 §§ 3071 et seq.].

§ 3075. Authorization for appropriations

There are authorized to be appropriated, without fiscal year limitation, $5,000,000 for the purpose of the chapter [18 USCS §§ 3071 et seq.].

§ 3076. Eligibility for witness security program

Any individual (and the immediate family of such individual) who furnishes information which could justify a reward by the Attorney General under this chapter or by the Secretary of State under section 36 of the State Department Basic Authorities Act of 1956 may, in the discretion of the Attorney General, participate in the Attorney General's witness security program authorized under chapter 224 of this title.

§ 3077. Definitions

As used in this chapter [18 USCS §§ 3071 et seq.], the term—

(1) "act of terrorism" means an activity that—

(A) involves a violent act or an act dangerous to human life that is a violation of the criminal laws of the United States or of any State, or that

would be a criminal violation if committed within the jurisdiction of the United States or of any State; and

(B) appears to be intended—

(i) to intimidate/or coerce a civilian population;

(ii) to influence the policy of a government by intimidation or coercion; or

(iii) to affect the conduct of a government by assassination or kidnaping.

(2) "United States person" means—

(A) a national of the United States as defined in section 101(a)(22) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(22) [8 USCS §§ 1101(a)(22)];

(B) an alien lawfully admitted for permanent residence in the United States as defined in section 101(a)(20) of the Immigration and Nationality Act (8 U.S.C. § 1101(a)(22) [8 USCS §§ 1101(a)(22)];

(C) any person within the United States;

(D) any employee or contractor of the United States Government, regardless of nationality, who is the victim or intended victim of an act of terrorism by virtue of that employment;

(E) a sole proprietorship, partnership, company, or association composed principally of nationals or permanent resident aliens of the United States; and

(F) a corporation organized under the laws of the United States, any State, the District of Columbia, or any territory or possession of the United States, and a foreign subsidiary of such corporation.

(3) "United States property" means any real or personal property which is within the United States or, if outside the United States, the actual or beneficial ownership of which rests in a United States person or any Federal or State governmental entity of the United States.

(4) "United States," when used in a geographical sense, includes Puerto Rica and all territories and possessions of the United States.

(5) "State" includes any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any other possession or territory of the United States.

(6) "governmental entity" includes the Government of the United States, any State or political subdivision thereof, any foreign country, and any state, provincial, municipal, or other political subdivision of a foreign country.

(7) "Attorney General" means the Attorney General of the United States or that official designated as the Attorney General to perform the Attorney General's responsibilities under this chapter [18 USCS §§ 3071 et seq.].

13. AMENDMENTS TO FOREIGN INTELLIGENCE SURVEILLANCE ACT (50 U.S.C. 1801) (to provide for a court order process for physical searches similar to that for electronic surveillance)

The Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq) is amended as follows:

1. The Table of Contents in Title I is amended by inserting "AND SEARCH" after "ELECTRONIC SURVEILLANCE".

2. The title of Title I is amended by inserting "AND PHYSICAL SEARCH" after "ELECTRONIC SURVEILLANCE."

3. Section 101(h) is amended by—

(a) inserting in the introductory clause after "surveillance" the words "or physical searches"; and

(b) by inserting in subsection (1) after "surveillance" the words "or search".

4. Section 101(k) is amended by striking the text and inserting in lieu thereof the following: "Aggrieved person means a person who is the target of electronic surveillance or physical search or any other person whose communications, activities or property were subject to electronic surveillance or physical search."

5. Section 101 is amended by inserting at the end thereof the following new subsection:

(p) "Physical search" means any physical intrusion into the premises or property (including examination of the interior of property by technical means) or any seizure, reproduction or alteration of information, material or property, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

6. Section 102 is amended by:

(a) inserting after "Electronic Surveillance" in the title of the section "or Physical Search"; and

(b) inserting in subsection (b) after the words "electronic surveillance" (at the first place they appear in the text), "or physical search".

7. Section 103(a) is amended by inserting "or physical searches" after the words "electronic surveillance", at each place they appear in the text.

8. Section 104 is amended by:

(a) inserting in the first sentence of subsection (a) after "electronic surveillance" the words "or physical searches";

(b) inserting in subsection (a) (3) after "electronic surveillance" the words "or physical search";

(c) inserting in subsection (a)(4)(A) after "electronic surveillance" the words "or physical search";

(d) inserting in subsection (a)(4)(B) after "directed", "or a physical search is conducted,";

(e) inserting at the end of subsection (a) (4) "and" and inserting a new subsection as follows:

"(C) where approval is sought for a physical search, the facility, place, or property to be searched is owned, used,—or possessed by, or is in transit to, a—foreign power or agent of a foreign power."

(f) inserting in subsection (a) (6) after "surveillance", the words "or search";

(g) inserting before the text of subsection (a) (8) "where approval for electronic surveillance is sought.";

(h) inserting before the text of subsection (a) (10) "where approval for electronic surveillance is sought,";

(i) inserting at the end of subsection (a) a new subsection (12) as follows:

"(12) where approval for more than one physical search is sought, a statement of the number of physical searches to be conducted, and the period of time required for such searches."; and

(j) inserting in subsection 104(b) after "electronic surveillance", "or physical search".

9. Section 105 is amended by:

(a) inserting in subsection (a) after each use of "electronic surveillance" the words "or physical search"; and

(b) inserting after subsection (a)(3)(B) the following new subsection:

"(C) where authority for a physical search is sought, each facility, place, or item of property to be searched is owned, used, or possessed by, or is in transit to, a foreign power or agent of a foreign power."

(c) inserting in the introductory clause of subsection 105(b) and in subsections 105(b) (1)(A)–(E) after "surveillance", wherever it may appear, the words "or physical search".

(d) inserting in subsection 105(b)(1)(F) after "whenever", the words "electronic surveillance is authorized and";

(e) striking "and" at the end of subsection—105(b)(1)(F) and inserting the following new subsection:

"(G) whenever more than one physical search is authorized under the order, the authorized scope of each search and what minimization procedures shall apply to the information acquired by each search; and,

(f) inserting in subsections 105(c) and (d) (1) after "surveillance", wherever it may appear, the words "or physical search";

(g) inserting at the end of subsection (d) (1) the following new sentence: "Any order issued under this section authorizing a physical search shall constitute a search warrant authorized by law for purposes of any other law."

(h) striking "a" before the word "surveillance" in subsection 105(d) (2), and inserting in lieu thereof "an electronic";

(i) inserting in subsections 105(d)(3) and (e), after each use of "surveillance", the words "or physical search"; and

10. Sections 106, 107, 108, 109, 110 and 111 are amended by inserting "or physical search" after each appearance of the word "surveillance" wherever it appears.

EXPLANATION: These amendments would expand the coverage of the Foreign Intelligence Surveillance Act of 1978 to physical searches for national security purposes that are now conducted in the United States without a court order, pursuant to approval of the Attorney General, who has been delegated such authority by the President. There is no judicial involvement in this process as there is with electronic surveillance as a safeguard to government overreaching. Further, it is clear that, as a practical matter, investigators do not appear comfortable acting under a claim of inherent Presidential authority to justify such searches if they should be chal-

lenged. Requiring a court order for such searches would provide protection for those involved in terms of their potential liability to civil or criminal lawsuits. Similarly, prosecutors sometimes shy away from using evidence collected in such manner since it will inevitably lead to challenges at trial.

The experience under the Foreign Intelligence Surveillance Act in the area of electronic surveillance has been excellent. Similar procedures are desirable to regulate physical searches.

A copy of the Foreign Intelligence Surveillance Act of 1978 is attached.

C. OTHER INTELLIGENCE STATUTES

FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978

Public Law 95-511
95th Congress

An Act

To authorize electronic surveillance to obtain foreign intelligence information.

Oct. 25, 1978
[S. 1566]

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That this Act may be cited as the "Foreign Intelligence Surveillance Act of 1978".

Foreign Intelligence Surveillance Act of 1978.
50 USC 1801 note.

TABLE OF CONTENTS

TITLE I—ELECTRONIC SURVEILLANCE WITHIN THE UNITED STATES FOR FOREIGN INTELLIGENCE PURPOSES

DEFINITIONS

SEC. 101. As used in this title: 50 USC 1801.

(a) "Foreign power" means—
(1) a foreign government or any component thereof, whether or not recognized by the United States;
(2) a faction of a foreign nation or nations, not substantially composed of United States persons;
(3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;
(4) a group engaged in international terrorism or activities in preparation therefor;
(5) a foreign-based political organization, not substantially composed of United States persons; or
(6) an entity that is directed and controlled by a foreign government or governments.

(b) "Agent of a foreign power" means—
(1) any person other than a United States person, who—
(A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4);

(B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities; or

(2) any person who—

(A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;

(B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;

(C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power; or

(D) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C).

(c) "International terrorism" means activities that—

(1) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State;

(2) appear to be intended—

(A) to intimidate or coerce a civilian population;

(B) to influence the policy of a government by intimidation or coercion; or

(C) to affect the conduct of a government by assassination or kidnapping; and

(3) occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

(d) "Sabotage" means activities that involve a violation of chapter 105 of title 18, United States Code, or that would involve such a violation if committed against the United States.

18 USC 2151 *et seq.*

(e) "Foreign intelligence information" means—

(1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against—

(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or

(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to—

(A) the national defense or the security of the United States; or

(B) the conduct of the foreign affairs of the United States.

(f) "Electronic surveillance" means—

(1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;

(2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States;

(3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or

(4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

(g) "Attorney General" means the Attorney General of the United States (or Acting Attorney General) or the Deputy Attorney General.

(h) "Minimization procedures", with respect to electronic surveillance, means—

(1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;

(2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in subsection (e)(1), shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance;

(3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about

to be committed and that is to be retained or disseminated for law enforcement purposes; and

(4) notwithstanding paragraphs (1), (2), and (3), with respect to any electronic surveillance approved pursuant to section 102(a), procedures that require that no contents of any communication to which a United States person is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than twenty-four hours unless a court order under section 105 is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person.

(i) "United States person" means a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 101(a)(20) of the Immigration and Nationality Act), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3).

8 USC 1101.

(j) "United States", when used in a geographic sense, means all areas under the territorial sovereignty of the United States and the Trust Territory of the Pacific Islands.

(k) "Aggrieved person" means a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance.

(l) "Wire communication" means any communication while it is being carried by a wire, cable, or other like connection furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications.

(m) "Person" means any individual, including any officer or employee of the Federal Government, or any group, entity, association, corporation, or foreign power.

(n) "Contents", when used with respect to a communication, includes any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication.

(o) "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Trust Territory of the Pacific Islands, and any territory or possession of the United States.

AUTHORIZATION FOR ELECTRONIC SURVEILLANCE FOR FOREIGN INTELLIGENCE PURPOSES

50 USC 1802.

SEC. 102. (a)(1) Notwithstanding any other law, the President, through the Attorney General, may authorize electronic surveillance without a court order under this title to acquire foreign intelligence information for periods of up to one year if the Attorney General certifies in writing under oath that—

(A) the electronic surveillance is solely directed at—

(i) the acquisition of the contents of communications transmitted by means of communications used exclusively between or among foreign powers, as defined in section 101(a)(1), (2), or (3); or

(ii) the acquisition of technical intelligence, other than the spoken communications of individuals, from property or premises under the open and exclusive control of a foreign power, as defined in section 101(a) (1), (2), or (3);

(B) there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party; and

(C) the proposed minimization procedures with respect to such surveillance meet the definition of minimization procedures under section 101(h); and

Report to congressional committees.

if the Attorney General reports such minimization procedures and any changes thereto to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence at least thirty days prior to their effective date, unless the Attorney General determines immediate action is required and notifies the committees immediately of such minimization procedures and the reason for their becoming effective immediately.

(2) An electronic surveillance authorized by this subsection may be conducted only in accordance with the Attorney General's certification and the minimization procedures adopted by him. The Attorney General shall assess compliance with such procedures and shall report such assessments to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence under the provisions of section 108(a).

Report to congressional committees.

(3) The Attorney General shall immediately transmit under seal to the court established under section 103(a) a copy of his certification. Such certification shall be maintained under security measures established by the Chief Justice with the concurrence of the Attorney General, in consultation with the Director of Central Intelligence, and shall remain sealed unless—

(A) an application for a court order with respect to the surveillance is made under sections 101(h)(4) and 104; or

(B) the certification is necessary to determine the legality of the surveillance under section 106(f).

Communication common carrier, duties.

(4) With respect to electronic surveillance authorized by this subsection, the Attorney General may direct a specified communication common carrier to—

(A) furnish all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier is providing its customers; and

(B) maintain under security procedures approved by the Attorney General and the Director of Central Intelligence any records concerning the surveillance or the aid furnished which such carrier wishes to retain.

Compensation.

The Government shall compensate, at the prevailing rate, such carrier for furnishing such aid.

Applications approval.

(b) Applications for a court order under this title are authorized if the President has, by written authorization, empowered the Attorney General to approve applications to the court having jurisdiction under section 103, and a judge to whom an application is made may, notwithstanding any other law, grant an order, in conformity with section 105, approving electronic surveillance of a foreign power or an agent of a foreign power for the purpose of obtaining foreign intelligence information, except that the court shall not have jurisdic-

tion to grant any order approving electronic surveillance directed solely as described in paragraph (1)(A) of subsection (a) unless such surveillance may involve the acquisition of communications of any United States person.

DESIGNATION OF JUDGES

Court to hear applications and grant orders. 50 USC 1803.

SEC. 103. (a) The Chief Justice of the United States shall publicly designate seven district court judges from seven of the United States judicial circuits who shall constitute a court which shall have jurisdiction to hear applications for and grant orders approving electronic surveillance anywhere within the United States under the procedures set forth in this Act, except that no judge designated under this subsection shall hear the same application for electronic surveillance under this Act which has been denied previously by another judge designated under this subsection. If any judge so designated denies an application for an order authorizing electronic surveillance under this Act, such judge shall provide immediately for the record a written statement of each reason for his decision and, on motion of the United States, the record shall be transmitted, under seal, to the court of review established in subsection (b).

Court of review.

(b) The Chief Justice shall publicly designate three judges, one of whom shall be publicly designated as the presiding judge, from the United States district courts or courts of appeals who together shall comprise a court of review which shall have jurisdiction to review the denial of any application made under this Act. If such court determines that the application was properly denied, the court shall immediately provide for the record a written statement of each reason for its decision and, on petition of the United States for a writ of certiorari, the record shall be transmitted under seal to the Supreme Court, which shall have jurisdiction to review such decision.

Record of proceedings.

(c) Proceedings under this Act shall be conducted as expeditiously as possible. The record of proceedings under this Act, including applications made and orders granted, shall be maintained under security measures established by the Chief Justice in consultation with the Attorney General and the Director of Central Intelligence.

Tenure.

(d) Each judge designated under this section shall so serve for a maximum of seven years and shall not be eligible for redesignation, except that the judges first designated under subsection (a) shall be designated for terms of from one to seven years so that one term expires each year, and that judges first designated under subsection (b) shall be designated for terms of three, five, and seven years.

APPLICATION FOR AN ORDER

50 USC 1804.

SEC. 104. (a) Each application for an order approving electronic surveillance under this title shall be made by a Federal officer in writing upon oath or affirmation to a judge having jurisdiction under section 103. Each application shall require the approval of the Attorney General based upon his finding that it satisfies the criteria and requirements of such application as set forth in this title. It shall include—

Approval of Attorney General.

(1) the identity of the Federal officer making the application;

(2) the authority conferred on the Attorney General by the President of the United States and the approval of the Attorney General to make the application;

(3) the identity, if known, or a description of the target of the electronic surveillance;

(4) a statement of the facts and circumstances relied upon by the applicant to justify his belief that—

(A) the target of the electronic surveillance is a foreign power or an agent of a foreign power; and

(B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;

(5) a statement of the proposed minimization procedures;

(6) a detailed description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance;

(7) a certification or certifications by the Assistant to the President for National Security Affairs or an executive branch official or officials designated by the President from among those executive officers employed in the area of national security or defense and appointed by the President with the advice and consent of the Senate—

(A) that the certifying official deems the information sought to be foreign intelligence information;

(B) that the purpose of the surveillance is to obtain foreign intelligence information;

(C) that such information cannot reasonably be obtained by normal investigative techniques;

(D) that designates the type of foreign intelligence information being sought according to the categories described in section 101(e); and

(E) including a statement of the basis for the certification that—

(i) the information sought is the type of foreign intelligence information designated; and

(ii) such information cannot reasonably be obtained by normal investigative techniques;

(8) a statement of the means by which the surveillance will be effected and a statement whether physical entry is required to effect the surveillance;

(9) a statement of the facts concerning all previous applications that have been made to any judge under this title involving any of the persons, facilities, or places specified in the application, and the action taken on each previous application;

(10) a statement of the period of time for which the electronic surveillance is required to be maintained, and if the nature of the intelligence gathering is such that the approval of the use of electronic surveillance under this title should not automatically terminate when the described type of information has first been obtained, a description of facts supporting the belief that additional information of the same type will be obtained thereafter; and

(11) whenever more than one electronic, mechanical or other surveillance device is to be used with respect to a particular proposed electronic surveillance, the coverage of the devices involved and what minimization procedures apply to information acquired by each device.

Foreign power, information exclusion.

(b) Whenever the target of the electronic surveillance is a foreign power, as defined in section 101(a) (1), (2), or (3), and each of the facilities or places at which the surveillance is directed is owned, leased, or exclusively used by that foreign power, the application need not contain the information required by paragraphs (6), (7)(E), (8),

and (11) of subsection (a), but shall state whether physical entry is required to effect the surveillance and shall contain such information about the surveillance techniques and communications or other information concerning United States persons likely to be obtained as may be necessary to assess the proposed minimization procedures.

(c) The Attorney General may require any other affidavit or certification from any other officer in connection with the application.

(d) The judge may require the applicant to furnish such other information as may be necessary to make the determinations required by section 105.

ISSUANCE OF AN ORDER

50 USC 1805.

SEC. 105. (a) Upon an application made pursuant to section 104, the judge shall enter an ex parte order as requested or as modified approving the electronic surveillance if he finds that—

(1) the President has authorized the Attorney General to approve applications for electronic surveillance for foreign intelligence information;

(2) the application has been made by a Federal officer and approved by the Attorney General;

(3) on the basis of the facts submitted by the applicant there is probable cause to believe that—

(A) the target of the electronic surveillance is a foreign power or an agent of a foreign power: *Provided*, That no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States; and

(B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;

(4) the proposed minimization procedures meet the definition of minimization procedures under section 101(h); and

(5) the application which has been filed contains all statements and certifications required by section 104 and, if the target is a United States person, the certification or certifications are not clearly erroneous on the basis of the statement made under section 104(a)(7)(E) and any other information furnished under section 104(d).

(b) An order approving an electronic surveillance under this section shall—

(1) specify—

(A) the identity, if known, or a description of the target of the electronic surveillance;

(B) the nature and location of each of the facilities or places at which the electronic surveillance will be directed;

(C) the type of information sought to be acquired and the type of communications or activities to be subjected to the surveillance;

(D) the means by which the electronic surveillance will be effected and whether physical entry will be used to effect the surveillance;

(E) the period of time during which the electronic surveillance is approved; and

(F) whenever more than one electronic, mechanical, or other surveillance device is to be used under the order, the authorized coverage of the devices involved and what minimi-

zation procedures shall apply to information subject to acquisition by each device; and

(2) direct—

(A) that the minimization procedures be followed;

(B) that, upon the request of the applicant, a specified communication or other common carrier, landlord, custodian, or other specified person furnish the applicant forthwith all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier, landlord, custodian, or other person is providing that target of electronic surveillance;

(C) that such carrier, landlord, custodian, or other person maintain under security procedures approved by the Attorney General and the Director of Central Intelligence any records concerning the surveillance or the aid furnished that such person wishes to retain; and

(D) that the applicant compensate, at the prevailing rate, such carrier, landlord, custodian, or other person for furnishing such aid.

(c) Whenever the target of the electronic surveillance is a foreign power, as defined in section 101(a) (1), (2), or (3), and each of the facilities or places at which the surveillance is directed is owned, leased, or exclusively used by that foreign power, the order need not contain the information required by subparagraphs (C), (D), and (F) of subsection (b)(1), but shall generally describe the information sought, the communications or activities to be subjected to the surveillance, and the type of electronic surveillance involved, including whether physical entry is required.

Approval.

(d)(1) An order issued under this section may approve an electronic surveillance for the period necessary to achieve its purpose, or for ninety days, whichever is less, except that an order under this section shall approve an electronic surveillance targeted against a foreign power, as defined in section 101(a) (1), (2), or (3), for the period specified in the application or for one year, whichever is less.

Extensions of an order.

(2) Extensions of an order issued under this title may be granted on the same basis as an original order upon an application for an extension and new findings made in the same manner as required for an original order, except that an extension of an order under this Act for a surveillance targeted against a foreign power, as defined in section 101(a) (5) or (6), or against a foreign power as defined in section 101(a)(4) that is not a United States person, may be for a period not to exceed one year if the judge finds probable cause to believe that no communication of any individual United States person will be acquired during the period.

Review of circumstances of order or extension.

(3) At or before the end of the period of time for which electronic surveillance is approved by an order or an extension, the judge may assess compliance with the minimization procedures by reviewing the circumstances under which information concerning United States persons was acquired, retained, or disseminated.

(e) Notwithstanding any other provision of this title, when the Attorney General reasonably determines that—

(1) an emergency situation exists with respect to the employment of electronic surveillance to obtain foreign intelligence information before an order authorizing such surveillance can with due diligence be obtained; and

(2) the factual basis for issuance of an order under this title to approve such surveillance exists;

Emergency order.

he may authorize the emergency employment of electronic surveillance if a judge having jurisdiction under section 103 is informed by the Attorney General or his designee at the time of such authorization that the decision has been made to employ emergency electronic surveillance and if an application in accordance with this title is made to that judge as soon as practicable, but not more than twenty-four hours after the Attorney General authorizes such surveillance. If the Attorney General authorizes such emergency employment of electronic surveillance, he shall require that the minimization procedures required by this title for the issuance of a judicial order be followed. In the absence of a judicial order approving such electronic surveillance, the surveillance shall terminate when the information sought is obtained, when the application for the order is denied, or after the expiration of twenty-four hours from the time of authorization by the Attorney General, whichever is earliest. In the event that such application for approval is denied, or in any other case where the electronic surveillance is terminated and no order is issued approving the surveillance, no information obtained or evidence derived from such surveillance shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired from such surveillance shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person. A denial of the application made under this subsection may be reviewed as provided in section 103.

Denial of application.

Review.

Testing of electronic equipment.

(f) Notwithstanding any other provision of this title, officers, employees, or agents of the United States are authorized in the normal course of their official duties to conduct electronic surveillance not targeted against the communications of any particular person or persons, under procedures approved by the Attorney General, solely to—

(1) test the capability of electronic equipment, if—

(A) it is not reasonable to obtain the consent of the persons incidentally subjected to the surveillance;

(B) the test is limited in extent and duration to that necessary to determine the capability of the equipment;

(C) the contents of any communication acquired are retained and used only for the purpose of determining the capability of the equipment, are disclosed only to test personnel, and are destroyed before or immediately upon completion of the test; and

Termination.

(D) *Provided*, That the test may exceed ninety days only with the prior approval of the Attorney General;

(2) determine the existence and capability of electronic surveillance equipment being used by persons not authorized to conduct electronic surveillance, if—

(A) it is not reasonable to obtain the consent of persons incidentally subjected to the surveillance;

(B) such electronic surveillance is limited in extent and duration to that necessary to determine the existence and capability of such equipment; and

(C) any information acquired by such surveillance is used only to enforce chapter 119 of title 18, United States Code, or section 705 of the Communications Act of 1934, or to protect information from unauthorized surveillance; or

18 USC 2510 *et seq.*
47 USC 605.

(3) train intelligence personnel in the use of electronic surveillance equipment, if—

Training of intelligence personnel, conditions.

(A) it is not reasonable to—

(i) obtain the consent of the persons incidentally subjected to the surveillance;

(ii) train persons in the course of surveillances otherwise authorized by this title; or

(iii) train persons in the use of such equipment without engaging in electronic surveillance;

(B) such electronic surveillance is limited in extent and duration to that necessary to train the personnel in the use of the equipment; and

(C) no contents of any communication acquired are retained or disseminated for any purpose, but are destroyed as soon as reasonably possible.

(g) Certifications made by the Attorney General pursuant to section 102(a) and applications made and orders granted under this title shall be retained for a period of at least ten years from the date of the certification or application.

Record retention requirement.

USE OF INFORMATION

SEC. 106. (a) Information acquired from an electronic surveillance conducted pursuant to this title concerning any United States person may be used and disclosed by Federal officers and employees without the consent of the United States person only in accordance with the minimization procedures required by this title. No otherwise privileged communication obtained in accordance with, or in violation of, the provisions of this title shall lose its privileged character. No information acquired from an electronic surveillance pursuant to this title may be used or disclosed by Federal officers or employees except for lawful purposes.

50 USC 1806.

(b) No information acquired pursuant to this title shall be disclosed for law enforcement purposes unless such disclosure is accompanied by a statement that such information, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General.

Statement for disclosure.

(c) Whenever the Government intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, against an aggrieved person, any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this title, the Government shall, prior to the trial, hearing, or other proceeding or at a reasonable time prior to an effort to so disclose or so use that information or submit it in evidence, notify the aggrieved person and the court or other authority in which the information is to be disclosed or used that the Government intends to so disclose or so use such information.

(d) Whenever any State or political subdivision thereof intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of a State or a political subdivsion thereof, against an aggrieved person any information obtained or

derived from an electronic surveillance of that aggrieved person pursuant to the authority of this title, the State or political subdivision thereof shall notify the aggrieved person, the court or other authority in which the information is to be disclosed or used, and the Attorney General that the State or political subdivision thereof intends to so disclose or so use such information.

(e) Any person against whom evidence obtained or derived from an electronic surveillance to which he is an aggrieved person is to be, or has been, introduced or otherwise used or disclosed in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the evidence obtained or derived from such electronic surveillance on the grounds that—

(1) the information was unlawfully acquired; or

(2) the surveillance was not made in conformity with an order of authorization or approval.

Such a motion shall be made before the trial, hearing, or other proceeding unless there was no opportunity to make such a motion or the person was not aware of the grounds of the motion.

(f) Whenever a court or other authority is notified pursuant to subsection (c) or (d), or whenever a motion is made pursuant to subsection (e), or whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States or any State before any court or other authority of the United States or any State to discover or obtain applications or orders or other materials relating to electronic surveillance or to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance under this Act, the United States district court or, where the motion is made before another authority, the United States district court in the same district as the authority, shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted. In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.

(g) If the United States district court pursuant to subsection (f) determines that the surveillance was not lawfully authorized or conducted, it shall, in accordance with the requirements of law, suppress the evidence which was unlawfully obtained or derived from electronic surveillance of the aggrieved person or otherwise grant the motion of the aggrieved person. If the court determines that the surveillance was lawfully authorized and conducted, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure.

(h) Orders granting motions or requests under subsection (g), decisions under this section that electronic surveillance was not lawfully authorized or conducted, and orders of the United States district court requiring review or granting disclosure of applications, orders, or other materials relating to a surveillance shall be final orders and binding upon all courts of the United States and the several States

except a United States court of appeals and the Supreme Court.

(i) In circumstances involving the unintentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States, such contents shall be destroyed upon recognition, unless the Attorney General determines that the contents indicate a threat of death or serious bodily harm to any person.

Disposal of contents.

(j) If an emergency employment of electronic surveillance is authorized under section 105(e) and a subsequent order approving the surveillance is not obtained, the judge shall cause to be served on any United States person named in the application and on such other United States persons subject to electronic surveillance as the judge may determine in his discretion it is in the interest of justice to serve, notice of—

(1) the fact of the application;

(2) the period of the surveillance; and

(3) the fact that during the period information was or was not obtained.

On an ex parte showing of good cause to the judge the serving of the notice required by this subsection may be postponed or suspended for a period not to exceed ninety days. Thereafter, on a further ex parte showing of good cause, the court shall forego ordering the serving of the notice required under this subsection.

Postponement or suspension of notice, time limitation.

REPORT OF ELECTRONIC SURVEILLANCE

SEC. 107. In April of each year, the Attorney General shall transmit to the Administrative Office of the United States Court and to Congress a report setting forth with respect to the preceding calendar year—

Report to Congress. 50 USC 1807.

(a) the total number of applications made for orders and extensions of orders approving electronic surveillance under this title; and

(b) the total number of such orders and extensions either granted, modified, or denied.

CONGRESSIONAL OVERSIGHT

SEC. 108. (a) On a semiannual basis the Attorney General shall fully inform the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence concerning all electronic surveillance under this title. Nothing in this title shall be deemed to limit the authority and responsibility of the appropriate committees of each House of Congress to obtain such information as they may need to carry out their respective functions and duties.

Report to congressional committees. 50 USC 1808.

(b) On or before one year after the effective date of this Act and on the same day each year for four years thereafter, the Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence shall report respectively to the House of Representatives and the Senate, concerning the implementation of this Act. Said reports shall include but not be limited to an analysis and recommendations concerning whether this Act should be (1) amended, (2) repealed, or (3) permitted to continue in effect without amendment.

Report of congressional committees to Congress.

PENALTIES

50 USC 1809. SEC. 109. (a) OFFENSE.—A person is guilty of an offense if he intentionally—

(1) engages in electronic surveillance under color of law except as authorized by statute; or

(2) discloses or uses information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized by statute.

(b) DEFENSE.—It is a defense to a prosecution under subsection (a) that the defendant was a law enforcement or investigative officer engaged in the course of his official duties and the electronic surveillance was authorized by and conducted pursuant to a search warrant or court order of a court of competent jurisdiction.

(c) PENALTY.—An offense described in this section is punishable by a fine of not more than $10,000 or imprisonment for not more than five years, or both.

(d) JURISDICTION.—There is Federal jurisdiction over an offense under this section if the person committing the offense was an officer or employee of the United States at the time the offense was committed.

CIVIL LIABILITY

50 USC 1810. SEC. 110. CIVIL ACTION.—An aggrieved person, other than a foreign power or an agent of a foreign power, as defined in section 101 (a) or (b)(1)(A), respectively, who has been subjected to an electronic surveillance or about whom information obtained by electronic surveillance of such person has been disclosed or used in violation of section 109 shall have a cause of action against any person who committed such violation and shall be entitled to recover—

(a) actual damages, but not less than liquidated damages of $1,000 or $100 per day for each day of violation, whichever is greater;

(b) punitive damages; and

(c) reasonable attorney's fees and other investigation and litigation costs reasonably incurred.

AUTHORIZATION DURING TIME OF WAR

50 USC 1811. SEC. 111. Notwithstanding any other law, the President, through the Attorney General, may authorize electronic surveillance without a court order under this title to acquire foreign intelligence information for a period not to exceed fifteen calendar days following a declaration of war by the Congress.

TITLE II—CONFORMING AMENDMENTS

AMENDMENTS TO CHAPTER 119 OF TITLE 18, UNITED STATES CODE

SEC. 201. Chapter 119 of title 18, United States Code, is amended as follows:

18 USC 2511. (a) Section 2511(2)(a)(ii) is amended to read as follows:

"(ii) Notwithstanding any other law, communication common carriers, their officers, employees, and agents, landlords, custodians, or other persons, are authorized to provide information, facilities, or technical assistance to persons authorized by law to intercept wire or

oral communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, if the common carrier, its officers, employees, or agents, landlord, custodian, or other specified person, has been provided with—

"(A) a court order directing such assistance signed by the authorizing judge, or

"(B) a certification in writing by a person specified in section 2518(7) of this title or the Attorney General of the United States that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required, 18 USC 2518.

setting forth the period of time during which the provision of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required. No communication common carrier, officer, employee, or agent thereof, or landlord, custodian, or other specified person shall disclose the existence of any interception or surveillance or the device used to accomplish the interception or surveillance with respect to which the person has been furnished an order or certification under this subparagraph, except as may otherwise be required by legal process and then only after prior notification to the Attorney General or to the principal prosecuting attorney of a State or any political subdivision of a State, as may be appropriate. Any violation of this subparagraph by a communication common carrier or an officer, employee, or agent thereof, shall render the carrier liable for the civil damages provided for in section 2520. No cause of action shall lie in any court against any communication common carrier, its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of an order or certification under this subparagraph.". Disclosure of information, prohibition. 18 USC 2520.

(b) Section 2511(2) is amended by adding at the end thereof the following new provisions: 18 USC 2511.

"(e) Notwithstanding any other provision of this title or section 605 or 606 of the Communications Act of 1934, it shall not be unlawful for an officer, employee, or agent of the United States in the normal course of his official duty to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act. 47 USC 605, 606.

"(f) Nothing contained in this chapter, or section 605 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications by a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, and procedures in this chapter and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire and oral communications may be conducted.".

(c) Section 2511(3) is repealed. Repeal.

(d) Section 2518(1) is amended by inserting "under this chapter" after "communication". 18 USC 2511. 18 USC 2518.

(e) Section 2518(4) is amended by inserting "under this chapter" after both appearances of "wire or oral communication".

(f) Section 2518(9) is amended by striking out "intercepted" and inserting "intercepted pursuant to this chapter" after "communication".

18 USC 2518.

(g) Section 2518(10) is amended by striking out "intercepted" and inserting "intercepted pursuant to this chapter" after the first appearance of "communication".

18 USC 2519.

(h) Section 2519(3) is amended by inserting "pursuant to this chapter" after "wire or oral communications" and after "granted or denied".

TITLE III—EFFECTIVE DATE

EFFECTIVE DATE

50 USC 1801 note.

SEC. 301. The provisions of this Act and the amendments made hereby shall become effective upon the date of enactment of this Act, except that any electronic surveillance approved by the Attorney General to gather foreign intelligence information shall not be deemed unlawful for failure to follow the procedures of this Act, if that surveillance is terminated or an order approving that surveillance is obtained under title I of this Act within ninety days following the designation of the first judge pursuant to section 103 of this Act.

Approved October 25, 1978.

Twenty Years of Espionage

Espionage Prosecutions	Arrest Date	Rank	Job	Clearance	Access	Services Involved	Initiation	Motivation	Foreign Travel	Disposition
Michael A. Peri	1989	E–4	Communications Specialist.	Top Secret Codeword.	Military plans Operations	East Germany	Volunteered	Disgruntlement	Yes	30 years Dishonorable discharge
James W. Hall III	1988	WO1	Communications analyst U.S. Army.	Top Secret Codeword.	Communications Intelligence	Soviet East Germany.	Volunteered	Money	Yes	40 years, $50,000 fine forfeiture of pay and allowances, dishonorable discharge
Clayton J. Lonetree	1987	E–5	Marine Security Guard	Top Secret	Moscow and Vienna Embassies	Soviet	Recruited	Romance, friendship.	Posted abroad.	30 years hard labor
Ronald W. Pelton	1985	GS–13	NSA	Top Secret Codeword.	Sensitive NSA Programs	Soviet	Volunteered	Money	Yes	Three life sentences plus 10 years
Jonathan J. Pollard	1985	GS–12	Counter terrorism analyst, watch officer U.S. Navy.	Top Secret Codeword.	Military and Intelligence Reports, Studies.	Israel	Volunteered	Ideology, Money	Yes	Life Sentence
Sharon M. Scranage	1985	GS–8	Operational Support Assistant, CIA.	Top Secret Codeword.	Information on Intelligence Operations.	Ghanaian	Recruited	Romance, Pressure.	Posted Abroad.	Five Years Later reduced to two years
John A. Walker, Jr	1985	WO3	Radioman, Crypto Custodian, U.S. Navy.	Top Secret Cryptographic.	Cryptographic material, message traffic after 1976 from Whitworth, son, brother.	Soviet	Volunteered	Money, adventure, egoism.	Yes	Two life sentences plus 10 years
Jerry A. Whitworth	1985	E–8	U.S. Navy	Top Secret Cryptographic.	Sensitive Military Communications.	Soviet	Recruited by John Walker.	Money	Posted abroad.	Five life sentences plus 197 years and $410,000 fine
Larry W. Chin	1985	GD–13	Translater and Intelligence Officer FBIS.	Top Secret	Intelligence Reports	Chinese	Probably Volunteered.	Ideology, Money, Egoism.	Yes	Suicide before sentencing
Karel F. Koecher	1984	GS–10 equiv.	CIA Contract Employee	Secret	Intelligence Sources and Methods.	Czech	Recruited	Adventure, Money, Egoism.	Yes	Exchanged in 1986

Richard W. Miller	1984	GS–13	Special Agent FBI	Top Secret	FBI Investigations and Operations.	Soviet	Allegedly Recruited.	Money, Revenge, Romance.	No	Conviction overturned, released, awaiting retrial
James D. Harper	1983	Civilian	Free-lance engineer	None	Secret Defense contractor material (through wife's job).	Polish	Recruited	Money	Yes	Life Sentence
Francisco de Asis Mira.	1983	E–4	Computer technician U.S. Air Force.	Secret	Technical documents on air defense and radar.	Soviet	Volunteered	Money	Posted abroad.	10 year sentence, reduced to seven, dishonorable discharge
William Holden Bell	1981	Civilian	Project Manager Hughes Aircraft Corp.	Secret (awaiting codeword).	Advanced radar designs and weapons plans.	Polish	Recruited	Money	Yes	Eight years
Christopher K. Cooke	1981	2d LT USAF	Titan missile launch officer U.S. Air Force.	Top Secret	Nuclear strike capabilities	Soviet	Volunteered	Egoism	No	Charged with unauthorized transfer of classified information, failure to report Soviet contacts
David H. Barnett	1980	Civilian (former GS–13).	Former CIA Officer	Top Secret	Prior access to CIA operations	Soviet	Volunteered	Money	Yes	18 years
William P. Kamples	1978	GS–7	Watch Officer CIA	Top Secret Codeword.	Message traffic, technical manuals, finished intelligence.	Soviet	Volunteered	Revenge, Adventure.	Yes	40 years
Christopher J. Boyce	1977	Civilian	Security/document control, TRW Corp.	Top Secret Codeword.	Sensitive documents and Intelligence.	Soviet	Volunteered	Money, Adventure	Yes	40 years
Raymond G. de Champlain.	1971	E–7	Senior NCO U.S. Air Force Base, Thailand.	Top Secret	Air force readiness, equipment, capabilities.	Soviet	Volunteered	Money	Posted abroad.	15 years, later reduced to seven

Chairman BOREN. Also without objection I'll place into the hearing record an unclassified study prepared by the Department of Defense personnel Security Research and Education Center, entitled "American Espionage, 1945–89", which is a statistical study reflecting trends in the espionage cases since World War II. I might say it confirms in large measure the work of the Jacobs Panel.

[The document referred to follows:]

OFFICE OF THE UNDER SECRETARY OF DEFENSE,
WASHINGTON DC. 20301-2000,
May 22, 1990.

MR. L. BRITT SNIDER,
General Counsel,
Select Committee on Intelligence,
United States Senate,
Washington, D.C. 20510–6475.

DEAR MR. SNIDER: In response to your verbal request on 4 May 1990, attached is information collected by the Department of Defense Personnel Security Research and Education Center reflecting trends in espionage. This information was derived from reviews of 131 U.S. espionage cases that PERSEREC has analyzed over the last two years under our direction.

The purpose of the research is to support development of more effective personnel security policies. While not all data elements have been collected for each of the 131 cases, we believe a sufficient number are known to permit preliminary analysis.

We are pleased to make this information available to the Senate Select Committee on Intelligence to support its important initiatives in this area. We are available to provide further assistance.

Sincerely,

MAYNARD C. ANDERSON,
Assistant Deputy Under Secretary of Defense,
(Counterintelligence and Security).

AMERICAN ESPIONAGE, 1945-1989

SUZANNE WOOD

Defense Personnel Security Research and Education Center

KATHERINE L. HERBIG

BDM Corporation

PETER A. W. LEWIS

Naval Postgraduate School

DEFENSE PERSONNEL SECURITY RESEARCH AND EDUCATION CENTER

99 PACIFIC STREET, BUILDING 455E

MONTEREY, CA 9394-2481.

Preface

The Defense Personnel Security Research and Education Center (PERSEREC) provides policy-makers with research data on personnel security. Much of the research effort undertaken since the founding of the Center in 1986 has focused on the process of granting clearances and on continuous assessment of cleared personnel. Yet the reason for creating PERSEREC lay in the Stilwell Commission's 1985 report, *Keeping the Nation's Secrets.* In the preface to that report President Reagan stated that, "We should recognize that spying is a fact of life. . . (but) we can counter this hostile threat and still remain true to our values."

To learn more about the nature of espionage, PERSEREC began in 1987 to assemble and file unclassified, open-source materials on American spies. We were not building a profile of the traitor, as we might have hoped, but gathering large amounts of data with no organizing framework. It soon became clear that an automated database would allow for more structured analysis.

The database portrayed in the present report is the result of that effort. Our espionage database is still missing many data in its cells. We are moving to eliminate those gaps through interagency review of files. In places we have also made subjective decisions concerning categorization of information. Where possible, we have noted our methods and the decision rules used to reach our conclusions.

It should be noted that the database includes only caught spies. It is not intended that this effort reflect the nature of all espionage, only those acts where an individual has been apprehended.

This report is the first in a series of documents that will describe work in progress. We will add additional cases and work to fill all gaps in information.

The value of such a database lies in its ability to aggregate and crosstabulate information. As an unclassified work the database has value in a comprehensive security awareness program. It will be useful to a host of governmental and other individuals interested in understanding the phenomenon of espionage and working toward its prevention.

ROGER P. DENK,
Director.

AMERICAN ESPIONAGE, 1945–1989

SUMMARY

SUZANNE WOOD

KATHERINE HERBIG

PETER LEWIS

Background

PERSEREC's initial research agenda, developed in May 1986, contained a priority one task to validate existing criteria for personnel security clearance determinations. Listed as a subtask was the requirement to review adjudication decisions of caught spies to determine if such information could provide additional cause for a new clearance determination. From that task grew the PERSEREC espionage database project.

Objectives

The database was intended originally to answer the adjudication question raised in the original 1986 task, but expanded to include providing a comprehensive listing of caught spies in the post-war period. A database that covers both biographical and situational variables has value for policy-makers and cleared personnel in general. This report will cover the work of building the database, examine some of the findings from preliminary analysis, and suggest further research.

Approach

All known cases of espionage convictions between 1945 and 1989 for which unclassified sources were available were included in the database. Sources reviewed included newspaper and magazine articles, biographies of spies, general works on espionage, and other government researchers' abstracts of official files. In a few cases, investigative files were consulted. The database presently includes 131 cases with 58 variables per case. Variables are grouped into three categories: Personal Factors, Job Factors at the Time of Espionage, and Espionage Characteristics. In addition, espionage trends over time are examined.

Results

There were 75 spies in the military services and 56 civilians, including contractors. Most were Caucasian, heterosexual and male. They were generally married, fairly well educated, held technical or intelligence positions, and had medium to high levels of clearance. If in the military, the vast majority were enlisted. They

began spying at an early age, but this is partly a reflection of the young age at which Americans enter the military.

Seventy-three percent of the spies were volunteers, the other 23% recruited. The percentage of recruits recruited while in foreign countries is twice as high as those recruited inside the United States.

Most spying for Americans lasts for short periods of time, often only for one incident. Individuals who begin espionage at a younger age are less likely to survive a 2-year spying career as those who come to espionage later. Those caught within 2 years are more than three times as likely to have volunteered as to have been recruited.

Money has been the major reason for espionage, followed by ideology and disgruntlement or revenge. However, despite this, spies have in general received very little in terms of monetary rewards.

Almost half the cases of espionage in the United States occurred in the mid-Atlantic area; another quarter in California. Abroad, West Germany had the most cases. The Soviet Union and other Communist Bloc countries accounted for three quarters of the information received through American espionage.

If we look at volunteering and recruitment over time, we find a major shift toward volunteering in the last 20 years. Similarly, money has increased dramatically as a motivation.

Future Research

Our priority is to fill out the missing data on the 131 spies and to add recent cases to the database. As more complete data are acquired, we will conduct further data analyses.

Introduction

Background

The gathering of information by intelligence agents, especially in times of warfare, is an age-old approach to gain strategic superiority over enemies. Official spies, those individuals working for government intelligence agencies, are trained to serve their country by gathering information. This report concerns those spies [1] who betray their country by selling classified information to foreign powers. The report primarily concerns those Americans who have committed espionage against the United States since 1945. They represent a wide variety of types and backgrounds, from middle-aged ideologues who served the Soviets as spies in the 1940s and 50s to teen-aged servicemen in the 1980s who wandered into foreign embassies seeking ready cash.

Over the four-and-a-half decades since World War II, the United States has had a generous share of spies. The Rosenbergs, Alger Hiss, and Klaus Fuchs are the most famous early perpetrators. In the Cold War period, with the Soviet Union's increasing hunger for strategic information and her eager search for shortcuts to more advanced technology, Americans were recruited or offered to commit espionage against the United States on an ever-increasing basis. Espionage rose to a peak in the early 1960s. The number of cases declined slightly from the mid-60s to the mid-70s, only to rise in the next 10 years to a record number by 1985, the year which has come to be known as the Year of the Spy. In fact, over the course of the 1980s, espionage by Americans grew to alarming proportions. Revelations about the extent and severity of the compromise to national security by John Walker and his accomplices, as well as by others including Edward Lee Howard, Larry Wu-Tahin, Jonathan Pollard and Ronald Pelton, highlighted the need to study espionage in systematic detail.

It is unlikely that espionage against the United States will diminish in the 1990s because of the new Soviet policy of glasnost or growing detente between the two super powers. Some in the United States intelligence community take the view that the relaxing of relations between the two countries may provide an especially rich opportunity for the Soviets to step up their espionage attempts.[2]

---

[1] While such people are technically traitors, throughout this report we use the more common term spy to describe them.

[2] Soviet Spying Increasing. Webster Says, *Los Angeles Times* (March 31,1989), p. 15; The Spy War is Heating up: The Age of Glasnost Means More Espionage, Not Less, *Newsweek* (August 21, 1989),p. 28.

Problem

How do we know which people will spy, and what makes them do it? Where do we direct our limited resources to help prevent espionage? Anticipating espionage—a major task of counterintelligence—is extremely difficult. However, counterintelligence strategy and policy can benefit from the systematic collection of information on the backgrounds and histories of those already convicted of espionage.

The goal of the present project was to compile in a centralized database information on all American spies since 1945, with a view to analyzing these data to identify themes and trends over time.

Review of Other Research

Formal social science research in the area of espionage has been quite limited. There has been no shortage, however, of journalistic, biographical writing about individual spies and their stories.[3] Also, several books have been written which attempted to paint broad-brush pictures of the development of espionage in recent history; in these the authors generally outlined the biographies and experiences of individual spies.[4] While these works provided context and illustration, they did not allow opportunity for synthesizing information across cases.

One commonly found category of research on espionage was the compilation of case histories.[5] Here spies and their circumstances were described as discrete cases. However, little or no attempt was made to put the cases together into an organizing framework or to compare and contrast them with each other. While there is much to framework or to compare and contrast them with each other. While there is much to learn from the individual life of the spy in terms of the effects of family and psychological background and unique life circumstances, this approach does not help researchers and policy-makers in looking for more general trends.

There appear to be only three systematic attempts to effect some level of synthesis. The first, produced by the Defense Intelligence Agency (DIA),[6] looked at some 54 cases involving Department of Defense (DOD)-affiliated persons convicted of espionage, of conspiracy to commit espionage, or of related unauthorized possession or passage of classified information. The cases spanned the period following World War II to December 1987. From these cases, Jepson developed a case chart of all the spies, listing such variables as duty assignment, age, education, marital status, years of federal service, dates of espionage, foreign intelligence agencies involved, motivation, volunteered or recruited, area of operation, payments, methods of operation, how discovered, materials compromised, and penalty. The report ended with a series of tables giving simple numerical counts for nine key variables. Important findings included the fact that 63% of the spies in the study committed espionage for monetary gain; information was directed to Eastern Bloc intelligence services in 80% of the cases; all the individuals were male; 52% had high school diplomas and 19% had college degrees; 56% were married; 32% began spying before they were 26; and most people were involved in espionage for only 2 years or less before being caught. For our purposes the study was limited because it covered only 54 cases. However, the case studies proved of immense help in providing biographical data on the individuals and also in suggesting clues to which variables should be included in our own database.

---

[3] Examples of such books are John Barron, Breaking the Ring: The Bizarre Case of the Walker Family Spy Ring (Boston: Houghton Mifflin, 1987); Wok Blitteir, Territory of Lies: The Exclusive Story of Jonathan Jay Pollard (New York: Harper & Row, 1989); Howard Slum, I Pledge Allegiance. The True Story of the Walkers: An American Spy Family (New York: Simon & Schuster, 1987); Pete Earley, Family of Spies: Inside the John Walker Spy Ring (New York: Bantam Books, 1 988); Jack Kneece, Family Treason: TheWalker Spy Ring (Toronto: Paperiacks, 1988); Robert Lindsey, The Falcon and the Snowman (New York: Simon & Schuster", 1979); and David Wise, The Spy Who Got Away (New York: Random House, 1988).

[4] A few books in this category are Thomas S. Allen and Norman Polmar, Merchants of Treason (New York: Delacorte Press, 1988) Constantine FittzGibbon, Secret Intelligence in the Twentieth Century (New York: Stein & Day, 1977); Philip Knightly, The Second Oldest Profession: Spies and Spying in the Twentieth Century (New York: Norton, 1986); and Chapman Pinchei", Traitors. (New York: Penguin Books,1988).

[5] Reports on espionage spy cases have been produced by the Department of Defense Security Institute, Recent Espionage Cases: Summaries and Sources (Richmond, VA: DODSl, 1975 onwards); the FBI, FBI Intelligence Division, Espionage Cases: 1983 to 1986 (Washington, DC: FBI, 1987); the Maldon Institute, American Espionage Epidemic (Washington, DC: Maldon Institute, 1986); and the Naval Investigative Service Command, Espionage (Washington, DC: NlSC0M, n.d.).

[6] Lawrence P. Jepson, The Espionage Threat *(Washington, DC: Defense Intelligence Agency. 1988), Report DOS-2400-219-88.*

A second report,[7] produced by the Air Force, was a comparative analysis of espionage involving U.S. Air Force military and civilian personnel. The report abstracted the lives and espionage histories of 23 Air Force personnel who spied or attempted to spy since 1947. The goal was to determine if there were common characteristics which could be used by counterintelligence personnel to identify and neutralize espionage agents. Many variables were illustrated in tabular form. Among these were age when espionage began, years of federal service, foreign influence, career fields, education, money received for espionage. The author concluded that there are no absolute characteristics of all spies which can be used to profile potential spies. Like the DIA report, this study provided excellent information from the cases for inclusion in our database. Its limitation, from our perspective, was the fact that it dealt only with Air Force personnel.

The third work that attempted simple cross-case analysis was Sandia's report for the Department of Energy.[8] The study reviewed 111 cases of espionage against the United States or its allies between 1950 and 1987. Of these, 92 were cases of American citizens prosecuted for espionage. The study examined several variables, paying detailed attention to motivation. Motivational factors were grouped into the following categories: revenge, greed, sense of adventure (ego), ideology, national pride, emotional or romantic involvement, loyalty, entrapment and fear (blackmail, coercion). The study found a 70% rate of volunteering for espionage and the following commonalities: spies appear to be more intelligent than normal, frequently have obsession with espionage matters, are often involved with intelligence professions, and display serious character flaws. In the military, young people often enter the service with problems, cannot satisfy their needs because of low pay, may often be assigned to geographical regions where they might be vulnerable to recruitment, and have access to classified materials.

This analysis of literature demonstrated there was a need for a centralized database on American espionage that contained an expanded number of variables and could be analyzed in a more sophisticated manner using variable crosstabulation. It was felt that the ability to manipulate data would eventually lead to a much richer and more comprehensive picture of espionage.

Methodology

Data Collection

Individuals were included in PERSEREC's database if they (1) committed espionage (gathered or transmitted sensitive or classified information to a foreign power not authorized to receive it); (2) attempted espionage (attempted to engage in the above actions); or (3) engaged in espionage related activities (committed security violations which logically precede or accompany attempts at espionage, such as stealing or secreting classified documents, defecting to a hostile power while in possession of sensitive information, or agreeing to work for a hostile power to procure information to advance its interests).

All the known cases of espionage convictions of American citizens between 1945 [9] and 1989 for which unclassified sources were available were included, as were defections for which it is clear that compromises of information occurred. In addition, cases were included which were handled by administrative sanction or were for other reasons (e.g., suicide) not prosecuted in the courts but for which there was clear evidence of espionage behavior. The total number of cases in the database is 131, and they were drawn from the military, civilian and contractor segments of the community that deal with classified information and technology. Their names are listed in alphabetical order in Appendix A.

The unclassified sources reviewed were newspaper and magazine articles, biographies of spies,[10] histories of espionage [11] and other government researchers' ab-

---

[7] David J. Crawford, Volunteers: The Betrayal of National Defense Secrets by Air Force Traitors (Washington, DC: Government Printing Office. 1988).

[8] Gerald B. Brown, Profile of Espionage Penetration (Albuquerque, NM: Sandia National Laboratories, 1988).

[9] Three earlier spies are included. Two of these were convicted after 1945. These are Harry Gold,courier for Klaus Fuchs, who operated from 1935 to 1945, and David Greenglass, Ethel Rosenberg's brother, who spied from 1944 to 1946. The third early spy, Whittaker Chambers, whose espionage career ran from 1932 to 1938, is included because of his later connection with Alger Hiss. In August 1948 he testified before the U.S. House Un-American Activities Committee that Hiss had been an underground member of the Communist Party. See Chapman Pincher, Traitors, p. 36.

[10] See Note 3, p. 2.

[11] See Note 4, p. 2.

stracts of official files.[12] In a few cases, actual investigative files were consulted. Most of the library research was conducted at the Naval Postgraduate School library in Monterey. Several trips were made from Monterey to Washington, DC, to (1) consult with the CIA; and (2) review espionage files at CIA, the Air Force Office of Special Investigations, and the Naval Investigative Service Command.

Initial work on the database design began June 1987. The information contained in this report was collected through December 1989.

Data Coding and Verification

A coding scheme was developed and used as the cases were reviewed. This included 58 variables for each espionage case (see Appendix 8 for a description of the variables and for decision rules). The variables comprised the following types of information: personal factors, including personal and demographic data on the individual; job factors at the time that the espionage began, including job type, location, and clearance level; characteristics of the espionage itself, such as how it began, how it was accomplished, motives, duration, dates of arrest and sentence, and length of sentence; and trends over time. The variables were selected for their availability in open sources. Additional variables can be added to the database in the future if required.

Not all data lend themselves to being neatly categorized, and several variables required additional qualifying descriptors which help explain the main variable. For example, "How Espionage Began" is explained concisely in one variable and then elaborated on in an accompanying variable, "How Espionage Began, Qualifier." Complex human emotions are hard to classify, and one of the most difficult variables in the database was that of motivation. The problem was addressed by creating multiple variables: stated motive (the reason the spy said he had spied), a second variable inferred motive (what the investigator, after reading the file or account, inferred was the real motive), and a third motive, a derived motive (the stated motive recoded into six major motive categories) for use in conducting crosstabulations.

Description of the Database Software

The data analysis was entered into a full-screen, scrollable spreadsheet-like editor called UEDIT. This was written at the Naval Postgraduate School by Uwe Steinfeld under the direction of Peter A. W. Lewis. This editor is written in the IBM APL2 language and implemented on a microcomputer in the IBM APL232 program product for 80386-based microcomputers. Beside data entry and manipulation, the editor has facilities for simple statistical functions such as frequency tabulation, crosstabulation and multiple regression.

Limitations of the Data

Several points must be kept in mind when reviewing the analyses.

We do not have data on psychological traits of the American spies, we cannot document strengths or weaknesses of character, and we cannot evaluate the quality of the values an individual held. While in-depth studies of single spies may have their own methodological limitations, they can often explain espionage in these qualitative terms. These dimensions are for the most part unavailable without extensive interviews and testing of the apprehended spy, and they are qualities which would resist abstraction in an automated database even if they were available.

Decision rules were developed and followed for the majority of the variables. However, the fragmented nature of some of the data, drawn as they were from often unsystematic sources, has proved to be a problem in coding. Further, human motives, because of their complexity, are difficult to code. Therefore, subjective decisions had to be made occasionally during the coding process. Since all decisions were made by the same investigator, it is presumed the decisions were consistent. In the future, it would be preferable to acquire a second opinion on coding difficult variables.

The major difficulty in working from open and secondary sources was the problem of missing data. Information on a spy culled from an article in the *New York Times* does not always cover all the variables included in the database. To date, court transcripts, a rich source of nonclassified information, have not been reviewed. We are also aware that there are still more espionage files to be read in military archives.

A second problem with data from open sources is the question of accuracy. We have high confidence in the accuracy of the data gathered by PERSEREC research

[12] Department of Defense Security Institute. Recent Espionage Cases: Summaries and Sources: Crawford, Volunteers; and Jepson, The Espionage Threat.

staff from investigative files. We are somewhat cautious, however, about the other commonly used sources: newspaper and magazine articles, biographies, and other people's abstracts of files. While source of information is coded each case, we have not as yet developed a formal system of weighting our confidence in the data.

The database is presently being reviewed by the military services for accuracy and, if possible, to have missing data filled in. In addition, the FBI is providing us with a review of its case data. Meanwhile, a decision was made to report the data as they stood as of December 1989 so that we could share with the counterintelligence community initial findings and general trends.

ANALYSES

We have grouped the variables into three categories: Personal Factors, Job Factors at the Time of Espionage, and Espionage Characteristics. The analyses on these tables represent only a description of the data, along with a small number of simple misstabulations. As more data are filled in, we intend to conduct research in which more complex interrelationships will be analyzed.

Personal Factors

Age

Espionage appears to be a young person's crime. We know the age at which individuals began their espionage for 94 of the 131 cases. Figure 1 shows that 17% of the individuals began spying between 18 and 23 years old; 28% between 23 and 28; and 17% between 28 and 33. Thus, 62% spied before the age of 33. Since young men predominate in the military services in the enlisted ranks, this result reflects the age distribution of the population of military personnel.[13] It also reflects the fact that young first-term enlisted personnel are given access to sensitive information. The age distribution among all civilians with security clearances is not available at this time.

The typical youthfulness of American spies in the military is supported by looking at the age that espionage began for the military cases in contrast to the civilian spy bases.[14] We know the age that espionage began for 45 of the enlisted personnel. Figure 2 shows that incidents of spying are distributed across the entire 20-year careers of most enlistees. Enlisted spies generally start early in their military careers, in many cases during the first enlistment. In fact there are five cases at age 21 near the end of the first enlistment. Espionage tapers off after age 35.

For civilians, we know the age of 35 people when they began spying. Spying is distributed across the 30-year working career. As with enlisted personnel, espionage starts early, in this case at about age 23, and then tapers off about age 50.

---

[13] "Active Duty Master List," September, 1989 and September, 1985. The rates of enlisted persons ages or less in the military in 1989 was 54.3, in 1985 was 59.2; officers age 25 or less was 15.3 in 1989, and was 11.7 in 1985.

[14] Because officers are so few in number, they are not included in Figure 1. The ages of the 7 officers are 21, 24, 25, 36(2), 41 and 44. The three warrant officers were 24, 26, and 30 when they began spying.

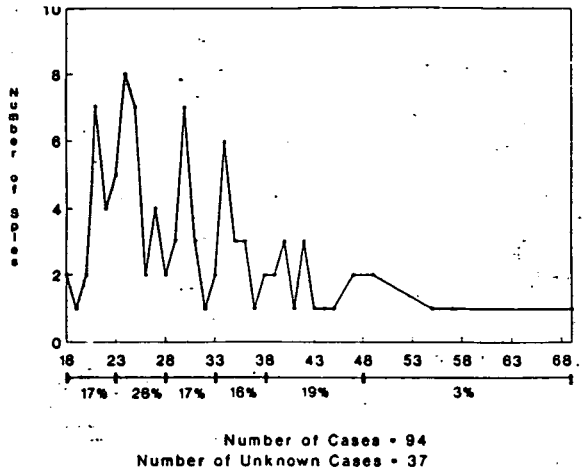

Figure 1. Age When Espionage Began

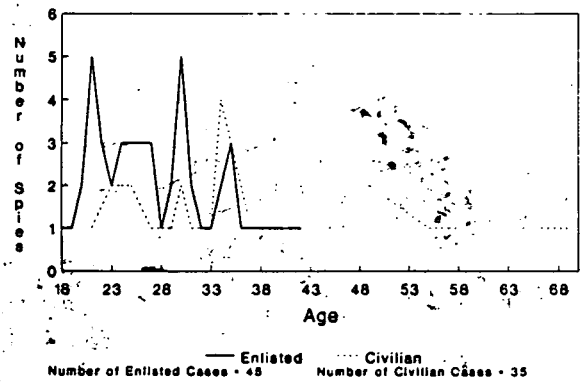

Figure 2. Age Espionage Began: Enlisted vs. Civilian Personnel

Gender

Over 95% of the cases have been men. Even given the fact that many more men than women have had access to classified information by holding security clearances, the numbers of women still seem especially small. The gender of holders of security clearances have not yet been obtained, however, so it is difficult to determine the extent to which women are underrepresented.

Race

The overwhelming majority of espionage by Americans has been committed by Caucasians. We know the race of 80 of the spies. Seventy-two were Caucasian, six Black, one Asian, and one American Indian. Thus 10% of the cases of espionage for which the race of the perpetrator is known involved racial minorities. Combined rates of Black, Asian, and American Indian minorities in the general population as well as rates for these minorities' participation in the armed services, suggest that

this is two to three times lower than an expected espionage rate for these minorities.[15] By the same token, Caucasians are overrepresented.

Education

Data on the level of education is known for 76 of the spies. Eleven percent had less than high school,[16] 38% were high school graduates. 15% were high school graduates who also had taken some college courses, 26% were college graduates, 3% were college graduates who had done some postgraduate work, and 7% had master's degrees or a doctorate. As Figure 3 illustrates, the level of education is relatively high, suggesting that espionage is committed by people who are capable of planning and organizing risky and sometimes complicated activities.[17]

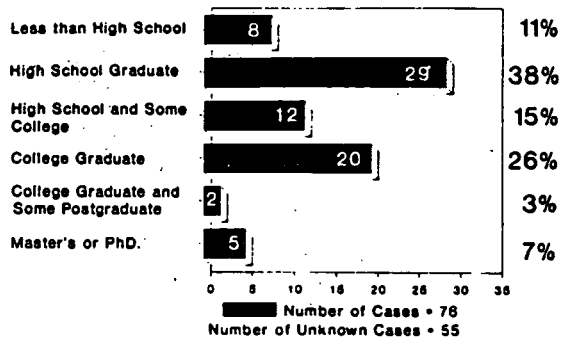

Figure 3. Levels of Education

Marital Status

In addition to being well educated and Caucasian, the typical American who has committed espionage against the United States was also married. Table 1 shows that of the 90 people whose marital status we know, 58% were married and 29% were single. (Given the higher than average proportion of young men, who are more likely to be single, the rates of marriage among spies reflect the rates found in the

---

[15] "Active Duty Military Master List," June 1971, September 1980, September 1985, and September1989, Defense Manpower Center, Department of Defense, Monterey, CA. Between 1971 and 1989 the percentage of racial minorities in the military services varied from 13% to almost 29% for enlisted personnel, and from 2.7% to 9.7% for officers. For the general population, see U.S. Department of Commerce, Bureau of the Census, Statistical Abstract of the U.S. 1989, 109th ed., Washington. DC: Government Printing Office 1989), p. 41.

[16] However, one of those, John A. Walker, Jr., proved to be among the most successful American spies ever. Despite the disadvantages of only an 11th grade education, he maintained himself as a spy for the Soviets for 17 years. See Pete Earley, *Family of Spies.*

[17] The relatively high educational attainments of American spies reflect the improving educational standards in the American military services over the past 20 years as well as the higher levels of education in the military for both officers and enlisted personnel compared with the general population. For all males in 1984, the Bureau of the Census lists highest degree attained as follows: less than High School graduate: 25.3%; High School graduate: 32.7%; High School diploma and some college: 4.8%; College Graduate: 11.9%; College Graduate and some postgraduate: 6.3. See U.S. Department of Commerce. Bureau of the Census, *Statistical Abstract* of U.S. 1989. 109th ed., Washington. DC: Government Printing Office 1989), p. 133. For the military in 1985 among enlisted ranks, only 3.5% held less than a High School diploma; 79% had High School diplomas; 15% had some college; 2.2% were college graduates, and .1% had postgraduate training as well. Among officers in 1985, 3.4% had High School diplomas; 3.7% had some college; 55.3% were college graduates; 32.3% had postgraduate training; and 1.1% held Ph.D. degrees. Comparison with levels of education in 1971 is startling mainly for the enlisted ranks with less than a High School diploma, which stood at 20.4%; High School diplomas: 63.9%; some college: 10.6%; college graduate: 3.4%; and postgraduate: .1%. For officers in 1971: 8.8 were high school graduates; 14.6 had some college; 54.3 were college graduates; and 17.9% had postgraduate work, see 'Active Duty Military Master List,' June 1971 and September 1985, Defense Manpower Data Center, Department of Defense, Monterey, CA.

military as well as in the general population).[18] Thirteen percent were either divorced, separated or widowed.

Table 1

Marital Status

Married	52	(58%)
Single	26	(29%)
Divorced/Separated/Widowed	12	(13%)

Number of Cases = 90
Number of Unknown Cases = 41

Sexual Preference

The sexual preferences of these individuals mirror the pattern of the population in general. We know, or can reasonably infer, sexual preference for 90. Ninety-one percent are heterosexual and 9% are homosexual. Researchers on rates of sexual orientation have found that roughly 90% of men in any human group will be "more or less exclusively heterosexual."[19]

Substance Abuse

The profile of the number of substance abusers among American espionage cases is necessarily tentative because information on substance abuse has not been routinely reported for such cases. In 22 of the 131 cases, substance abuse is known to have been a factor; alcohol abuse accounts for 9 cases, drug abuse for 10. Three additional individuals were abusing both. Thus in 17% of the espionage cases substance abuse is known to have played a part. In 3 cases involvement with illegal drugs was the reason for the espionage.[20] Several of the alcohol abusers committed espionage because their alcohol problem had earned them demotions or lost them opportunities to advance; their resentment about these problems in turn contributed to their becoming involved in espionage.[21]

Foreign Connections

Security doctrine holds that persons with foreign connections are greater risks for espionage because their loyalties may be divided and they may have more opportunities to contact foreign buyers of information. Therefore, the backgrounds of these

---

[18] For the general population of all men in 1987,25.3% were single and 65.5% were married. For the military population, where rates of marriage have been increasing for both officers and enlisted persons over the last two decades, enlisted personnel in 1989 had rates of 43.7% single and 53.2% married; officers had rates of 24.2% single and 72.6% married. U.S. Department of Commerce, *Statistical Abstract*, p. 41; 'Active Duty Master List,' September, 1989, Defense Manpower Data Center, Monterey. CA.

[19] Kinsey, W. Pomeroy, & C. Martin, *Sexual Behavior in the Human Male.* (Philadelphia: W.B. Saunders & Co., 1948), p. 538.

[20] Andrew Daulton Lee was a drug dealer who got involved with espionage to earn capital for further drug deals; Jeffrey Pickering tried espionage to raise money to support his heroin habit; and Francis Pizzo agreed to help sell cryptographic cards to raise money to pay his debts to drug dealers. See Lindsey, *The Falcon and the Snowman* for Lee; Federal Bureau of Investigation files, for Pickering and Plo.

[21] Dennis O'Brien, 'Army Panel Hears Testimony Spy Charges.' *The Baltimore Sun*, June 2, 1983 for Daniel Walter Richardson; 'Lesser Charge Accepted in Military Secrets Case.' *New York Times*, May 29, 1987, for Allen John Davies.

persons are given stricter scrutiny by clearance investigators.[22] One hundred and sixteen (89%) of the spies were native-born and 15 (11%) naturalized. Twenty-eight individuals were known to have had foreign relatives such as wives or parents. Figure 4 summarizes the distribution of foreign relatives for these individuals.

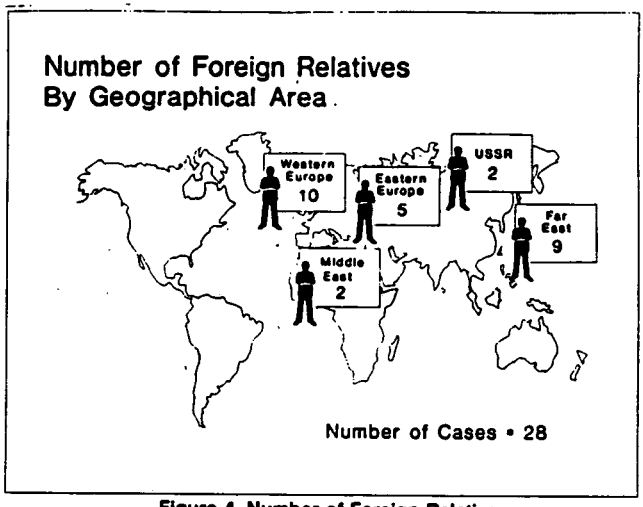

Figure 4. Number of Foreign Relatives by Geographical Area

As far as we can tell from reading open sources, there is only one case in which a foreign relative cooperated as an accomplice to espionage.[23] There are a few other cases in which a foreign relative or loved one may have been the precipitating cause of espionage.[24] In some situations, being born abroad, having lived abroad, or having married a foreigner, may have provided an emotional or political environment that might contribute to conflicts of loyalty and lead to later espionage.[25] In most cases, however, having foreign relatives and connections was not a contributing factor. Of course, this may have been the result of effective screening and adjudication of background investigations.

JOB FACTORS AT THE TIME OF ESPIONAGE

Responsibility for Information by Military Services and Civilian Intelligence Agencies

Figure 5 illustrates which military services or civilian intelligence agencies were responsible for the information being compromised. Some individuals committed es-

---

[22] U.S. Department of Defense, 'Personnel Security Program.' DOD 5200.2-R, 'Adjudicative Guidelines' (Washington. DC: Government Printing Office, January 1987) and DCID 1/14 Minimum Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information. November 1987.

[23] This is the case of Specialist Fifth Class Leslie J. Payne, stationed with the U.S. Army in West Germany when he attempted to pass classified documents to a foreign government, probably East Germany; his East German-born wife acted as an intermediary. See Jepson, *The Espionage Threat*, p. 28.

[24] For example, Stephen Anthony Baba, a Naval officer, committed espionage in 1981 in order to get money to send to his fiancee in the Philippines. See Jepson, *The Espionage Threat* pp. 11, 12 and NIS investigative file. In 1976–1978 Ronald Louis Humphrey, a civilian in the U.S. Informational Service, provided information to the Vietnamese Government via a go-between in order to gain favor to get his Vietnamese mistress out of Vietnam. See Jepson, *The Espionage Threat*, p. 22.

[25] Mrs. Ahadi (pseudonym) was born of Syrian parents, raised a strict Moslem, married an Egyptian (naturalized), husband, and was strongly anti-Jewish. She finished up committing espionage on behalf of the United Arab Republic. Herman (pseudonym), a sergeant in the U.S. Air Force, came from a Jewish Romanian family, had survived Auschwitz as a child, after losing all his close family, and was liberated by the Soviets in 1945. He came to the U.S. in 1949. The Rosenbergs, coming from Jewish immigrant parents, were committed Communists.

pionage after they had left the organization from which the information they sold (or attempted to sell) was associated. For the purposes of Figure 5, these individuals are included under their former organizations. If we know they were formerly in the military, they are coded as military in their former service.[26] Similarly, civilians who spied after leaving intelligence agencies are included as being part of the agency whose information was compromised.[27]

Figure 5 shows that 9 civilians were working as part of the military when they committed espionage (2 in the Army, 3 in the Air Force, and 4 in the Navy), and 7 worked for private contractors. The CIA had responsibility for the information in 8 espionage cases, NSA for 5, and the DIA and FBI one each. The individuals in the miscellaneous category include 3 spies in the State Department, one in Justice, a mathematician, a journalist, a self-employed foreign policy analyst, a drug dealer, a chemist, and several engineers (electronic, electrical and computer).

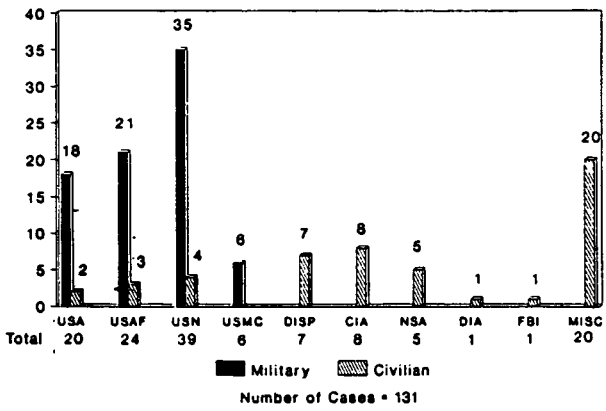

Figure 5. Responsibility for Information by Military Service and Civilian Intelligence Agencies

Rank

Figure 6 illustrates the fact that 75 of the espionage cases involved personnel in military service. Fifty-one of these were enlisted men, 7 were officers, 3 were warrant officers, and 14 were unknown to us. Thus, roughly one fifth of the uniformed espionage cases involved officers currently serving in the military and four fifths were enlisted people. This is slightly higher than the percentages of officers to enlisted men across the military, which has varied from roughly 12 to 16 % over the past three decades.[28]

[26] The cases we know about are Robert C. Wolf (former Air Force), Craig D. Kunkle and Jay Clyde Wolff (former Navy), and Clyde Lee Conrad (former Army).

[27] For example, Ronald William Pelton, a former NSA employee at the time of espionage, is coded under NSA; David H. Barnett, Edward Lee Howard, Edwin G. Moore II and Nick Clark Wallen, who committed espionage after they left the CIA, are coded under CIA.

[28] Selected Manpower Statistics. Fiscal Year 1950, tables 2-12 and 2-13; and Military Manpower Statistics. Quarter Ending June 30, 1989, p. 6. Department of Defense, Directorate for Information, Operations, and Reports, Washington, DC.

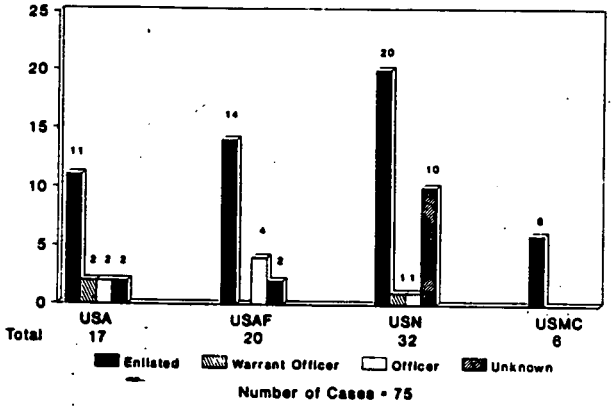

Figure 6. Ranks of Military Personnel Conducting Espionage

Occupation

Occupation was a particularly difficult variable to code. Often, open sources were not altogether clear about exactly what kind of job a spy might have been doing at the time he was committing espionage. For example, words such as "clerk," "intelligence," etc., may have been the only clue to a person's job. We have done our best to classify the occupations, but realize that the categories are not always precise and mutually exclusive.

Information on the types of work Americans spies were doing at the time of their espionage shows a wide variety of occupations. Occupational type is known for 106 individuals. Figure 7 summarizes the various occupational categories. The largest occupational groups are technical specialties such as electronics, sonar, nuclear, or radar (19%) and the intelligence specialties (16%). Intelligence officers and analysts by definition would have access to sensitive information, while the large number of technicians reflects the increasingly specialized technologies of military combat and the interest among foreign powers in acquiring American technologies. The remaining categories include clerical, communications, and cryptographic specialties, all of which would expose workers to sensitive information of great interest to foreign powers. The miscellaneous category contains such jobs as watch officer, student, driver, automobile painter, finance officer, translator and being self-employed.

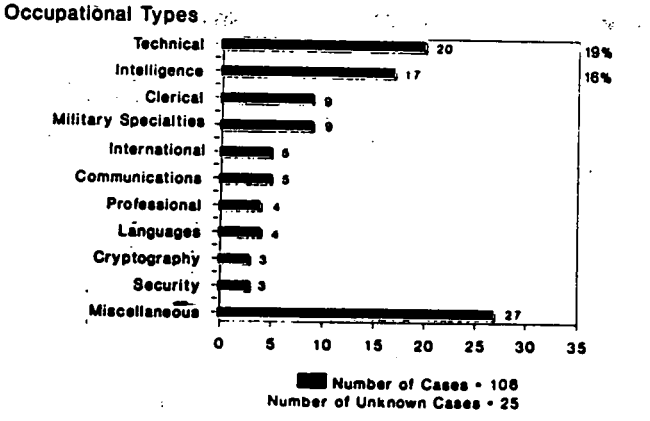

Figure 7. Occupations

Level of Clearance

At present, we know the level of security clearance for only 69 individuals. As might be expected, given the greater interest in highly classified information on the part of foreign buyers, twice as many people held TOP SECRET clearances as held lower level ones: 58% held TOP SECRET clearances, 28% held secret clearances, and one individual was only cleared for confidential information. Thirteen percent of the people had no security clearance at all; some of these used friends or relatives as sources, others simply stole information to which they had no legal access.[29]

We are presently attempting to acquire more information on clearance level, but it must be pointed out here that even if we know the level of clearance for all the spies it does not necessarily mean that we know the circumstances surrounding their actual access.

Length of Time in Federal/Military Service [30]

In only 56 cases do we know the length of time the person had been working for the federal government (including military service) at the beginning of the espionage incident. In the remaining 75 cases, the length of time in federal service is either unknown or the individual had not worked for the government.

Figure 8 summarizes the numbers of cases in the various categories. The largest group had been federal employees for the shortest time: 27% of the cases had worked for the federal government less than 2.5 years. The next largest contingent had been federal employees for most of their careers: 21% committed espionage at between 15.5 and 20 years of federal service.

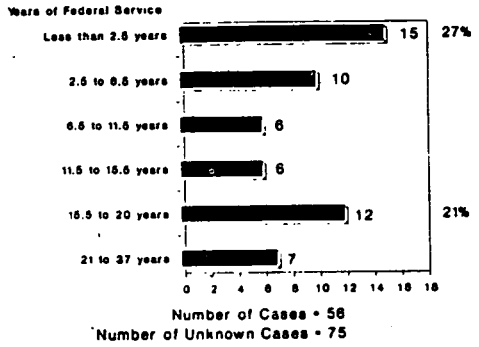

Figure 8. Length of Time in Federal/Military Service

ESPIONAGE CHARACTERISTICS

Volunteer vs. Recruited

Americans have been much more likely to volunteer to commit espionage than to be recruited by others for the job. Information on whether the person volunteered or was recruited is known for 115 cases. Table 2 shows that of these, 73% volunteered and 27% were recruited. It must be noted that in this database recruited includes individuals recruited by fellow Americans as well as by foreign intelligence agencies. Thus, Michael Walker, Arthur Walker and Jerry Whitworth are considered recruits. Table 2 shows the breakdown of those recruited by hostile intelligence services and by friends or family members. For purposes of crosstabulation and subsequent tables in this paper, however, we have grouped all recruits into one category.

---

[29] Michael Walker, son of John Walker, Jr., claimed he held a clearance when questioned by the naval officer who was his supervisor on an aircraft carrier; Walker was never bothered about clearances again and he was able to remove classified documents from burn bags unobserved and stash them out of sight alongside his bunk. See Earley, *Family of Spies*, pp. 287–288.

[30] The number of years an individual had spent in federal service was taken from Jepson, *The Espionage Threat*, pp. 41–47, and includes military and civilian service.

Table 2

Volunteered vs. Recruited

Volunteers		84	(73%)
Recruited:			
by HOIS	20		
by friends or family members	9		
Unknown	2	31	(27%)
		115	

Unknown = 16

Of the espionage cases that occur overseas, one would expect a greater proportion to be the result of recruitment rather than volunteering. This is because there is less restriction and surveillance placed upon representatives of various powers overseas than in the US. Yet in fact there have been more American volunteers than recruits both overseas and on home ground. Table 3 shows that we have information for 105 cases. Of these, 80% of the domestic cases have been volunteers, in contrast with 20% who were recruited. Sixty-One percent of the overseas cases volunteered, as opposed to 39% in which individuals were recruited. Thus volunteering remains a strong and consistent trend among American spies whether they are at home or abroad. It is particularly interesting to note that the percentage of spies who were recruited overseas was twice as high (39% vs. 20%) as those recruited at home.

Table 3

Domestic vs. Overseas Espionage
of Volunteer vs. Recruited Spies

	Domestic	Overseas
Volunteered	59 (80%)	19 (61%)
Recruited	15 (20%)	12 (39%)
TOTAL:	74	31

How Individuals Began Their Espionage

There are 80 cases where we know what the spies did to initiate the espionage act, whether they had been recruited or were volunteering. Figure 9 shows that 14

cases involved contacts made or attempted at the Soviet Embassy or consulates in the United States. In 2 of these cases, information or offers were left on the Embassy grounds; the other 12 cases were "walk-ins" where individuals went into the embassy with offers of information and volunteered their services. In 12 more cases the individuals offered information directly to hostile intelligence, 9 others used the telephone to make such an offer, and 7 more used the mail. Ten individuals gave or sold their information to go-betweens who made the contact with the foreign powers. Seven cases involved professional intelligence agents of hostile powers or declared members of the Communist Party of the United States, and another 7 involved actual or attempted defections to hostile foreign powers. Five individuals stole classified information and kept it but were discovered before they made contact with hostile intelligence agencies. Three attempted to sell information to double agents.

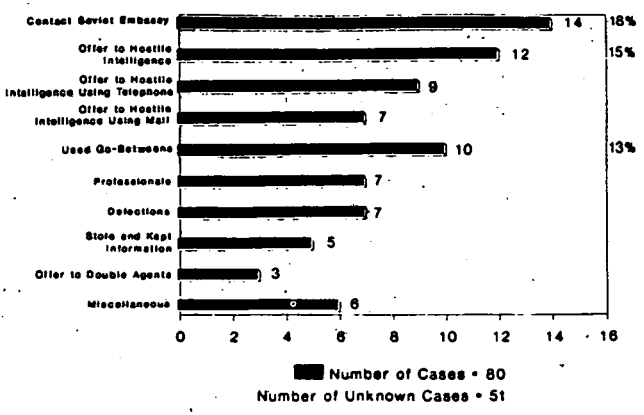

Figure 9. How Individuals Began Their Espionage

Motivation

Of all the issues raised in spy cases, the motivations for committing espionage are among the most eagerly sought and the most difficult to document. As explained earlier, in this database we have two main variables for motivation. The first is the motive the spy himself gave, the stated motive; the second is the motive the investigator, on reading the case story, *inferred* to be the real motive. For example, a person may tell a court that he spied for ideology, but from a reading of the file it is clear that he committed espionage for money. In this example, then, ideology is the stated motive and money the inferred. In the current analyses, we used the stated motive unless the investigator inferred otherwise, in which case we used the *inferred*.[31] Of those 110 cases for which we had either a stated or inferred motive, we moved from stated to inferred in 25% of the cases. In another 8% of the cases, there was no stated motive, but a motive was inferred based on a thorough review of the case. In the remaining cases, there was neither a stated motive nor sufficient information to infer a motive.

Table 4 shows that the most frequent motive for espionage by Americans has been money. Of the 110 cases where we have a motive, 52% featured a mercenary motivation.

---

[31] We are aware that human feelings and sentiments cannot readily be simplified; people commit crimes for myriad reasons having to do with personalities, life experiences, current emotional situations, etc. However, for the purposes of looking for general trends among spies and of allowing for computer manipulation, we sometimes have to force sentiments into constricting categories. In this study, seven spies gave more than one motive, or the investigator inferred more than one motive. For these seven cases, we have taken the liberty coding what we consider to be the overarching motive, recognizing that by doing so we lose richness of data and do some violence to the complexity of these people's feelings.

Table 4

Motivations for Espionage

Money	57	(52%)
Ideology	18	(16%)
Disgruntlement/ Revenge	15	(14%)
Thrills	9	(8%)
Ingratiation	6	(5%)
Coercion	3	(3%)
Miscellaneous	2	(2%)
Total	110	

Ideology proved to be the second strongest motive, accounting for 16% of the cases. Some of these ideological spies crimes date from the early Cold War period when Communist sympathizers ferried American atomic research secrets to the Soviets. Nevertheless, ideology of various sorts has continued to motivate some spies down through the 1980s.[32]

The third most frequent motive for espionage, 14% of the spies, is disgruntlement and revenge. Disgruntlement usually refers to frustration and anger over treatment received at work: lack of promotion, punishment for some infraction, a perceived slight or persecution. Revenge seekers are also annoyed by problems similar to the disgruntled group's, such as dismissal from a job, a dishonorable discharge, or discrimination in job assignment. However, they appear to be attempting to strike a blow at the system or person who angered them.

Three other motivations demonstrate that espionage serves a range of human purposes beyond the typical mercenary or ideological ones. Eight percent of the people spied wholly or in part for the thrills they got from espionage. Such people were motivated by the successful mastery of danger, or they sought the satisfactions

[32] For example, Mrs. Ahadi (pseudonym), a civilian intelligence analyst and chief of her division for HQ 21st Air Force, passed intelligence about Israel to Egyptian contacts in 1967 because of her commitment to Egyptian President Nasser and her hatred for Israel. See Crawford, *Volunteers*, pp. 86–88.

James Frederick Sattler, a foreign policy analyst, was recruited as a spy for East Germany based on his sympathies for that country while studying there in 1967. Sattler continued to send information by mail, courier, or by taking it himself to East Germany, until 1974 when he was exposed. See Allen and Polmar, *Merchants of Treason*, pp. 276–280.

Thomas Joseph Dolce, a weapons evaluator for the Army, mailed classified information to South Africa beginning in 1979 based on his admiration for that country. His espionage continued until 1983, but he was not discovered until 1988. See Paul W. Valentine, 'Maryland Man Admits to Espionage for South Africa,' *The Washington Post*, October 12, 1988 p. A1.

Lastly, Glenn Michael Souther worked as a civilian intelligence analyst for the Navy in Norfolk, VA, until suspicions of his espionage prompted him to defect to the Soviet Union in May 1986. Although the FBI's case against him could not proceed in his absence, the Soviets admitted after his death by suicide in 1989 that Souther had served them faithfully as a committed Communist and an important spy, perhaps for nearly a decade. See Michael Dobbs. 'U.S. Navy Defector Dies in Soviet Union,' *The Washington Post*, June 28, 1989.

of the con man, getting away with something risky and putting something over on compatriots, or they conceived of espionage as a glamorous activity.[33]

Another 5% spied primarily to ingratiate themselves with others, either from friendship or to please another family member.[34]

Despite the prominence of the colorful theme of blackmail in dozens of espionage novels, only 3% of the individuals claimed they spied because they were being blackmailed.[35]

Duration of Espionage

As Figure 10 illustrates, most cases of American espionage do not persist very long. We know how long the espionage lasted for 110 of the spies. For 55% of the cases, espionage lasted less than one year. In another 20% of the cases the espionage activity continued for between 1 and 2 years. In only 7% of the cases did the espionage last for more than 10 years.[36]

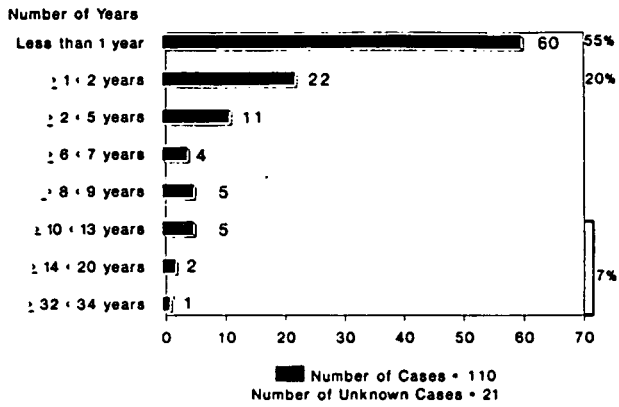

Figure 10. Duration of Espionage

Payment for Espionage

If most American spies do not stay in business very long, it is equally true that they are not very well rewarded for the risks they take. We know the amounts of payment received in 80 of the cases. Figure 11 illustrates that of the 80, 48% received nothing for their crimes, either because they were discovered before they

---

[33] John Walker appears to be the archetype of the con man type, although in his constellation of motives a desire for money vied with the need to manipulate others. See Earley, *Family of Spies*, pp. 369–371.

[34] For example, Michael Walker became a spy in an adolescent quest to please his father; Clayton Lonetree spied to protect and sustain his relationship with a Soviet woman; William Bell eased into espionage gradually under the expert manipulation of a Polish intelligence agent who befriended him at a time when his family life had left Bell vulnerable. It is also true to say that he needed money. See Earley *Family of Spies*, p. 205 for Michael Walker; Pete Earley, 'Spy Fiasco.' *The Washington Post Magazine*, February 7, 1988 for Clayton Lonetree; and U.S. Senate, 'Meeting the Espionage Challenge: A Review of United States Counterintelligence and Security Programs,' Report of the Select Committee on Intelligence. Report 99–522 (99th Congress, 2nd Session, October 3, 1986). Appendix C, p. 118 for William Bell.

[35] Herbert Boeckenhaupt's claim in court that he was blackmailed into espionage with threats against his relatives in Germany was less than convincing since he had walked into a Soviet embassy in October 1982 and volunteered to sell them information. See Crawford, *Volunteers*, pp. 88–91

Three blackmail cases involved Soviet or polish female intelligence agents seducing American men, collecting evidence of their sexual liaisons, and then confronting them with a choice of cooperation in espionage or exposure. This unhappy device trapped Roy Rhodes in 1952, and Glenn Rohrer and Irving Scarbeck in 1950. See Jepson, *The Espionage Threat*, pp. 30–31, for Rhodes; Robert Morris, private clippings files on espionage, for Rohrer and Scarbeck.

[36] These are Larry Wu-Tai Chin, Clyde Lee Conrad, Sergeant Herman (pseudonym), Karl F. Koecher, Jonathan J. Pollard, John Anthony Walker Jr., and Jerry Alfred Whitworth.

could be paid or because they acted from other than mercenary motives. Of the remaining cases, 29% received less than $20,000; indeed, 12% of these individuals received paltry sums between $50 and $999. Only 10% of the spies made $100,000 or more from espionage.[37]

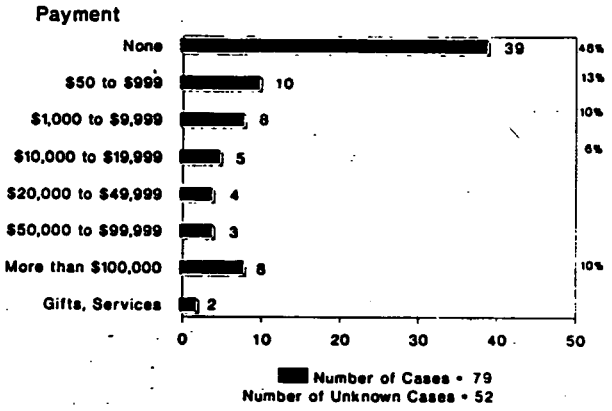

Figure 11. Amounts of Payment for Espionage

The annual income from espionage for the 38 spies for whom we have estimates on money received for espionage is shown in Appendix C.

Figure 12 shows that for the 38 individuals for whom we have information 26% received less that $1,000 per year, 37% received between $1,000 and $9,999 per year, and another 37% received over $1,000 per year.

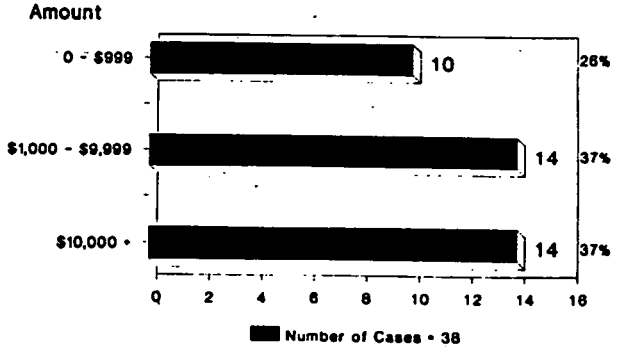

Figure 12. Estimated Annual Income from Espionage

Length of Sentences

Once espionage is uncovered and the case has gone to trial, the severity of the punishment metered out in fines or prison sentences is one indication of how seriously society rates espionage as a crime. The length of sentences for espionage has

[37] These are William Holden Bell, Larry Wu-Tai Chin, James W. Hall III, James D. Harper. Jr., Joseph George Helmich, Jr., Edward Lee Howard, John Anthony Walker, Jr., and Jerry Alfred Whitworth.

differed considerably between military and civilian courts in the United States. Civilians on the whole have received longer prison terms for espionage than military personnel.

Among the 75 military cases, we know the length of sentence for 70. Figure 13, which compares percentages of lengths of sentence for individuals in the military and civilian world, shows that 24% of the military cases of espionage received sentences of less than 5 years, 23% received 5 to 14 years, and another 23% 15 to 39 years. Only 10% received sentences of 40 or more years. Twenty percent of the individuals received no prison time at all, often because they were administratively charged from the military. One committed suicide; another defected.

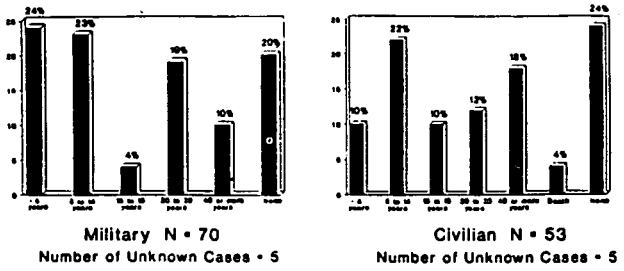

Figure 13. Comparison of Length of Sentences Imposed on Military and Civilian Personnel Convicted of Espionage

For civilians, we know the length of sentence for 51 of the 56 cases. Ten percent of the individuals received sentences of less than 5 years, 22% of 5 to 14 years, 10% of 15 to 19 years, 12% of 20 to 39 years, and 18% of 40 or more years. Two received sentences of death. Twenty-four percent of the civilians were not given prison time. In some cases, these civilians had defected, committed suicide, or for various reasons had been granted immunity.

Short-term and Long-term Spies

An interesting exercise is to identify individuals whose careers lasted longer than others. When the duration of espionage is lined up for all cases, 2 years stands out as a reasonable cut-off point. So for analytical purposes a short-term spy is here defined as one who was caught within 2 years or less and a long-term spy as one whose espionage persisted for more than 2 years. By this definition, there are 82 short-term spies and 27 long-term (see Table 5).[38]

[38] We recognize, of course, that lasting 2 years or more in an espionage career does not necessarily imply that more harm to national security occurred. William Kampiles, for example, a former CIA employee and short-term spy, in 1977 did serious harm by selling to the Soviets one TOP SECRET technical manual on an intelligence surveillance system. It is our intention in the next report to acquire general estimates of the amount of damage caused by the spies' actions.

Table 5

Rationale for Selecting a Two-Year Cut-Off for Short-term and Long-term Spies

Duration of Espionage in Years	Number of Spies	
0	25	82
<1	35	
1 - 1.9	22	
2 - 2.9	5	27
3 - 3.9	1	
4 - 4.9	3	
5 - 5.9	2	
6 - 6.9	3	
7 - 7.9	1	
8 - 8.9	0	
9 - 9.9	5	
10+	7	
Total	109	
Missing Cases	22	

Are there characteristics which distinguish the two groups? One factor appears to be the age at which espionage began. Table 6 compares the 67 short-term and 24 long-term spies for whom we know age when they began espionage. Fifty-two percent of those who began espionage at an earlier age (27 years or below) were caught within 2 years while only 25% lasted beyond the 2 years. Thus, age appears to make a difference in how long spies survive. The younger starters fare less well.

Table 6

Age at Which Espionage Began
Short-term vs. Long-term Spies

Age Began	Short-term		Long-term	
18 - 22	14 (21%)	52%	2 (8%)	25%
23 - 27	21 (31%)		4 (17%)	
28 - 32	7 (11%)		8 (34%)	
33 - 37	11 (16%)		4 (17%)	
38 - 42	9 (13%)		2 (8%)	
43 - 47	4 (6%)		1 (4%)	
48+	1 (2%)		3 (12%)	
Total Number of Cases =	**67**		**24**	

Number of Cases = 91
Number of Unknown Cases = 40

A second factor which covaries with short-term and long-term spying is recruitment and volunteering to commit espionage. Duration of espionage and whether the individual volunteered or was recruited is known for 105 of the 131 cases. Table 7 shows there are 81 short-term spies and 24 long-term spies. Of the 81 short-term spies, 78% volunteered while 22% were recruited. Of the 24 long-term spies, 54% volunteered while 46% were recruited. So spies appear to do less well when they volunteer than if they are recruited.

Perhaps being recruited gives new spies the immediate attention of experienced foreign intelligence service personnel to provide training in techniques in the first activities of espionage, and this may account for the greater survival rate of recruits (46% long-term vs. 22% short-term).

Table 7

Short-term and Long-Term Spies by Volunteer or Recruit

	Short-term	Long-term
Volunteered	63 (78%)	13 (54%)
Recruited	18 (22%)	11 (46%)
TOTAL:	81	24

Number of Cases = 105
Number of Unknown Cases = 26

Motives vary somewhat between short-term and long-term spies. A crosstabulation of the variables *motive for espionage* [39] and *duration of espionage* is illustrated in Table 8. Unfortunately, the sample size for long-term spies is rather small, so we have to be cautious about making generalizations. However, money is still the dominant motive, followed by disgruntlement/revenge (16%) for the short-term spies and ideology (19%) for the long-term ones. Overall, the patterns of motives appear fairly similar for both groups.

[39] The stated motive was recoded into the six most common motives (derived motive) to simplify the analysis.

Table 8

Motives for Short-term and Long-term Spies

Motive	Short-term (< 2 yrs.)		Long-term (> 2 yrs.)	
Money*	43	(58%)	13	(50%)
Ideology*	5	(7%)	5	(19%)
Disgruntlement Revenge	12	(16%)	2	(8%)
Thrills	7	(9%)	2	(8%)
Ingratiation	3	(4%)	3	(12%)
Coercion	2	(3%)	1	(3%)
Miscellaneous	2	(3%)	0	(0%)
Total	74		26	

Number of Cases = 100

Number of Unknown Cases = 31

* *For eight cases where ideology was the motive and for one case each where money and revenge were motives, there was no information on duration of espionage.*

Geographical Concentrations of Espionage

A picture of the geographical concentrations of espionage can be drawn when we know where the 131 incidents of espionage occurred. Of the 72 cases in which the U.S. location is known, Washington, DC, with 15% of the cases is the most popular city for espionage; New York City and Norfolk, VA, are next with 7% of the cases each. Given the concentration of Defense Department facilities, intelligence agencies, and other agencies of the federal government in these three areas, it is not surprising that more cases would occur there.

Aggregating the locations of espionage into regions and localities yields a more general picture. Figure 14 shows that the Mid-Atlantic region, defined to include New York, Maryland, Washington, DC, and northern Virginia, had the most espionage cases (44%). California is next with 24%, reflecting that state's increasing importance as a center for defense industries. These two regions also represent the areas where Soviet diplomats are permitted to operate: at the United Nations in New York, at the embassy in Washington, and at the large consulate in San Francisco. It is also possible that more espionage cases are discovered in these regions simply because more counterintelligence resources are directed toward these lucrative areas.

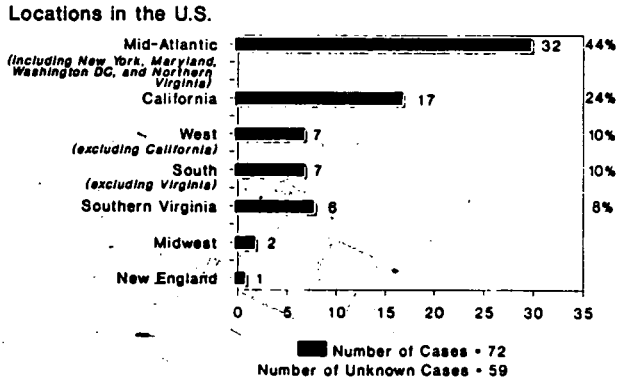

Figure 14. Geographical Concentrations of Espionage in the United States

Figure 15 shows the 37 known locations of espionage by Americans outside the United States. West Germany, with its large contingent of Americans with military duties, had the most instances of Americans betraying American secrets, with 32% of the cases; Japan with 11% was next.

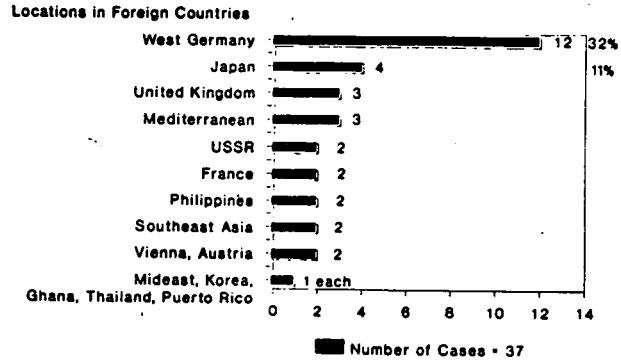

Figure 15. Geographical Concentrations of Espionage Outside the United States

Countries Receiving Information

Figure 16 lists the countries receiving information through espionage against the United States. Not surprisingly during the Cold War period, the country receiving the most information from espionage by Americans has been the Soviet Union; 63% of the cases directed information to the USSR. In another 11% of the cases information was sent to Warsaw Pact countries, from which it most likely was shared with the USSR. Thus 74% of the cases ultimately benefited the USSR. In 14% of the cases there was no recipient, usually because the person was apprehended before he or she could make the transfer. The remainder of cases are a miscellany: three Arab countries and China benefited from one case each, and South Africa from two. Five

close allies of the United States gained information from espionage in at least one instance: Great Britain, Israel, Holland, and the Philippines.[40]

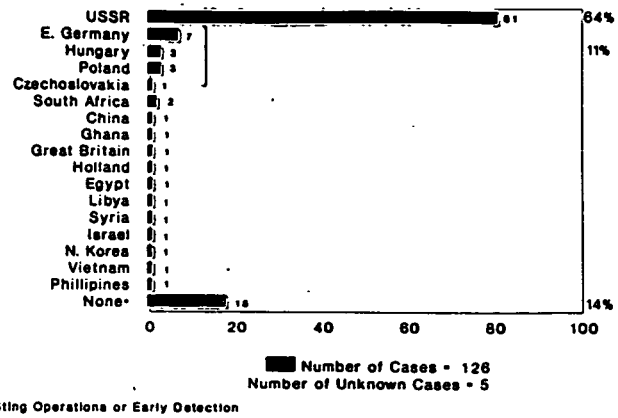

Figure 16. Countries Receiving Information

Espionage Trends

Recruitment and Volunteering Over Time

Table 9 shows how the pattern of recruitment and volunteering has changed over time. For the 107 cases where we have information, recruitment and volunteering were equal during the the 1940s, and there is even a slight shift toward recruitment in the 50s. However, the three decades since 1960 have seen a dramatic shift towards volunteering, culminating in the 80s with almost 90% of the cases volunteering.

[40] The three Arab countries were Egypt (Mrs. Ahadi, pseudonym), Syria (Richard Hughes Barrett), and Libya (Waldo H. Dubberstein). The spies who provided information to South Africa were Stephen Anthony Baba and Thomas Joseph Dolce and to China, Larry Wu-Tai Chin, Great Britain received classified materials from Samual Loring Morison, Israel from Jonathan J. Pollard, Holland from Joseph S. Petersen, and the Philippines from Michael N. Allen.

Table 9

Volunteering and Recruitment Over Time

	Volunteered		Recruited	
Before 1945	1	(33%)	2	(77%)
1945 - 1949	2	(50%)	2	(50%)
1950 - 1959	4	(36%)	7	(64%)
1960 - 1969	15	(71%)	6	(29%)
1970 - 1979	16	(70%)	7	(30%)
1980 - 1989	40	(89%)	5	(11%)
	78		29	

Number of Cases = 107

Number of Unknown Cases = 24

Motivation Over Time

A crosstabulation of variables *motive for espionage* by *data espionage began* confirms that the motives of American spies have shifted over the last 44 years. Table 10 shows that money as a motive substantially increased over the time period; ideology has tapered off somewhat, as also has coercion; disgruntlement and revenge have increased slightly, and spying to please a loved one (ingratiation) has remained constant over the last 30 years.

Table 10

Motivation Over Time

	Money	Ideology	Disgruntlement/Revenge	Thrills	Ingratiation	Coercion
Before 1945	-	2	-	-	-	-
1945 - 1949	-	3	-	1	1	-
1950 - 1959	3	3	2	-	-	1
1960 - 1969	8	3	2	1	3	4
1970 - 1979	10	3	2	1	3	1
1980 - 1989	27	1	7	1	3	-
	48	15	13	3	7	6

Number of Cases = 92

Number of Unknown Cases = 39

Espionage Cases Over Time

Some final aspects of espionage are the comparative duration of espionage cases over time and the number of espionage cases active at various points in time. Each of the following three figures includes all 131 of the cases in the database.

Figure 17 depicts the number of active espionage cases in each year from 1930 to 1990. This illustration gives one indication of the year-by-year vulnerability of the nation from espionage. It demonstrates that espionage against the United States by Americans has risen slowly during the 1940s and 1950s to a peak in the early 1960s, when for 5 years there were 8 to 12 cases active each year. From 1965 to 1975 the number of cases fell off to between 5 and 7 per year. The espionage cases rose again in 1975 through the next decade to a new peak of 24 active cases in 1985, after which the levels dropped off once again. However, this does not necessarily mean there were actually fewer espionage cases in the late 1980s; it is possible that spies may have been committing espionage during that period but have not yet been discovered or are under investigation.

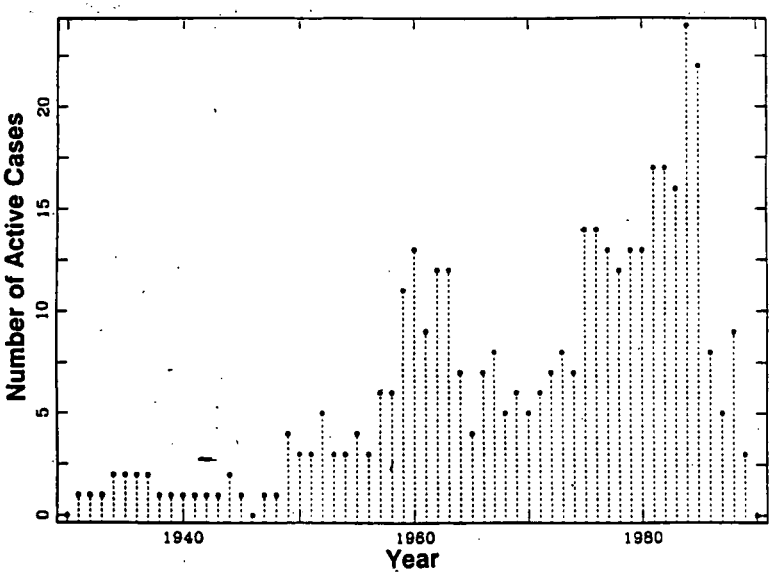

Figure 17. Active Esplonage Cases During a Year

Figure 18 combines the number of active cases in a given year with the duration of each case. Each case of espionage is pictured starting with a small circle, lasting through time with a horizontal line, and ending with another small circle. Counting up from a given year the number of lines crossing that year gives a sense of the number of cases active then, although the total numbers are somewhat impressionistic due to the overlapping of cases which had very small durations, such as a single incident, which appear as single small circles on the graph. The pattern noted for Figure 17, of a peak around 1960, a falling off, followed by another higher peak in the mid-1980s, can be seen in the overall pattern in this figure as well.

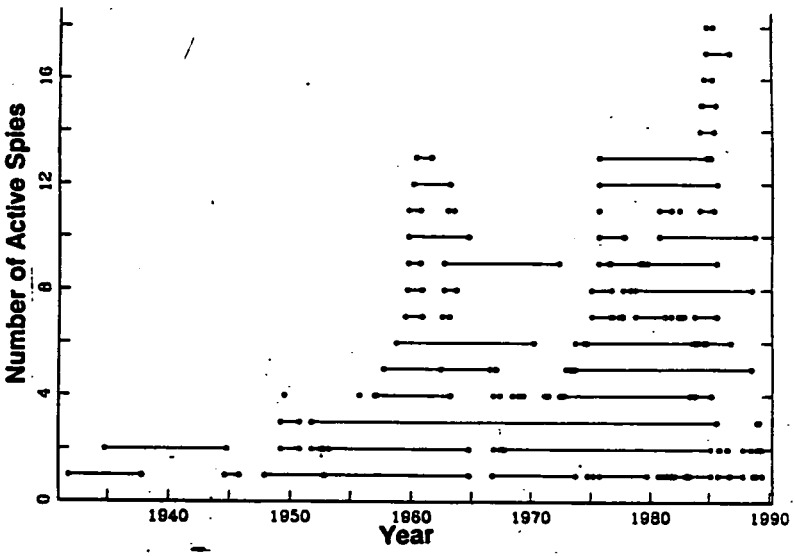

Figure 18. Known Espionage Cases at any Time

Finally, Figure 19 illustrates for the cumulative number of cases of espionage the duration of each case over time.

Finally, Figure 19 illustrates for the cumulative number of cases of espionage the duration of each case over time.

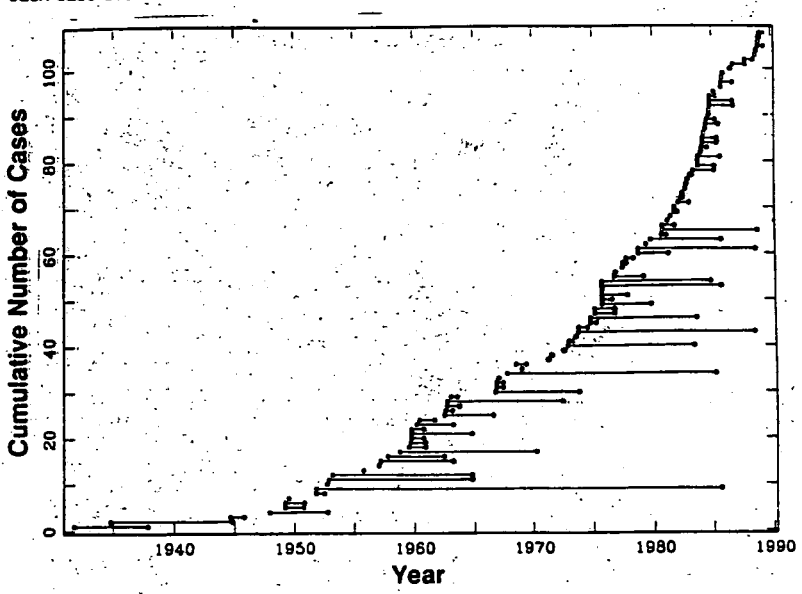

Figure 19. Estimated Duration of Espionage Activity

The earliest case starts at the far left of the chart, and as each new case starts the graph moves up and to the right one position. Larry Wu-Tai Chin is an obvious benchmark, running from 1952 until 1985 along the bottom of the graph. Cases of very short duration are shown with short horizontal lines; a single incident is shown with a single circle. This graph illustrates in a different way the cluster of cases seen in the earlier two figures that date from the early 1960s and the later, larger cluster in the 1980s. The figure also depicts the trend in the 1980s toward many more cases of short-term espionage which were caught immediately or after a short time. It must be noted also that there may well be more spies who have operated for long periods of time but who are as yet undetected. Their cases are obviously not reflected in this graph.

Discussion/Conclusions

General Findings

The descriptive analyses of the espionage data allow us to say something about American espionage and those who spy, although it must be understood that one cannot use such a "profile" as a basis of prediction without more complete data and additional analyses.

Most American spies have been Caucasian, heterosexual males. Of those in the military, most have been enlisted rather than officers. Espionage most often takes place at a young age, partly reflecting the young age at which Americans enter the military. The spies are fairly well educated, generally married, and most frequently hold technical or intelligence jobs.

In terms of volunteering and recruiting, 73% of the spies were volunteers as compared with 27% who were recruited, either by foreign intelligence agencies or by fellow Americans. Patterns of volunteering and recruiting changed over the 44-year period with the large shift toward volunteering in the past 20 years.

Eighty percent of those who spied inside the United States were volunteers, 20% were recruited; 61% of those who spied overseas volunteered, 39% were recruited. The percentage of people recruited overseas is twice as high as those recruited within the United States.

As for motivation, money has been the major reason for espionage, followed by ideology and disgruntlement/revenge. When we look at motivation over the past 44 years, money has increased dramatically. However, despite the fact that espionage

was mostly committed for money, rewards have been very small, with 48% of the spies receiving nothing, either because they were discovered before they could be paid or because they acted for motives other than money. Ideology as a motive did not completely die out; there were several cases in the last 20 years where ideology played a role.

Most spying careers last for only short periods of time, many just for one incident. Only eight have lasted more than 10 years, as far as we know.

There are more long-term spies, here defined as those whose espionage careers lasted more than 2 years, among those to come to espionage at a later age. In other words, spies who begin espionage young are less likely to survive a 2-year career. Long-term spies are slightly more likely to have volunteered than to have been recruited; failures, those who were caught within 2 years, were more than three times as likely to have volunteered as to have been recruited.

Almost half the cases of espionage in the United States occurred in the mid-Atlantic area, and the next most important region was California. Outside the United States, spying occurred most frequently in West Germany. The Soviet Union and four other Communist Bloc Countries accounted for three quarters of the information received through American espionage.

Future Research

This report has provided an initial view of individuals who have committed espionage. We have described the nature of the database, and we have run some simple crosstabulations to examine relationships among some of the data elements.

The most pressing future requirement is to fill in the missing data where possible. While the database will never be "complete," we anticipate a great deal of new information in the near future.

A second undertaking will be to supplement the espionage file. Recent cases will be added as they are identified, and more variables may also be added.

Finally, more sophisticated analytical tools will be applied to the database to extract information concerning interactions among the variables. For example, a particular subcategory, young enlisted personnel, could be analyzed in depth to extract combinations of factors which appear related to the espionage behavior. The goal will be to make the information more readily interpretable both to policymakers and to field agents. It is our hope that the materials can be used to enhance security education and awareness programs.

LIST OF APPENDIXES

APPENDIX A

SPIES IN THE MILITARY

Army

Attardi, Joseph O.
Barrart, Richard Hughes
Dunlap, Jack Edward
Gessner, George John
Greenglass, David
Hall, James W., III
Harris, Ulysses L.
Helmich, Joseph George, Jr.
Johnson, Robert Lee
Mintkenbaugh, James Allen
Payne, Leslie J.
Peri, Michael A.
Rhodes, Roy Adair
Richardson, Daniel Walter
Rohrer, Glenn
Safford, Leonard Jenkins
Slavens, Brian Everett
Whalen, William Henry

Navy

Baba, Stephen Anthony
Brown, Russell Paul
Drummond, Nelson Cornelious
Ellis, Robert Wade
Fleming, David
Fryer, Edwin Richard
Garcia, Wilfredo
Graf, Ronald Dean
Haguewood, Robert Dean
Hawkins, Stephen Dwayne
Horton, Brian Patrick
Irene, Dale Verne
Johnson, Michael Charles
Kearn, Bruce L.
King, Donald Wayne
Ledbetter, Gary Lee
Madsen, Lee Eugene

McGuinness, James Francis
McIntyre, Glenn Arthur
Murphy, Michael
Pickering, Jeffrey L.
Pizzo, Francis X.
Pugh, Ernest C.
Tobias, Bruce Dean
Tobias, Michael Timothy
Walker, John Anthony. Jr.
Walker, Michael Lance
Whitworth, Jerry Alfred
Wilmoth, James R.
Wine, Edward Hilledon
Wold, Hans P.
Wydra, Roman Michael

Marine Corps

Coberly, Alan D.
Cordrey, Robert E.
Lonetree, Clayton J.
Moore, Michael R.
Yager, Joel

Air Force

Boeckenhaupt, Herbert W.
Bronson, Staff Sergeant (pseudonym)
Buchanan, Edward O.
Cascio, Guiseppe E.
Cooke, Christopher M.
Crest, Sergeant (pseudonym)
DeChamplain, Raymond G.
French, George H.
Grunden, Oliver Everett
Herman, Master Sergeant (pseudonym)
Hughes, William H.
Kauffman, Joseph Patrick
Mira, Francisco de Asissi
Mueller, Gustav Adolph
Ott, Bruce D.
Perkins, Walter T.
Thompson, Robert Glenn
Walton (pseudonym)
Wesson (pseudonym)
Wood, James D.

Civilian Spies

Mrs. Ahadi (pseudonym)
Allen, Michael H.
Bacon, Douglas Roger
Barnett, David H.
Bell, William Holden
Borger, Harold N.
Boyce, Christopher John
Butenko, John William
Cavanagh, Thomas Patrick
Chambers, Whittaker
Chin, Larry Wu-Tai
Cohen, Morris
Conrad, Clyde Lee
Coplon, Judith
Davies, Allen John
Dedeyan, Sahag K.
Dolce, Thomas Joseph
Dubberstein, Waldo H.
Gilbert, Otto Attila (illegal)
Gold, Harry
Hamilton, Victor Norris
Harper, James Durward, Jr.
Hiss, Alger
Howard, Edward L.
Humphrey, Ronald Louis
Jeffries, Randy Miles
Kampiles, William
Koecher, Karl F. (illegal)
Kunkle, Craig D.
Lee, Andrew Daulton
Martin, William H.
Meyer, Paul Carlo
Miller, Richard
Mitchell, Bernon Ferguson
Moore, Edwin G., II
Morison, Samuel Loring
Pelton, Ronald William
Petersen, Joseph S.
Petka, Lona
Pollard, Jonathan J.
Pollard, Anne Henderson
Ponger, Kurt Leopold
Rees, Norman
Rosenberg, Ethel
Rosenberg, Julius
Sattler, James Frederick
Scarbeck, Irvin C.
Scranage, Sharon M.
Sobell, Morton
Souther, Glenn Michael (Navy Reserve)
Spade, Henry Otto
Verber, Otto
Walker, Arthur James
Wallen, Nick Clark
Wolf, Robert C.
Wolff, Jay Clyde

APPENDIX B

Description of Fields

The following comprise the variables in the PERSEREC espionage database. Self-explanatory variables are simply listed; the others are explained in a short paragraph within the list.

1. **Name**
2. **Given Name(s)**
3. **Social Security Number**
4. **Citizenship**. All cases are U.S. citizens; if native born, they are designated "USA," if naturalized citizens, they are designated "USA nat."

5. **Date of Birth.** This is given in the recording format of the Department of Defense: year, month, day e.g., 601225.

6. **Year of Birth.** This is given in common date form, e.g., 1966.

7. **City of Birth.** The city in which the individual was born.

8. **State of Birth.** The state in which the individual was born.

9. **Country of Birth.** The country in which the individual was born.

10. **Education Level.** The highest level of education attained and degree received if known.

11. **Marital Status.** The marital state of the individual at the time espionage began, if known, and changes in that status during the period of espionage.

12. **Sexual Preference.** The pattern of sexual behavior by the individual, i.e. "heterosexual" or "homosexual." Married individuals are inferred to have been heterosexual, although we recognize this assumption may oversimplify the situation.

13. **Gender.**

14. **Race.** Caucasian, Black, Asian, or American Indian.

15. **Clearance.** The level of security clearance held by the individual at the beginning of the espionage incident.

16. **Clearance Qualifier.** An explanation field for the Clearance field. It includes details or circumstances relating to clearance level other than the names of the levels themselves.

17. **Type of Information Involved.** The type of information compromised or endangered by the espionage incident. Subject matter which remains sensitive is given in general terms, relying on what has been made public.

18. **Alias.** Other name(s) under which the individual operated during the espionage incident.

19. **Military or Civilian.** If a civilian at the time espionage began, given as "civilian." If a member of the military services, the name of the service is given.

20. **Rank.** The military rank of those individuals in military service; if civilian, given as "civilian."

21. **Years of Federal Service.** The number of years the individual had served the United States government in any job at the beginning of the espionage incident.

22. **Former Job.** Description of job formerly held if this previous job had provided the access to classified information which the individual later divulged in the espionage incident. This variable will eventually be expanded to include all former jobs.

23. **Job Organization at Time of Espionage.** The name of the organization in which the individual worked at the beginning of the espionage incident.

24. **Job Type.** The type of job the individual held at the beginning of the espionage incident, e.g., "intelligence analyst," "clerk," or "finance officer."

25. **Job Location.** The geographical location of the job held by the individual at the beginning of the espionage incident.

26. **Job Field.** The generic or general occupation in which the individual worked at the beginning of the espionage incident, e.g., "clerical," "cryptography," or "personnel."

27. **Age Began Espionage.** The individual's age when he began the incident of espionage.

28. **Volunteer or Recruit.** Designates whether the individual offered to commit the espionage or security violation, or was recruited by another individual or organization.

29. **Receiving Country.** The name of the country which received the information, or was the intended recipient of the information.

30. **Payment.** Gives the total amount of money or other compensation received by the individual over the course of the espionage incident.

31. **Payment Asked.** Gives the amount of compensation requested by the individual for his participation in the espionage incident.

32. **Stated Motive.** Gives the motive(s) ascribed by the individual to his behavior after the espionage incident was ended, usually during questioning by authorities.

33. **Motive Qualifier.** An explanation field in which details about the individual's motivations can be included.

34. **Inferred Motive.** Gives the motive(s) inferred for the individual's behavior during the espionage incident from other statements and circumstances developed about the case during the investigation. Inferences may have been made either by investigating authorities or by the present author.

35. **Derived Motive.** The stated motives were recoded into the six most common motives, *derived motives* to simplify analysis. These are money, ideology, disgruntlement, revenge, thrills, ingratiation and coercion.

36. **Accomplice.** Name(s) of other persons with whom the individual worked or cooperated during the espionage incident. This could be an American accomplice or a control from a foreign intelligence agency.

37. **How Espionage Began.** Categorizes the initiating behaviors of the individual into a limited number of generic patterns, in order to facilitate comparison across cases, e.g., gave info to go-between.

38. **How Began Qualifier.** Describes in some detail the initiating behaviors undertaken by the individual at the start of the espionage incident.

39. **Mode of Operation.** Describes how the individual went about committing espionage, particularly if the espionage occurred over a period of time in which patterns were developed.

40. **Later Job.** Gives the job the individual took after the espionage incident ended, for those persons who stopped committing espionage and were not immediately apprehended.

41. **Foreign Relatives.** Lists "yes," "no," or "unknown."

42. **Foreign Relatives Qualifier.** An explanation field which gives details about the foreign relatives of the individual, such as the relationship between them and their country of origin.

43. **Substance Abuse.** Gives the names of intoxicating or illegal substances known to have been abused by the individual during the period of the espionage incident.

44. **Risk Taker.** Categorizes the individual as having a behavior pattern of seeking risk; given as "yes," "no," or "unknown."

45. **Risk Taker Qualifier.** An explanation field which gives details about the type of risks courted by the individual, other than engaging in espionage.

46. **Date Began.** The date on which the espionage incident began.

47. **Date Ended.** The date on which the espionage incident ended.

48. **Date of Arrest.** The date on which the individual was arrested.

49. **Arresting Agency.**

50. **Date of Sentence.** The date on which the individual was sentenced.

51. **Sentence.** Given in years and fractions thereof.

52. **Sentence Qualifier.** An explanation field giving details about the sentence or disposition of the case, such as defections, suicides, paroles, plea bargains, administrative discharges.

53. **Coercion.** Designates whether the individual was subjected to coercion, i.e., blackmail or threats, by listing "yes" or "no."

54. **Coercion Qualifier.** Gives the details of the coercion.

55. **Duration.** Gives the length of time the espionage incident lasted.

56. **Money Problems.** Lists whether money problems were the main cause of the espionage, "yes" or "no."

57. **Money Problems Qualifier.** An explanation field which gives the details of the money problems involved, usually "debt" or "greed."

58. **Source.** The source(s) from which the information for the record was derived.

APPENDIX C

Estimated Annual Income From Espionage

Name	Estimated Period	Average Annual Gross Income *	Income
Howard	** 1984–85	161,000	161,000
Walker, Jr	1968–85	1,000,000	59,000
Bell	1979–81	100,000	50,000
Helmich	1963–66	131,000	44,000
Hall	1981–88	130,000	43,000
Whitworth	1976–85	332,000	37,000
Boyce	1975–77	70,000	35,000
Lee	1975–77	70,000	35,000
Harper	1975–83	250,000	31,000
Chin	1952–85	1,000,000	30,000
Barnet	1976–80	92,000	23,000
Dubberstein	1977–79	32,000	16,000
Bunlap	1960–83	40,000	13,000
Walker, A	1981–82	12,000	12,000
Pelton	1980–85	35,000	7,000
Pollard, J	1976–85	45,000	5,000

Estimated Annual Income From Espionage—Continued

Name	Estimated Period	Average Annual Gross Income *	Income
Broekenhaupt	1962–66	17,500	4,370
DeChamplain	1971–71	3,800	3,800
Mira	1982–83	3,750	3,700
Lonetree	1985–86	3,500	3,500
Kampiles	1978–78	3,000	3,000
Rhodes	1952–53	3,000	3,000
Drummond	1958–62	2,500	2,500
Whalen	1959–61	5,000	2,500
Sattler	1967–74	15,000	2,000
Williams	1963–72	17,000	2,000
Dedeyan	1975–75	1,000	1,000
Sattord	1967–67	1,000	1,000
Brandon	1977–78	9,500	9,500
Grunden	1973–73	9,500	9,500
Wood	1973–73	9,500	9,500
Madsen	1979–79	700	700
Garcia	1985–87	800	400
Haguewood	1986–86	360	360
Greenglass	1944–46	700	350
Gersher	1960–61	208	208
Thompson	1957–63	500	90
Cooke	1980–81	50	50

* Not corrected for inflation.
** Anything less than 2 years is scored as 1 year.

Chairman BOREN. We've also received a communication from the American Civil Liberties Union from Mr. Morton Halperin in the form of a letter, and if there is no objection, I will enter that letter into our hearing record so that it will be studied also.

[The document referred to follows:]

AMERICAN CIVIL LIBERTIES UNION
Washington Office, April 4, 1990.

HON. DAVID L. BOREN,
Chairman,
Permanent Select Committee on Intelligence,
SH 211, Hart Senate Office Building,
Washington, D.C. 20510.

DEAR CHAIRMAN BOREN: I write on behalf of the ACLU to express our opposition to the FBI being given authority, in the Intelligence Authorization Act for 1990, for a national security letter exemption to obtain telephone toll and credit records. Such an exemption would give the FBI authority to obtain these protected records without a subpoena in foreign-counterintelligence cases. Similar changes sought by the FBI last sparked Congressional concern for privacy and other civil liberties.

The ACLU's concerns remain the same: 1) the FBI has not demonstrated a compelling need for either of the exemptions; and 2) we believe that legislation that implicates civil liberties should be addressed separately and not as part of the authorization act process.

There are only two instances in which Congress has authorized the FBI, in counterintelligence investigations, to obtain information about individuals without a subpoena, search warrant or court order pursuant to a national security letter. First, in 1986, the Electronic Communications Privacy Act (ECPA) included a provision requiring communications common carriers to disclose subscriber information and long distance toll records to the FBI in response to a national security letter.

The FBI now seeks to drastically expand that exemption to allow them access to the telephone toll records of people who have merely been in contact with people the Bureau has reason to believe are agents of a foreign power. If authorized, the Bureau could easily gain access to personal information on people who are not sus-

pected of criminal activity, but who, for example, may have placed an innocent call to the Soviet Embassy.

Second, Congress also authorized in the 1987 Intelligence Authorization Act an amendment to the Right to Financial Privacy Act (RFPA) that requires banks to provide customer records to the FBI in response to a similar letter. In that case, the FBI presented to Congress its case for obtaining financial records in foreign counterintelligence cases and the difficulty of obtaining those records without a court order. The ACLU opposed the national security letter in ECPA, but we understood it was a necessary price of securing new protections on electronic communications.

The FBI now seeks similar access to individuals' credit records held by consumer reporting companies. The FBI has yet to justify its need to add such highly personal, sensitive information to the narrow category of records subject to the national security letter exemption. Further, the House Banking Committee's Subcommittee on Consumer Affairs is currently engaged in a comprehensive updating and strengthening of the Fair Credit Reporting Act. To our knowledge, the FBI has not requested the Subcommittee's involvement in this matter.

In both instances where Congress authorized the national security letter, Congress recognized that the national security letter procedure departs dramatically from the procedure necessary to obtain a court order. A national security letter gives the FBI the authority to obtain records, without judicial approval, and without providing notice to the individual that his or her records have been obtained by the Bureau.

As set forth in both ECPA and RFPA, the FBI may present a national security letter, signed by the Director or his designee, to a phone company or bank alleging specific and articulable facts giving reason to believe that the subject of the record is an agent of a foreign power, as defined in the Foreign Intelligence Surveillance Act (FISA). The exemption requires no judicial review of the request, and the record holder is barred from disclosing to anyone that a letter has been issued.

Two years ago, the FBI was unsuccessful in its efforts to obtain a national security letter exemption in a bill that would have created a federal right of privacy in library and video records. The section of the legislation that would have protected library records was dropped because of the controversy, but the Video Privacy Protection Act passed without the exemption.

In addition, during the CISPES investigation the FBI made extensive use of the national security letter, issuing dozens of letters to receive access to telephone toll records of CISPES chapters and, in some cases, of chapter members' homes.

The national security letter exemption diminishes the due process and privacy protections for individuals; the two current proposals should be introduced as separate legislation on which public hearings can be held. The Committee would then be able to test the FBI's case for the exemptions and to hear from witnesses who have objections.

We are available to work with you on this matter.

Sincerely,

MORTON H. HALPERIN.

cc: Members, Permanent Select Committee on Intelligence
Patrick J. Leahy, Chair
Senate Judiciary Subcommittee on Technology and the Law
Donald W. Riegle, Jr., Chair
Senate Committee on Banking, Housing, and Urban Affairs

Chairman BOREN. In addition, Senator D'Amato and Senator Cranston, neither of whom will be able to be with us today, have asked me to place in the record their statements, which I will do at this point, without objection.

[The prepared statements of Senator D'Amato and Senator Cranston follow:]

PREPARED STATEMENT OF SENATOR ALFONSE D'AMATO

Thank you, Mr. Chairman. During the 99th Congress, the Senate Select Committee on Intelligence issued a report entitled "Meeting The Espionage Challenge: A Review of United States Counterintelligence and Security Programs." In that report, the Committee stated:

"The Committee's finding underscore a fundamental challenge to the nation. The hostile intelligence threat is more serious than anyone in the Government has yet acknowledged publicly. The combination of human espionage and sophisticated tech-

nical collection has done *immense damage* to the national security. To respond to the threat, the U.S. must maintain effective counterintelligence efforts to detect and neutralize hostile intelligence operations directly, and defensive security countermeasures to protect sensitive information and activities."

Last fall, this Committee requested the establishment of a Panel to study ways to improve our ability to deter and detect espionage activity. I would like to welcome today our distinguished witnesses, including the Panel's Chairman, Eli Jacobs, who will discuss the Panel's specific counterintelligence recommendations. These suggestions deserve our careful review and attention as we consider a framework for future legislative action.

Over the last decade, there have been a number of prominent espionage cases, technical security compromises, electronic surveillance incidents, and technology transfers which have caused great concern. These cases, to varying extents, compromised our military plans and capabilities, impaired our intelligence operations, and diminished some of our technological advantages.

As the Committee further stated in its 99th Congress report, "while there is always a need not to let worst-case analyses paralyze our military and intelligence services, the greater current danger appears to be a *wishing away* of the consequences of hostile intelligence efforts."

Mr. Chairman, we all have come to recognize that every entity within the United States government must work together in a unified effort if we are to adequately counter this serious problem.

Although there has been some recent debate over whether the relaxation between the Warsaw Pact and Nato has diminished espionage activity, I think it is interesting to note the words of CIA director William Webster in a February 21, 1990 *Washington Post* article entitled "CIA Director: East European Spies at Work." Director Webster stated, "It is important to remember that espionage and counterintelligence are widely recognized in Eastern Europe as necessary functions and the apparatus for this work is likely to remain in place."

He further stated, "but fundamental changes in intelligence missions are not likely while the Warsaw Pact treaty commitments are still in place. And so I don't expect military intelligence collection efforts to abate, certainly not in the near future."

I thank the members of the Jacobs' Panel for their time and their effort in addressing an issue of vital importance to the national security interests of this country and for suggesting ways to improve our counterintelligence capabilities. I look forward to their testimony.

Thank you, Mr. Chairman.

PREPARED STATEMENT OF SENATOR ALAN CRANSTON

I would like to commend the Panel members for the time and effort they have dedicated to reviewing U.S. counterespionage laws and policy. The members of this Panel have-undertaken the task with dedication and seriousness and have provided the Committee with a thoughtful report.

A number of the Panel's recommendations, however, cause me great concern. As a long-time champion of civil rights, I believe we should proceed very cautiously in enacting changes in law or advocating policy shifts that encroach upon the civil liberties of U.S. citizens. I find it ironic, that at a time of rapid, worldwide change in which tensions between the U.S. and the Soviet Union have been at their lowest level in years, and more and more countries throughout the world are building their own democratic institutions based on a respect for civil liberties, human rights, and free speech, we may be heading in a direction which places restrictions on the privacy rights of U.S. citizens and take actions which could have a chilling effect upon our First Amendment right to free speech.

There are three specific recommendations that I would like to focus on. The item that causes me the most concern is the recommendation to expand the Foreign Intelligence Surveillance Act to include physical searches. Under this provision the FBI would be given the authority to obtain a secret court order to conduct break-ins into the homes of Americans without ever notifying the targeted person. This provision seeks to legitimize activities now conducted pursuant to presidential authority. I do not believe the so-called "warrantless searches" now conducted are consistent with Fourth Amendment rights, nor do I believe legitimizing these activities by making statutory changes to permit the FBI to obtain secret court orders to carry out such searches is the appropriate response to the concerns raised by this Panel.

Americans whose homes are searched should be told of the transgression so they can assert their constitutional rights to challenge such conduct by the Government.

There are two other recommendations I would also like to touch upon since they have already been proposed by the Administration and are currently being considered by the Intelligence Committee.

The Administration is seeking an amendment to the Electronic Communications Privacy Act to give the FBI authority to use the national security letter procedure to obtain telephone subscriber information on persons with unlisted telephone numbers who are contacted by foreign power establishments or foreign agents. In other words, if a U.S. citizen is contacted by the Soviet embassy for legitimate reasons, that individual could later receive a visit from an FBI agent asking why she or he was phoned by the Soviet embassy. The FBI should have some other basis to question an individual aside from the fact that she or he was simply a party to a phone call. Unless that issue is clarified, granting additional authority to the FBI would certainly lead to more cases in which the FBI questions Americans who legitimately and innocently communicate with foreign nationals, embassies, or organizations. Two years ago the Committee held hearings on the FBI's unjustified investigation of CISPES—the Committee in Solidarity with the People of El Salvador—and last year this Committee issued a public report criticizing the FBI's conduct of that investigation. One of the techniques the FBI used improperly in that case was obtaining the long-distance phone records of numerous CISPES chapters throughout the country. The FBI investigation turned out to be grossly misguided. This record of abuse of authority, however, does not give me great confidence that investing more power in the FBI will be used prudently and judiciously.

The Panel has also endorsed legislation proposed by the Administration this year to amend the Consumer Credit Protection Act to give the FBI authority to obtain consumer credit information without the knowledge of the targeted person by using the national security letter procedure in foreign counterintelligence and international terrorism investigations.

This type of consumer credit information, depending upon the credit reporting office involved, is oftentimes inaccurate and unreliable. Misuse of this information could disrupt or devastate one's personal life and professional career if carelessly employed. It is unclear under what circumstances the FBI would seek the information and how it could use the information once obtained. Those circumstances must be clarified and strict safeguards required.

Mr. Chairman, an American citizen's right to privacy and free speech are precious and fragile. We should proceed with great caution.

Senator MURKOWSKI. Mr. Chairman I wonder if my opening statement may be entered also.

Chairman BOREN. Without objection, we will enter Senator Murkowski's statement.

Senator MURKOWSKI. Thank you.

[The prepared statement of Senator Murkowski follows:]

PREPARED STATEMENT OF SENATOR FRANK MURKOWSKI

Mr. Chairman, let me commend you and the Vice Chairman for taking the initiative to convene this illustrious Panel and let me thank Mr. Jacobs and his distinguished colleagues for the impressive service they have rendered this Committee and the country.

Every casual viewer of the evening news is aware that in recent years we have had an alarming succession of revelations of traitorous activity by some individuals in collaboration with foreign intelligence services. First, it was the "year of the spy" but soon it became the "decade of the spy." Whatever the time period, it is clear that our most valuable national secrets have proven disturbingly vulnerable to foreign espionage.

Loss of secret information has already cost the U.S. Government billions of dollars to repair known damage. Lives have been lost and national security has been jeopardized.

The Panel before us was convened to take a hard look at the problem—with particular attention to possible changes in the law that might improve our capacity to deter and defeat espionage.

At the same time, we must proceed with caution. Steps designed to tighten control over sensitive information and employees with access to that information, almost inevitably raise civil liberties concerns. This is a perpetual balancing act and

there are few easy answers. This is particularly the case when the current international climate suggests that the threat from Soviet and other East Bloc agents may be declining as the Cold War, itself, recedes.

Are we proposing to administer strong medicine for a disease that may be going into remission? I don't know the answer, but I look forward to the testimony here today to help provide it.

Chairman BOREN. Senator Metzenbaum, I believe you also have an opening statement.

Senator METZENBAUM. I do have a statement, Mr. Chairman, but let me just take one second to address myself to a subject that is not new to you nor to this Panel, and that is the question of overclassification. And I will enter it into the record rather than take up the time of the hearing at the moment. But in doing so I would urge upon you, and say that at the next Committee hearing I would hope that you and the Vice Chairman might advise me as to whether you'd be willing, to insist that the Administration come up within a time certain with its recommendations on this subject of overclassification. At the same, time I ask this Panel for their recommendations, but in each instance I would hope we would set a time certain, and I'm not talking about a year or two years, but I'm talking about relatively short periods of time.

Chairman BOREN. I appreciate your comments and we will put your full opening statement into the record. Senator Metzenbaum, on several occasions, has expressed his concern about the fact that while we want to protect those things that are legitimate secrets, we do not want to overclassify that which doesn't have national security importance. This can really impede the process because when so many things are classified that don't need to be, it causes people to become lax. So I appreciate and welcome his comments.

[The prepared statement of Senator Metzenbaum follows:]

PREPARED STATEMENT OF SENATOR HOWARD M. METZENBAUM

Mr. Chairman, counterintelligence and security are important functions of the Intelligence Community. Together, they form a crucial defense for our Government's sensitive information, operations, equipment and personnel. It is absolutely vital that this Government protect its secrets and combat the hostile operations of other countries' intelligence services.

I commend you, Mr. Chairman, as well as our Vice Chairman, for enlisting such a distinguished Panel to consider means of improving counterintelligence and security in the U.S. Government. They have been very thoughtful and hardworking. While some of their legislative proposals give cause for concern, there is also much that I will support.

Legislation can only go so far, however, to deal with a world that will see vastly increased contacts between east and west. Stiffer security and easier prosecutions will be tolerated only so far in a world where our enemies will be not the implacable foes of yesterday, but a shifting set of countries that may well cooperate with the United States in some spheres while competing in others.

If our secrets are truly to be protected, Mr. Chairman, then our security laws and regulations must be respected. Unfortunately, this is not the case today. The United States Government is in the ridiculous position of trying to protect uncounted numbers of secret documents, with millions more being created each year. Roughly 4 million people have access to such material. Over 700,000 people have access to TOP SECRET information alone.

Our current system for protecting secrets is rather like telling a park ranger to protect all the wildlife in Alaska from would-be poachers:

—there is too much to protect;

—too many people have access;

—nobody respects a system that classifies nearly everything; and

—the "poachers" of classified information will have more contact than ever with potential buyers, many of whom may be considered "respectable."

The first three aspects of this state of affairs are far from new, Mr. Chairman. In 1985, the Stilwell Commission that studied the "Year of the Spy" for the Defense Department concluded that "too much information appears to be classified and much at higher levels than is warranted." The Government's Information Security Oversight Office (or "ISOO") called overclassification "a continuing nuisance that eats away at the credibility of the entire system."

In 1986, our Committee found "that the classification system is unduly complicated and that it breeds cynicism and confusion in those who create and use classified information."

I submit that the only way to truly protect secret information in the modern world is to stop trying to protect everything. There must be discipline in the classification system, right from the start. People must be required to think before they classify, and there must be sanctions for overclassification—just as there now are sanctions for underclassification.

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.

In 1986, we endorsed a series of ISOO recommendations to curb overclassification and improve security awareness. ISOO had found several causes of overclassification, including sheer ignorance of the standards for classification, overcaution, and a desire to give more prestige to one's work or to avoid routine oversight. To curb these practices, ISOO recommended mandatory training, better agency inspection of their classification practices, and an Executive Order amendment to require reporting of cases of improper classification.

Four years later, we are still waiting for the Executive branch to act on those recommendations. But the world is not standing still while we wait. It is time for the Executive branch to act.

President Bush has endorsed revising the classification procedures, but asked the head of ISOO to get another group together and up-date their recommendations. Meanwhile, defense and intelligence officials have told this Committee that the security system itself is just much too big and too cumbersome—almost self-defeating at times—and that one solution must be to revisit the entire fundamental definition of what is national security information.

I agree with those officials. As useful as the suggestions of today's witnesses may be, they will achieve little without such a complete overhaul of the classification system.

Mr. Chairman, this Committee should call on the Administration to develop within 60 days, and to share with us, plans for significant classification reforms that can be enacted by the end of the year. Our national security cannot wait another five years. At the same time, Mr. Jacobs and his Panel should examine this issue and bring their influence to bear on the Executive branch to reduce substantially both the amount of classified information and the number of persons with access to that information.

Finally, if the Administration cannot revamp the classification system this year, I propose that this Committee and other interested committees report out legislation to enact this needed reform.

Several of the legislative proposals to be presented today place special burdens on more than two-thirds of a million loyal Americans who have access to TOP SECRET information. I firmly believe that the Administration must share those burdens by reforming its own system. Until it does so, I will be very concerned over proposals to make so many Americans give up more of their privacy or to create new criminal offenses that are easier than ever to prosecute.

Chairman BOREN. Let me ask other members of the Panel if they would like to make comments and I would welcome these comments.

Let me say also I know there are some proposals that have not been recommended that some wanted to be recommended. On the thirteen major legislative proposals it would help as we do call upon you for comments, if you would point out any disagreement or dissent from any particular recommendations. I would gather that the first three of you who have spoken do not dissent from

any one of the particular recommendations, is that correct? That you are basically supportive of the thirteen recommendations?

[The Panel nods in the affirmative.]

Chairman BOREN. Let me begin—with the understanding of the others—with Ambassador Linowitz, because I know that he needs to leave shortly for another appointment. We welcome your participation on this Panel. We particularly appreciate the sensitive concern which you've given to civil liberties issues. You have a long, very established record of sensitivity to civil rights. We appreciate your participation on this Panel, particularly because of your focus on those issues.

Ambassador Linowitz.

TESTIMONY OF AMBASSADOR SOL LINOWITZ

Mr. LINOWITZ. Thank you, Mr. Chairman.

I have very little really to add to the excellent presentations of Messrs. Jacobs, Inman and Edgar. But as I was listening to the presentation, it struck me that there are three questions that probably would be asked and should be asked about what we are doing here and the proposals we are making.

The first would be: if these proposals are adopted, does that assure we would have the kind of counterintelligence capability we need and should have. The answer of course is no. All we're doing here is offering some proposals which we think will be helpful in strengthening our capability. But certainly this is no prescription for doing it in its full sense the way it should be done and which will require, obviously, further study and effort.

The second question: can we be assured that what has to be done has been done to assure the protection and the preservation of constitutional rights and civil liberties. From the outset, as you know Mr. Chairman, we've been very much concerned about that aspect. It's clear enough that every time you try to work in the security field, you have got to be careful that you don't pass over the line into infringement on rights which people have been guaranteed.

And we have tried assiduously to examine every proposal and the language as we've crafted these proposals in order to assure that that does not happen. My own view is that we've succeeded in doing that, and that the proposals as they now have been presented to you will not raise any questions of significance with respect to the abuse or infringement of either constitutional rights or civil liberties.

And the third question is perhaps a little more difficult to tackle but I think one that we can expect: Aren't you really looking back to yesterday's experience to tell us how to deal with the problems of today and tomorrow? It's a new world, there are going to be new challenges, there are going to be new things we're going to have to be worrying about. And isn't this a case, as some have said, of locking the barn door after the horse is out, or as another aspiring classicist once put it, opening Pandora's box and letting out a Trojan horse.

[General Laughter.]

Mr. LINOWITZ. It doesn't seem to me that's it either of those, Mr. Chairman. It seems to me that what we've done here is precisely

because we are entering a new era of many unknowns and unanticipatables, that we have said we need strengthening in this intelligence capability by the kind of proposals we have put forward so we can do our job more effectively as we await the unknowns of the future.

And it seems to me that the proposals have succeeded in doing that and therefore, I think, merit support.

Chairman BOREN. Thank you very much, Ambassador Linowitz. We appreciate the comments and your contribution. We'll understand if you have to leave us before the proceedings are completed. Let me go on down the table and ask Mr. Lloyd Cutler if he might have a comment from his own perspective as a member of this Panel and from his wide ranging experience including serving as Counsel to the President.

TESTIMONY OF MR. LLOYD CUTLER

Mr. CUTLER. Thank you Mr. Chairman.

I join in all of the recommendations and I want to pay my compliments and respect to you and the Ranking Minority member and all of the other members of the Committee for the support and cooperation that you and the staff have given to us.

I also agree with everything that Ambassador Linowitz has said. I think I am in the one who first referred to this committee as the barn door committee. But I think the answer to that question is that there is lots of other horses still in the barn.

With respect to civil rights, I think we have tried to be as sensitive as we could to the civil rights and constitutional rights issues involved. And the best testimony of that is probably what we have left on the cutting room floor. There were many other proposals that were advanced that we did not endorse, because we thought they raised serious civil rights, constitutional or privacy issues.

Third, we have proposed—and I think this should be stressed—a number of civil remedies, which you will find in these proposals, in addition to criminal remedies. I think those are very important. First because of the enormous difficulty of proving a criminal case and the potential for gray mail in a criminal espionage related case. And second, because the standard of proof is different and particularly where the remedy sought is an equitable injunctive remedy it may be possible also to try the case without a jury.

There is one other civil remedy I think should be considered. We did not have time to develop it sufficiently. But in the mail fraud, the mail and wire fraud sections of the criminal code, it is Title 18 and it is in the 500 series, in addition to a criminal remedy, the government under the revision of the criminal code on which Senator Metzenbaum and others worked so hard, is entitled to bring a civil injunctive proceeding to enjoin a continuing mail or wire fraud, and to seek restitution, civil restitution. And it specifically provided that the standard of proof is a preponderance of the evidence standard of proof rather than a beyond a reasonable doubt standard of proof.

I think that section should be looked at and might be adapted so that a similar civil injunctive remedy including restitution was

available under all of the criminal espionage and national security laws.

Chairman BOREN. Thank you very much.

Mr. Warren Christopher has served as Deputy Secretary of State and also as Deputy Attorney General. We welcome you and any additional comments that you might like to make.

TESTIMONY OF MR. WARREN CHRISTOPHER

Mr. CHRISTOPHER. Thank you Mr. Chairman and members of the Committee. I want to be very brief so that you can get to your questions. Let me just add a brief comment from the rather parochial perspective of somebody from the Pacific rim side of our country.

I think it is important we not be lulled into, a false sense of security by events in Eastern Europe. Looking at the world west of the United States, looking at the world west from our Pacific rim, the world doesn't seem to have changed so much. The dangers of espionage in the Pacific basin are largely unchanged, conceivably even enhanced in the case of the world's most populous nation.

The conditions in the Middle East, as you look further west from the Pacific basin, are probably more dangerous now in terms of espionage than they were five or ten years ago. So I see, looking from where I reside, a fairly dangerous condition.

In terms of economic espionage, California is a good reminder of the importance of economic espionage in the future, in the high tech areas around Stanford University and around the University of California in San Diego. So I think that these statutory proposals are equally as significant now as they would have been before the dramatic events in Eastern Europe.

Mr. Chairman, I associate myself with all of the proposals that have been put forward. As Mr. Cutler has said, we had a rather active discussion of a number of proposals that did not come forward because we felt they went further than they should go in the civil liberties area.

The legislative process no doubt will unearth other problems with some of these suggestions. We don't think this is a perfect set of recommendations. But we hope they will be helpful to the Committee in the work that you now commence on these proposals.

Thank you very much, Mr. Chairman.

Chairman BOREN. Thank you very much, Mr. Christopher.

Mr. Culvahouse, we would welcome your comments. The Committee had the privilege of working with you when you served as Counsel to the President especially in the area of improving the oversight relationships between the Legislative branch and the Executive branch in the aftermath of the Iran-Contra matter. A number of very important, and I think very constructive, understandings were reached between the Committee and the Executive branch. We appreciate the role you played at that time. We welcome your thoughts on these recommendations.

TESTIMONY OF MR. ARTHUR B. CULVAHOUSE

Mr. CULVAHOUSE. Thank you Mr. Chairman. It is nice to be here today.

My colleagues admonished me that I could say something profound when my gray hair reached my temples; but saying that, I must say that I am reminded that almost 17 years ago, to the day, I came to work in the Senate as a staffer for the then-Vice Chairman of the Senate Watergate Committee. And as we all remember, a gentlemen only known as Deep Throat apparently advised one of our great newspapers investigating Watergate that it should "follow the money". And I think that is what we on the Panel have endeavored to do, once we identified that our current espionage problem in one of volunteers for money. We attempted to craft a number of appropriate solutions that would allow our investigators, our security officers and our background analysts to "follow the money" at the personnel security stage, at the detection and investigatory stage, and at the prosecution stage. I endorse and support all of the proposals of the panel.

Chairman BOREN. Thank you very much.

I would like to turn now to members of the Committee for their questions. We will basically follow the order of arrival rule and we will try to hold the first round of questions to five minutes each so that all the members of the Committee will have a chance to ask at least one round of questions. Senator Metzenbaum has indicated to me that he will return, and I think some others will as well.

We will begin with the Vice Chairman, Senator Cohen.

Senator COHEN. Thank you Mr. Chairman.

I am not sure who should answer this—Mr. Edgar or Admiral Inman—but in your first proposal you recommend that uniform requirements be established by law for persons who have TOP SECRET clearances. But these recommendations don't standardize the review processes used by either CIA or NSA. In other words, you have got the standards as uniform, but the evaluation techniques are not necessarily uniform. And what kind of problem does that present? I am thinking specifically of the Pollard case, and others that one might imagine where an individual could fail to get a TOP SECRET clearance in one agency, and move to a different agency that might have different techniques, and thereby secure access to TOP SECRET level documents?

Admiral INMAN. The principal difference Senator Cohen, is that we did not ultimately decide to bring forth any recommendation on mandatory use of the polygraph by other agencies except for personnel having access to cryptographic materials. And that is the primary difference in what is now applied at CIA at NSA, but not applied at other agencies.

Senator COHEN. Are there psychological tests that are applied at every agency?

Admiral INMAN. There are not psychological tests, but some of the—there are some areas where we did not specifically include recommendations on law where we believe the implementing directives prepared by the Executive branch are likely to bring some additional breadth.

Professor Edgar?

Senator COHEN. Does that create a problem for us in terms of having the appearance of uniformity and yet perhaps some deficiencies in one agency over another so that a person could still be declined access to TOP SECRET classified information in one

agency and get it in another even though you have got a uniform standard?

Mr. JACOBS. The effort was to develop a minimum uniform standard, Senator Cohen. Agencies would be free to go beyond that minimum standard and I believe that is the case both with the Central Intelligence Agency and National Security Agency.

Senator COHEN. Under your proposals, one of the recommendations is having access to travel records that are not currently authorized. What are the impediments now to getting access to those travel records? What did the Panel discover?

Admiral INMAN. There is not a clear authority to provide the records. And therefore, at least some of the airlines have been reluctant to provide information. Here we are trying to deal with very explicit issues of travel, in some cases where we have some leads of activity that we particularly want to pursue, others where we believe an individual may have engaged in activity and we want to be able to track the prospect of foreign travel. This is to remove the ambiguity about cooperating.

Mr. EDGAR. May I add that there is currently no legal inhibition to supplying these kinds of records. So it is not as though we are changing a protective law. We are simply making clear that an individual can give consent to this, in the belief that with his consent clear, more companies will be prepared to provide such records.

Senator COHEN. One of the recommendations you have is the criminalization of the possession of espionage devices. And of course those devices are not spelled out in terms of any kind of definitional language. What kind of devices—you mentioned a couple, Professor Edgar—what did you have in mind? Some of the press might inquire about Minox cameras——

Mr. EDGAR. Yes, these are the kinds of things—burst transmitters, one time pads, secret writing materials, materials of that kind. The language comes from present law. It does have a similar prohibition about possessing electronic surveillance equipment defined in terms of equipment that is primarily useful for these purposes. And of course the prohibition does not—I mean, you are only guilty of an offense under the proposal if in addition to possession, the intention to use the equipment in espionage can also be shown. So simply having possession of this equipment is not alone enough to ground a criminal prosecution.

Senator COHEN. Give me an example of how you would show intent if I have possession of a burst transmitter that I have acquired from the agency to look at over the weekend, to say look Bill, I got this new technique out here at the CIA, take it home and see what you think about it over the weekend. I mean how would you show intent?

Mr. EDGAR. I wouldn't in that case. But I think if someone has a burst transmitter that could only be read for example, by a foreign satellite and——

Senator COHEN. Suppose I take it as a collector's item?

Mr. EDGAR. Well, there are problems of proof. In the same way that a burglary tool situation has problems of proof, you have someone with a crow bar at 3 o'clock at someone's house and the prosecution has to prove that it is the intention to use the crow bar to get inside the house. So those kinds of difficulties of proof will be

present here as they would be in a comparable State prosecution for possession of burglary tools.

Senator COHEN. My time is up.

Chairman BOREN. Thank you very much.

Senator Danforth.

Senator DANFORTH. Mr. Christopher, I would like to focus on your comment that the problems are not behind us, and particularly as you said from your vantage point on the Pacific coast. And you talked about the universities and the high tech industries that are located in California and the possibilities of economic espionage. Do you consider that to be the wave of the future? Is this the big threat that we are looking at now, economic espionage?

Mr. CHRISTOPHER. Senator Danforth, I would say it is a major threat, but waves of history come and go. We are in a somewhat euphoric period with respect to Eastern Europe at the present time. But in 5 or 8 years, we could see a substantial change in that. So at the moment I would put a good deal of emphasis on economic espionage, especially as we have very large numbers of Asian students in our graduate schools and in our top research positions, and because there has always been a good deal of espionage from some of the Asian countries. But I would not want us to let down our guard on good old fashioned espionage for national security purposes as well as economic reasons.

Senator DANFORTH. Focusing though on the economic espionage, could you think up some possible examples that you could share with us about how it might work? Not real examples necessarily, but hypothetical cases of how economic espionage works. These particular cases on the chart are reasonably easy to understand. They tend to be government employees, they are working in particular agencies, they have TOP SECRET clearance, access to certain information, they are retained for money by mainly eastern bloc governments. What would be a hypothetical type of a situation in the field of economic espionage?

Mr. CHRISTOPHER. Well, Senator, as you well know I am a lawyer, not a technician or a scientist—there is a good deal of research going on in some of the California laboratories on superconductivity. A great deal of the economic future of the United States is tied up in that area. Some of that research can be in a TOP SECRET or highly classified area. The area of supercomputers is also ripe for research that has mainly economic focus, but could have an underlying national security threat to the United States because there is such a crossover between their use in business and their use in national security matters.

Senator DANFORTH. It would seem to me that in those cases the profile of the person who was doing the espionage might be different than in the case of somebody doing it within a government agency. It could be an employee of a high tech company, or it could be a graduate student at Cal Tech. Something on that order. Would that be conceivable, do you think, that it might be a different profile?

Mr. CHRISTOPHER. Yes, that certainly fits the concern I have, Senator Danforth. In the commercial world, it might be a different type of person. On the other hand, a number of those people in that category also have tremendous financial demands, and the

same reasons that caused the relatively low level government people that you see in this matrix to have turned to espionage could be effective, both in terms of their volunteering, that is their wanting to sell information, or being sought out.

Admiral INMAN. Senator Danforth, if I may, sixth from the bottom on the chart, I did not point out when we were going through, the Bell case. He was, in fact, not a government employee, but rather an employee of Hughes. Bell happened to have access to classified information related to radars. I think that one is a classic example of what are likely to see in industries particularly on the West Coast.

Senator DANFORTH. I have just one minute left, and this was given to me about 30 seconds ago. But let me ask Professor Edgar, I think these recommendations seem excellent, and I am sure the Committee will be addressing these specific recommendations. But do they go to the area of economic espionage? Most of them seem to be directed at employees of the Federal government who are operating in government agencies and dealing with government secrets. Would the same provisions be easily applicable to the field of economic espionage, or would there be a different list of possible remedies to deal with that problem?

Mr. EDGAR. The proposals do not specifically treat economic espionage. On occasion, in fact frequently, economic espionage directed at computer systems, would be directed at information that the government has protective interest in and would be characterized as classified or defense information. And so in that context, the proposal would pick the conduct up.

We did give some thought with respect to the possession of espionage devices—and indeed, it is something that might be further considered in the legislative process—to broadening coverage to include industrial espionage. That is, make possession with intent to commit industrial espionage as well as classical espionage criminal. The problem in doing it that made us stop at this moment is that you get into complexities of federal versus state law as the source of a legal authority protecting trade secrets. And so we decided to let that pass for now in this set of recommendations with the thought——

Senator DANFORTH. The hypothetical case, let's say, of a graduate student at Stanford, who is working part-time in Silicon Valley doing some work and is retained by a private concern, in let's say Japan, for cash, though that would be a different kind of a situation——

Mr. EDGAR. That would not be covered by——

Senator DANFORTH [continuing]. That was not covered by these recommendations.

Mr. EDGAR. That is not specifically covered by these recommendations. Correct.

Chairman BOREN. Congressman Bereuter, we would welcome any questions that you might like to ask. As I said, we have had conversations with Chairman Beilenson, Vice Chairman Hyde, and certainly welcome the involvement of the House Committee in this matter.

Representative BEREUTER. Thank you Chairman Boren. Thank you very much for inviting the House Select Committee on Intelli-

gence. I very much appreciate and I know all of the Members of the Committee do.

It is an unusually active day on the floor with the Clean Air Act, and we are preparing for the Export Administration Act through special briefings today on the Committee. Otherwise I am sure we would be joined here.

I want to compliment the prestigious Panel on their set of recommendations. I think they are particularly well crafted to be of direct value to our two Committees as we look at legislation. And I was particularly encouraged and pleased by the winnowing process that you have gone through to try to assure that you are not in any fashion negatively affecting constitutional or civil rights, and that you may have left significant amounts of things on the cutting room floor.

But as I say, I think that these recommendations are particularly valuable to us and I am going to encourage Chairman Beilenson and Vice Chairman Hyde directly and through the staff, to work with you, Mr. Chairman, in seeing if we can move legislation.

Thank you. I have no specific questions.

Chairman BOREN. Thank you very much. We are glad that you joined us and we do hope for an active pursuing of these recommendations on both sides of the Capitol and hope that before the year is out, we will see enacted into law a number of these recommendations.

We have been joined by Senator Bradley. Senator Bradley, are there any comments that you would like to make at this point, or any specific questions that you would like to address to the Panel?

Senator BRADLEY. Mr. Chairman, I just want to thank the Panel for their work, which has really been extraordinary. All of them are very busy people and it is a real act of public service to give this time.

Chairman BOREN. Thank you very much.

Let me ask just a few questions.

Going back to the question of commercial espionage that Senator Danforth raised, it is a matter of grave concern to me because I think we are going to see more and more of it. We are not talking about the theft by private companies in this country or elsewhere of private secrets. We are talking about the active involvement of foreign government intelligence services for the purpose of stealing our private commercial secrets which is certainly on the upswing. If a person with a TOP SECRET clearance working on a classified government project were to sell or give information to a representative of a foreign government intelligence service, I gather he or she would be covered under these recommendations?

Mr. EDGAR. That is correct. The key is whether or not the information involved is classified information or TOP SECRET information. If it then the case may be brought under the general framework of the espionage laws and these additions, or proposed additions, to the basic framework of espionage laws.

Chairman BOREN. Right. Not included is the situation where a person, who worked for a private company dealing with highly sensitive information, sold this commercial or technological secret that no one else in the world had except this U.S. company to a foreign intelligence service. I gather that unless the document or informa-

tion had been classified through our government process, even though it was sold and delivered to a foreign intelligence service and was a great advantage economically to another country, this would not be covered under these recommendations, is that correct?

Mr. EDGAR. That gets more complicated, Senator Boren. It would not be covered by these proposals. The basic espionage laws are drafted in terms of national defense information, not in terms of classified information. And it is possible that technical materials that are not formally classified could count as national defense information under the espionage statutes. If they did, however, it would not matter under the espionage laws that the recipient was a foreign government as against any other recipient.

Now, in the ordinary case you mention of the theft of a non-military secret, the behavior is frequently made criminal under state criminal law as an offense. As well, there have been prosecutions under the basic Federal law with respect to interstate transportation of stolen property.

Chairman BOREN. Right. I understand. Basically, theft of private property, in essence.

Mr. EDGAR. Right, that is where you end up picking it up.

Chairman BOREN. But in this case, I assume that, if it were purely private property but of great benefit to a foreign government, we might at least engage the counterintelligence resources of, say, the FBI to assist a private company that was targeted by a foreign government intelligence service. Would that be correct?

Mr. EDGAR. Yes.

Chairman BOREN. Let me ask a question concerning the financial information because I think people might easily misunderstand this. We are not talking about asking everyone who gets a security clearance to offer up access to all their financial records, let's say their tax returns and their bank account records for five years. As I understand it, this is only a targeted group within those that have security clearances? Is that correct?

Mr. EDGAR. Yes. The proposals reach the much smaller subset of individuals who have TOP SECRET clearances. We are told the number is approximately 700,000 counting both government, private sector, et cetera. Of course, that is much smaller than I believe the 4 million or so that are——

Chairman BOREN. Approximately 4 million have security clearances and about 700,000 roughly are TOP SECRET. Are you talking about encompassing all the 700,000?

Mr. EDGAR. Yes.

Chairman BOREN. In the financial records——

Mr. EDGAR. In the financial records part of it.

Chairman BOREN. By consent? In other words, the person knowingly would do this. When the person filed for application for their clearance and the position requiring a TOP SECRET clearance, they would know that they were authorizing the government to have access to this information?

Mr. EDGAR. That is right. It would be by consent.

Chairman BOREN. It would be by consent. So that if the government went in and checked certain financial records, that person

would be aware of the fact that, during this period of time, the government indeed would have the right to do so?

Mr. EDGAR. And indeed they would be told.

Chairman BOREN. They would be told that.

Now what about the polygraph situation. As I understand that, that is an even more restricted group that could be subjected to polygraphing. Not all of those with TOP SECRET clearances but a much smaller sub-group principally communicators and those with access to codes. Is that correct?

Mr. EDGAR. Correct. It is a very small sub-set of individuals with access to the especially sensitive materials of codes, coding devices.

Chairman BOREN. Do you have any idea how many people that would be? Just a rough ballpark estimate, does anyone have any idea?

Mr. EDGAR. Not on the tip of my tongue at the moment.

Admiral INMAN. I don't have, Mr. Chairman. I think I would refer to that as the John Walker/Jerry Whitworth Memorial Statute. Because indeed it is that precisely the demonstrated extraordinary damage done by those who have that kind of access.

Chairman BOREN. We are talking more in terms of maybe 25 to 30,000 as opposed to 3 or 400,000 aren't we?

Admiral INMAN. Yes, that is correct.

Chairman BOREN. I mean we are talking about a group that is relatively small.

And the kind of polygraph, I understand, that would be indicated here would be one restricted strictly to what we might call counterintelligence as opposed to lifestyle questions. They wouldn't say, Mr. Whitworth, or Mr. Walker, what X-rated movies have you been watching, or how many cocktails did you have before dinner. But it would be, have you sold secrets to a foreign power.

Mr. EDGAR. That is right. The questions are, are you a spy, have you sold secrets, et cetera. They are asked a very limited number of questions about counterespionage.

Chairman BOREN. Right. So what we are talking about here in terms of polygraph is a limited use of polygraph to a limited category of persons.

But on an unannounced basis, as I understand.

Mr. EDGAR. Right. Correct.

Mr. JACOBS. Senator Boren, it is important, going back to your previous question, to indicate that we do not recommend, even volitionally, persons who have TOP SECRET clearances making available their tax returns.

Chairman BOREN. You do not?

Mr. JACOBS. We do not. We think that is a category that the Congress has traditionally viewed as privileged and we think for good and sufficient reasons.

Chairman BOREN. So tax returns are not covered?

Mr. JACOBS. Tax returns are not covered.

Chairman BOREN. Not covered in any of the recommendations, even for the smallest sub-set?

Mr. JACOBS. No sir.

Chairman BOREN. But certain banking records would be?

Mr. JACOBS. Yes.

Admiral INMAN. That is one I lost, that was left on the cutting room floor.

Chairman BOREN. As one that has revealed his tax returns every year since 1966, I think I mainly am seeking sympathy from my constituents.

[General Laughter.]

Chairman BOREN. Senator Metzenbaum?

Senator METZENBAUM. I am a little bit concerned about making access to travel and financial records a condition for TOP SECRET clearances. I think you said there would be about 700,000 people whose records would be available. Now, when you say making them available to the government, the government is people. We had an FBI Director, some years ago, who had access to much information and really created more problems than he should have. That was one man. And I am concerned that I don't know how many thousands of people will have access to these travel and financial records. I am concerned about the abuse to which they might put that information, and I am wondering whether, in solving one problem, we aren't creating a greater problem.

Chairman BOREN. Any members like to comment on that? Members of the Panel?

Mr. EDGAR. Well, I think we have tried to limit that. It is a concern. But it is not anyone in government who can have access to these records. The authorization is limited to those who are in the business of reviewing these things for authorized government security purposes.

The problem that is——

Senator METZENBAUM. Give me your guesstimate as to how many people that would be.

Mr. EDGAR. How many in fact would do it on on a regular basis?

Senator METZENBAUM. No. How many people would have access?

Mr. EDGAR. My belief is that the number would be one thousand or down.

Senator METZENBAUM. Thousand or down?

Mr. EDGAR. Or down. A couple of hundred. I mean if you go through all of the agencies of the government and everybody up and down the charts, superior to the person actually doing the investigation, that would be my rough guess.

Senator METZENBAUM. Would you not have some concerns about how that information could be misused by one or more of those thousand people?

Mr. EDGAR. One must always have such concern. However the law provides—now provides, against the misuse of such information for inappropriate purposes. So I don't know that you are dramatically increasing the likelihood of such misuse. Apparently the problem——

Senator METZENBAUM. But you are providing more information. You are providing financial data. You are providing travel data. Let's assume that Mr. X, or Miss X, who is one of those thousand people, finds that some one or more people are involved in extramarital affairs, traveled in order to get an abortion, or whatever the case may be—information that is very personal and that the individual would not want to have made known.

Mr. EDGAR. Senator Metzenbaum, travel records are not protected by present law. Anyone in the government can go—or anyone anywhere, you can go, I can go, a private citizen can go and ask for the records. There is no protection against the request that a person maintaining travel records tell you what those travel records disclose.

So if the—I mean, as it now stands, as I believe the situation is, all two hundred million Americans can make these requests.

Senator METZENBAUM. How about the financial—

Mr. EDGAR. As for the financial records, the limitation on authorized disclosure is now three months. As I say for this category of people, the present authority to permit disclosure which is exercised by the Government in the course of preliminary security investigations, is extended. So the same records that are accessible presently would stay accessible longer. The individual as a condition for seeking and getting such a TOP SECRET clearance, would extend the period of time that records that are already accessible would remain accessible.

So in that sense, any time you increase the time, you are increasing the amount of information and the number of people potentially over time, who might come in contact with it. But it is——

Chairman BOREN. Excuse me, let me ask Mr. Cutler to comment on this matter. We already know that there is a lot of access to information in personal files, let's say at the FBI and elsewhere. We would be adding, to some degree, to the amount of information that would be available. I think Senator Metzenbaum wants to know what protections are there against the unauthorized disclosure of that kind of information?

Mr. CUTLER. Well, we are all very sensitive to the point that Senator Metzenbaum has raised. I think as a factual matter, the risks of disclosure from the investigators has been relatively low. It is still a serious problem and undoubtedly there have been leaks from the FBI, there have been leaks or at least charges of leaks from the Senate staff among others on confirmation hearings. But unless you are prepared to give up the whole notion of a security check, an investigation before someone is hired, you have to trust someone to acquire information. This information, the credit information and the travel information is no different in character than what is already in the personnel questionnaire forms that people are being asked to fill out. And as Mr. Edgar said, in the case of an investigation of someone applying for a TOP SECRET clearance, it is quite routine to check credit records with the consent of that person. It is limited to three months today.

Let us assume that someone has been checked and approved and he then comes under suspicion. You want to go back and look at his credit records without alerting him by asking him to sign another consent. So you get the consent in advance for the period of his employment. That was the intent of this legislation.

Senator METZENBAUM. You would have access to those financial records over the entire period of his employment?

Mr. CUTLER. That is the idea, yes. And I think for some brief period thereafter.

Senator METZENBAUM. And are you not concerned that there indeed could be considerable misuse and, as happens so often in

Washington, leaks that employee X was in this particular deal, or that deal—that may be a perfectly legitimate deal, but might be embarrassing in the hands of some' newspaper writer?

Admiral INMAN. Senator Metzenbaum, those of us who are not public figures, have not been subjected to that. It is only when we get to the stage of being confirmed here or get publicity where someone decides it is news worthy to misuse.

But a point for you that you can look at. You have imposed in other legislation minimization requirements that limit the access to information. I don't think that that would be a real problem in this one to simply require the Executive branch in their implementation to establish minimization rules that effectively limit the number of people who would review and who would have the prospect of abusing.

Senator METZENBAUM. I want to go to a different area.

Chairman BOREN. Go ahead.

Senator METZENBAUM. With respect to proposal number three, retaining TOP SECRET information, I am concerned as to when would a person be judged to have retained a document illegally. What if a whistle-blower put a document in his car, drives over here and gives it to the Committee? Would that be illegal?

Mr. EDGAR. I don't think so; no. He would not be retaining it if he drives over here and gives it to the Congress. It was certainly not our intention to make that illegal, and if we stumbled, we stumbled. But our ambition was not to cover that.

Senator METZENBAUM. If he took it home, put it under his pillow, and brought it to us the next morning, would he be violating the law?

Mr. EDGAR. No.

Senator METZENBAUM. Pretty sure?

Mr. EDGAR. Well, it's our—I mean, certainly the legislative history can be made to make clear the concept we focus on is the concept of retention. And the ambition is to distinguish between the person who—first of all, people shouldn't take TOP SECRET documents home. But even for the person who does, the behavior becomes criminal under this proposal only when the person retains the document. And the word retains is intended to suggest some appreciable period of time and not simply overnight, and certainly not overnight as part of delivering it to this Committee.

Admiral INMAN. Senator Metzenbaum, what we are trying to deal with here is the specific instance of an individual who took TOP SECRET documents, put them in a safe deposit box, didn't deliver——

Senator METZENBAUM. A what?

Admiral INMAN. Put them in a safe deposit box with the clear intent of profiting from selling them after he finished his employment. And that is what we are trying to deal with.

Senator METZENBAUM. I understand the thrust of what you are attempting to achieve. I just want to be certain that in attempting to reach that objective, you don't at the same time write it so broadly that it unfairly reaches the whistle-blower, or maybe that individual who takes the document home because he is working and writing his memoirs and has no intention of violating any secrets or anything of the kind, but is merely refreshing his or her

memory. I just want to be sure we don't wind up making criminals out of law-abiding citizens who are doing a job for the government.

Senator COHEN. Would you yield on this?

Senator METZENBAUM. Sure.

Senator COHEN. Is it specifically the intent of the Panel to limit those situations to the unlawful retention or removal of documents for the purpose of sale or profit in the future? Because I could envision, for example, someone who might be out at the Agency or NSA who has typed a TOP SECRET memo to his superior and it is labeled, TOP SECRET, and he wants to retain a copy for himself in the event that sometime in the future he is accused of not having duly reported something. Now he has a copy at home for his own, quote, "protection," to say, "No, I fully communicated the following transfer of weapons to Iran"—by way of example—"and here is the memo to prove it."

Now, is that the kind of situation that would be excluded under the Panel's recommendation? It may be a violation of something else, but that is not your intent. It is really not to have this document for purposes of sale or profit.

Admiral INMAN. You could add that—to establish the intent to profit.

Mr. EDGAR. Well, we didn't discuss it quite this way. Some of the cases include cases where people took substantial numbers of documents home, probably without the intention to sell them at the time, but thinking that this is a safety cache, and that sometime down the road, who knows, five or ten years from now, if I ever need them, these documents may be useful to me for any number of reasons. Now, it was our intent to pick up that case, and to pick up that case you cannot require the prosecutor to prove that the individual has an intention to sell the documents from the start, even though the pattern that we fear is ten years down the line, someone would sell it.

In the case you pose, Senator Cohen, it's not clear to me that the document is itself a TOP SECRET document, the memoir. I mean, his—this only applies to things that have in fact been classified TOP SECRET. So if it were not, I would think that might be a way out for the individual.

Senator COHEN. Senator Boren and I communicate on a daily basis by letter to the Agency, and it is stamped TOP SECRET.

Chairman BOREN. Nearly always.

Mr. EDGAR. Then that is an issue to consider in the on-going legislative process, whether that kind of retained personal record should or should not be brought under or excluded from this provision.

Chairman BOREN. For the benefit of the Executive Branch, I will say that Senator Cohen and I have the policy to retain a copy in the Committee files in the vault as a record and to verify our notification of the Executive Branch on matters.

Senator Metzenbaum?

Senator METZENBAUM. You fellows send notes to each other like that?

[General Laughter.]

Senator METZENBAUM. I don't think I have any further questions. I think there is some fine tuning to do, but I think that your Panel

has done yeoman's work. I think you have opened up some avenues that we should explore. I would strongly urge upon you that if we are all to be successful in achieving that which you are attempting to achieve, we are going to need your help as well in prevailing upon the Administration—I know some of you have relations with them—to move forward on this whole question of overclassification which, in my opinion, is a subject that has been kicked around too long. We have some responsibilities to ensure such a broad approach to improving U.S. security procedures. I would hope that you would direct some of your efforts along the same line.

I have nothing further, Mr. Chairman.

Chairman BOREN. Thank you, very much.

Senator Cohen, additional questions?

Senator COHEN. Yes. I would like to go back to the issue of sale, because one of your proposals would criminalize the sale of TOP SECRET documents to foreign governments, but that doesn't appear to cover transfers where there is no consideration. Is that an oversight or a policy decision arrived at by the panel? Assuming there is no consideration, should it not be an offense to transfer documents labeled TOP SECRET to any foreign official or government?

Mr. EDGAR. It was a policy choice, and the thought behind it was that this provision removes from the government the burden of proving that the document really contained important defense information. The person who simply gives such a document to a foreign agent violates the regular espionage statutes and can be prosecuted.

Senator COHEN. But they have to show there in that case——

Mr. EDGAR. Right. The government there has to prove that the TOP SECRET information—that the information genuinely was defense related. Our thought was that there are some cases in which people might have a document and think that it is something that a foreign government should know, be motivated that way, and turn it over, thinking that it could do no harm, that kind of thing. And that there is a clear line between bargains and gifts. And that the person who makes a deal basically deserves no sympathy whatever.

Senator COHEN. Let me give you an example. Let's assume that a top State Department official who is concerned about arms control, has a document in his or her possession stamped TOP SECRET, and goes to a counterpart and provides that document, which has to do with bargaining positions, strategies on the part of the United States—a host of issues that would be of importance to the other country in arriving at an arms control position. That would not be covered under this particular provision. Under this recommended——

Mr. EDGAR. Under this provision, it would not.

Senator COHEN. I think that is an issue that we ought to at least take into account, the policy as to whether you must have a financial interest involved. You may have something that is done initially out of an ideological reason which eventually becomes a pecuniary one down the line, and the initial transfers would not be covered under this and we would have to go under the much more difficult prosecutorial standard.

Mr. JACOBS. We'll review that issue with that specific point in mind.

Senator COHEN. With respect to consumer credit information, is there anything that you would recommend by way of forcing the Agency who's doing the check into the consumer credit information as to reviewing the reliability of that information? We've had examples in the field of computer matching, to give you some illustration, in which we have computer matches done of individual's financial records with that of an application for an SBA loan, and we found programs terminated based upon the information that had been found in those computer matches, only to discover later on that the information was erroneous. Should there be some kind of protection here about the verification of the consumer credit information that is disclosed?

Mr. EDGAR. Our thought was—and again, this is another area where more thought may be desirable—but this proposal authorizes the securing of this consumer information in the course of an on-going investigation. And our understanding is that in ordinary course, that information, when it came—when it became available, would lead people to do in fact that further checking because the information is the trigger in an on-going investigation. It does not control a decision whether to make a mortgage or something like that.

Senator COHEN. Another final point if I can, Mr. Chairman. When a search is made through someone's financial records, is the individual entitled to notification that such a search has been conducted?

Mr. EDGAR. Yes.

Senator COHEN. OK.

Mr. EDGAR. Well, pursuant to the Bank Privacy Act, if that's the reference.

Chairman BOREN. Well, I guess I don't understand that. Let's say my bank records were going to be examined, and I gave consent at the time of my employment for the period of my employment plus what, five additional years——

Mr. EDGAR. Five years.

Chairman BOREN [continuing]. Thereafter. Now it is found that all of a sudden I deposited an additional million dollars, and I hadn't hit oil—well, that's not a good example any more—but in the good ole' days that used to be the case.

[General Laughter.]

Chairman BOREN. And you already have consent to go and look in my bank records.

Mr. EDGAR. Right.

Chairman BOREN. But you have to come and tell me we've looked at your bank records?

Mr. EDGAR. No. But there are two categories. For the broad category, the person who is subject—under 700,000, that category—that individual could ask if his bank records had been examined. He can under present law and can under our proposed amendment of the law.

Chairman BOREN. He can ask.

Mr. EDGAR. He can ask.

Chairman BOREN. But it would not be volunteered.

Mr. EDGAR. It is not volunteered under present law either. But it is something you can get, if you want to ask. Has the government come and looked, you can ask, and present law provides that you can get that information, and this proposal does not change the law in that respect.

Senator COHEN. But let me extend that now. Under the FISA statute, now you want to propose to extend that to include physical searches of a person's residence or place of business or whatever, right?

Mr. EDGAR. Right.

Senator COHEN. Now, under that particular proposal, would an individual who comes back and notices that something is out of place and says I would like to know whether or not an application has been made to a Federal Court to search my premises or my home, is that something that was considered and rejected or something that was not considered?

Mr. EDGAR. We tried—our thinking there was to treat physical searches just as present electronic surveillance is treated. And when one is dealing in the national security, the certification of a—that someone—there is reason to believe that someone is an agent of a foreign power, there is no automatic notification. And so our proposals here are simply to track the present authority with respect to electronic communications.

Senator COHEN. There's no notification, but is there any requirement that that individual would then have a right to go to the Court to find out whether he is the subject of a search by domestic officials?

Mr. EDGAR. I would really want to check and be sure, but I think the answer is no.

Chairman BOREN. That kind of search of a premises would, again, only apply to this narrowly constrained group that we are talking about.

Mr. EDGAR. Oh, yes, very definitely.

Chairman BOREN. Would consent have to be given for this as well as consent to access of records or not?

Mr. EDGAR. No, no, that's under FISA. That's a different part of the recommendation.

Chairman BOREN. OK. I understand that about electronic——

Admiral INMAN. But the Special Court would have had to consider the affidavit on which the application was based, and in fact——

Chairman BOREN. So this has nothing to do with the clearance procedure of a consent like the financial records?

Mr. EDGAR. That's right.

Chairman BOREN. This is expanding existing law and it would require a court action to allow an electronic surveillance, without the person being notified, to include physical searches of a residence.

Mr. EDGAR. Let me reemphasize the point, Senator Boren, that that has nothing to do with these problems of government employment generally. I mean, it is restricted to people for whom there is reason to believe that they are agents of foreign powers.

Chairman BOREN. And that must be established by a court.

Mr. EDGAR. Right. And that is—they are commonly not government employees. I mean——

Chairman BOREN. So there would be judicial oversight over that matter.

Mr. EDGAR. That's correct.

Chairman BOREN. Is that true also of telephone subscriber information? Would you go into that recommendation again?

Mr. EDGAR. Well, the recommendation is to amend the 1986 statute, to clarify, to make plain that when there is authorized telephone surveillance of foreign powers or agents of foreign powers, and they call a telephone number——

Chairman BOREN. Authorized by a court.

Mr. EDGAR. Authorized by a court. And they call a telephone number, which telephone number is unlisted, the proposal would permit the agency to find out the name of the person who had the telephone listing. But nothing else. In other words, it would not give any authority to check the toll records of the person whom the foreign agent called. All it would permit the agency to find out was whose number is 737, or whatever.

Chairman BOREN. Nor would it allow for a tap on that number at that point.

Mr. EDGAR. No.

Chairman BOREN. Obviously, if they had a court order and they were electronically eavesdropping, they would have heard the conversation.

Mr. EDGAR. Correct.

Chairman BOREN. That particular conversation. But then you wouldn't have the right to then automatically electronically eavesdrop on the person who had been called, let's say, by the Soviet embassy or something.

Mr. EDGAR. Not only would you not automatically have the right, you wouldn't have the right unless you could independently meet whatever criteria are necessary in order to authorize a telephone tap.

Senator COHEN. Just one final question with respect to polygraphs. Your proposal is limited to government communicators specifically. My understanding is that communicators at CIA are polygraphed, and I am told that communicators at DOD could be polygraphed. And the question I have is are we talking primarily about communications at the State Department?

Admiral INMAN. Not primarily, but they would indeed be included. At this point in time really the only two agencies that specifically focus on them are NSA and CIA.

Senator COHEN. The Department of Defense has recognized some of the limitations involved in polygraphs; in other words, they are not infallible. Should there be some measure of protection here to avoid an adverse action taken towards an individual based solely upon the reaction to a polygraph, unless the Secretary himself or herself were to specifically authorize that? Is that something that we should consider here as well, that there should be no adverse action towards an individual based solely on a polygraph test?

Mr. JACOBS. Our belief is that the polygraph and the polygraph results are not an end in themselves and not the sole determinant of whether a person should retain a security clearance, but rather part of a pattern that would cause an adjudicating authority to make a decision.

Senator COHEN. In other words, the Panel would have no objection to the Committee either writing it into the statute itself or an accompanying report to indicate that caution should be exercised here; that simply showing deception what is described as deception on a polygraph—or not meeting the standards one would expect—that that in itself would not produce adverse consequences without the Secretary or the head of the department specifically authorizing it.

Mr. CHRISTOPHER. Senator, as one who is concerned about polygraphs, let me say two things. First, I personally would welcome the kind of provision that you suggest as a safeguard. The polygraph, at least as it has been explained to the Committee—and there was great effort to explain it fully to the Committee—is not an end in itself, but simply an important tool. Second, I would say that I was persuaded on this particular recommendation by the point that individuals in other agencies—the CIA and NSA—performing substantially the same functions as the communicators in the State Department and the Department of Defense, were subject to polygraphs. This is a very high risk area, and so for that narrow group of individuals, there seems to be a special basis for the use of polygraphs as a part of a technique of detection. But as to this group, I would welcome personally the safeguard that you mentioned.

Senator COHEN. And just one final point.

Senator Metzenbaum is no longer here now, but he raised the issue of travel, and I think that if we took the time to go down through this chart, we would find that virtually all of the cases involved travel to a foreign country, all of them seemed to have a crossroads, I believe in Vienna, and——

Admiral INMAN. Vienna or Mexico City.

Senator COHEN. Vienna or Mexico City, and that one can assume that given the changes in Europe, the locus is likely to change to various other desirable spots in Europe; perhaps Canada and Mexico or maybe even the United States. As we start to have a more open policy, there will probably be less inhibition on the part of a foreign intelligence service to meeting with a U.S. official or government employee, even here at home. With more people coming in, having greater access, it seems that perhaps foreign travel will not be as necessary as it has been in the past.

Mr. CUTLER. I think, Senator Cohen, that foreign travel records, or access to those records, is one of the least intrusive of all of the forms of investigation. When you travel, it is usually on a commercial airliner, it's in public, there's a ticket with your name on it. It isn't a clandestine activity. And it is hard to see any privacy reason why if you take a personal trip in that way, the record of the trip should be immune at least from government investigators. So it is not much of an intrusion compared to, say, the bank records or to other things like that.

Senator COHEN. Unless you have Senator Metzenbaum's hypotheticals of assignations or abortions. Then it is a bit more intrusive.

Mr. CUTLER. Well, your personnel questionnaire will require you to state every place you have traveled for the last 30 years.

Admiral INMAN. I guess if every state has a law, you will then——

Mr. CUTLER. That is much more intrusive and it is impossible for someone like me to fill out. [General Laughter.]

Chairman BOREN. We won't pursue that line of questioning any further. Let me note on the chart—and again I think the Panel has certainly done a great service for calling this to our attention—if you look at motivation, over and over and over again money is mentioned. The money is a factor. And yet it is quite obvious that through the classification process, the reclassification process and trying to monitor the behavior patterns of people with sensitive information, we have put a lot more emphasis upon other items, even lifestyle, the possibilities of blackmail, a lot of other areas of a person's behavior, than we have financial records. Really once this person has passed the three month period, we know less about them than a bank might know if they were applying for an auto loan in terms of what their financial behavior is.

So I think this is extremely important, as we go into a period of time where I would guess that financial motivation will become even more important. And when you can say to yourself, oh, I am not really selling out the national security of my country, I am not really selling out to someone who might use this as a military secret to come and take over our country or invade or launch a surprise nuclear attack. You can say, oh well, we all have such friendly relations with other countries. Now, peace has broken out. I can justify to myself, because I need the money, to sell these items of information which might have some other application other than strictly military or even a military application to a country that now has a more benign image than it has in the past. I would guess that the financial motivation will become even more dangerous in that kind of world and even more likely for people to talk themselves into this kind of behavior based upon their own greed or their own financial stress.

So I think you have provided a great service in calling this to our attention. It has really been a blind spot in many respects in the very area where the threat is now greatest.

Senator COHEN. Might I add, I think this is the first time that such an analysis or matrix has been put together by anyone to analyze the commonality of characteristics here, from the personnel, their jobs, their access to information, travel, and their motivation. I don't think that has been done before and I think it does show a fairly consistent pattern which is very, very helpful for us.

Chairman BOREN. Before we close these proceedings, I want to pay special tribute also to the members of our staff, many of whom are seated up behind us. George Tenet, the Majority Staff Director and Jim Dykstra, the Minority Staff Director. Also our General Counsel, Britt Snider, who has worked long and hard with members of the panel. There are other members of the Committee staff as well who provided a lot of assistance to this group to whom we want to express our appreciation. As the members of the Panel know, this has been a bipartisan panel. As they have discovered in working with our staff, it is a bipartisan staff. We try to work in that spirit. And I think that the Panel is to be commended for coming forward with consensus recommendations that really span a broad philosophical spectrum, a bipartisan spectrum of the Panel

itself, and we are very, very appreciative of the work that has been done.

We will share these—Senator Metzenbaum and others overlap with us on the Judiciary Committee recommendations and transmit them to the Judiciary Committee. I have already mentioned them to Senator Biden who has had, of course, service on this Committee. Senator Leahy chairs the appropriate Subcommittee and really had planned to be here. He is a previous Vice Chairman of this Committee. They are very interested in these recommendations which I am very optimistic will be vigorously pursued as part of the legislative agenda this year.

I am going to have to exit very quickly—I apologize to go chair a meeting that may be far more dangerous than the area of espionage, and that is campaign finance reform negotiations. But please accept my appreciation and that of Senator Cohen and all the members of the Committee for the outstanding work that you have done.

We have to tell you we are not going to let you off the hook yet. There are obviously still some other items that we want you to look at for us. And as we go through the legislative process, we also want to be able to return to you to bounce some ideas, refinements perhaps, for a fine tuning of these recommendations. We would value your input as we go forward in the legislative process with these recommendations.

Thank you all, very, very much.

We'll stand in recess.

[Whereupon, at 4:11 pm., the Committee stood in recess.]

HEARING ON S. 2726 TO IMPROVE U.S. COUNTERINTELLIGENCE MEASURES

THURSDAY, JULY 12, 1990

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

The Select Committee met, pursuant to notice, at 2:09 p.m., in room SH-216, Hart Senate Office Building, the Honorable David L. Boren, (chairman of the committee), presiding.

Present: Senators Boren, Metzenbaum, Cohen and Specter.

Also present: George Tenet, Staff Director; James Dykstra, Minority Staff Director; Britt Snider, Chief Counsel; Kathleen McGhee, Chief Clerk; and Keith Hall, David Holliday, Fred Ward, John Elliff, James Wolfe, Andre Pearson, James Currie, Edward Levine, Connell Sullivan, Larry Kettlewell, Blythe Thomas, Chris Straub, Chris Mellon, Charles Battaglia, Marvin Ott, Sarah Holmes, Mary Sturtevant, Regina Genton and Rosemarie Nahrgang, Staff Members.

PROCEEDINGS

Chairman BOREN. We have other Members of the Committee that are expected to attend, but we're going to go ahead and proceed because all our witnesses are already present today.

The Committee convenes today to receive testimony concerning a bill the Vice Chairman and I introduced on June 13, the Counterintelligence Improvements Act of 1990. We are pleased that a number of the Members of the Committee are cosponsors of this proposal, as well as the distinguished Chairman and Ranking Minority Member of the Judiciary Committee, Senators Biden and Thurmond.

The bill under consideration, S. 2726, embodies the recommendations made to the Committee on May 23 by a distinguished panel of private citizens, chaired by Eli Jacobs, a New York businessman with extensive participation on panels in the defense and foreign policy areas. The Panel also included former NSA Director and Deputy Director of Central Intelligence, Bobby Inman; former Deputy Secretary of State and former Deputy Attorney General Warren Christopher; former Counsel to President Carter, Lloyd Cutler; former Counsel to President Reagan, A.B. Culvahouse; former Director of Central Intelligence, Richard Helms; former Ambassador to the Organization of American States, Sol Linowitz; former Ambassador and State Department official, Seymour Weiss; and Columbia University of Law Professor Harold Edgar.

Senator Cohen and I commissioned this group last fall to review the Government's capabilities to deal with the problem of espionage. Working without compensation and on their own initiative, they took as their first task a review of the statutory framework which governs the investigation and prosecution of espionage.

In 6 months of meetings with Executive branch officials and briefings by the Intelligence Community, they focused upon the most serious espionage cases of the last 15 years. The Panel then arrived, with considerable deliberation, at 13 separate recommendations which they presented to the Committee several weeks ago.

Indeed, many proposals were rejected by the Panel because they failed to strike the correct balance between actions required to effectively deter espionage and the rights of Americans. As Ambassador Sol Linowitz stated in his appearance before the Committee, "It's clear enough that every time you try to work in the security field, you have got to be careful that you don't pass over the line into infringement on rights which people have been guaranteed. My own view is that the proposals as they now have been presented to you will not raise any questions of significance with respect to the abuse or infringement of either constitutional rights or civil liberties." Those were the words of Ambassador Linowitz that I just quoted.

The Panel emphasized at that time that their proposals could be improved upon. They also made the point that their proposals by no means covered the waterfront in this area and there are other areas and concerns still to be addressed.

Following the hearing, Senator Cohen and I decided it was important that we start with a bill which embodied the Panel's recommendations without substantial change, recognizing that such change may well grow out of the legislative process and out of hearings as we are having today. So, while we certainly are in accord with the objective of these proposals, we keep an open mind as to how they might be best accomplished and to refinements and changes that might be made to these recommendations.

Let me re-emphasize, as Senator Cohen and I have both said, we want to be particularly mindful that these proposals could cause concern for civil liberties. While I know that the Panel itself was acutely sensitive in this regard, we want to accommodate any such lingering concerns wherever possible. So, in this regard, we welcome today the testimony of Mort Halperin representing the American Civil Liberties Union.

Let me also emphasize that we recognize that many of these proposals fall within the jurisdiction of other Committees. We intend to seek their views before taking action ourselves on these proposals.

The first proposal, in section 2 of the bill, would establish by statute uniform minimum requirements for everyone granted a TOP SECRET security clearance. At the present time, there are no uniform procedures and they vary from agency to agency.

Section 3 of the bill is intended to strengthen the protection of cryptographic information which basically means codes and coding machines. The key element of the section would require that all Government communicators, in whatever agency they might be employed, be subject to the possibility of a very limited counterin-

telligence scope polygraph examination during the period of their employment in communications.

Section 4 would give the Director of the National Security Agency discretionary authority to provide certain assistance to employees for up to 5 years after they leave NSA to help them cope with personal or economic problems which we've learned often lead to people being tempted into espionage.

Section 5 would amend the right to Financial Privacy Act to permit persons with TOP SECRET clearances to provide their consent to the appropriate Government authorities to obtain access to certain of their financial records. It strengthens our ability to have financial background information about people during the course of their employment.

Section 6 would make it a crime to possess espionage devices where the intent is to violate the espionage statutes.

Section 7 would make it a crime to sell to a person representing a foreign power documents or materials that are marked or otherwise identified as TOP SECRET. Without the Government having to prove as an element of the offense that the classification marking had been properly applied.

Section 8 of the bill would add a new provision to that part of the Criminal Code which deals with the responsibilities of Government employees. It would create a new misdemeanor offense for any Government employee who knowingly removes TOP SECRET documents without authority and retains them at unauthorized locations, so-called stockpiling of classified information with the intent to possibly later misuse that information.

Section 9 would extend an existing statute which provides for the forfeiture of profits associated with violations of 18 U.S.C. 794, the so-called Son of Sam law, to other types of espionage convictions.

Section 10 would permit the Government to deny retirement pay to U.S. retirees, convicted of espionage in foreign courts which involve U.S. national defense information, from the Civil Service Retirement System, the Federal Employees Retirement System, the CIA Retirement System or any other Federal retirement system.

Section 11 would amend the Fair Credit Reporting Act to permit the FBI to obtain consumer credit reports on persons who are certified by the Director of the FBI as suspected of being agents of foreign powers.

Section 12 of the bill would amend the Electronic Communications Privacy Act of 1986 to permit the FBI to obtain limited identifying information about persons with unlisted telephone numbers who are called by foreign powers or agents of foreign powers.

Section 13 of the bill would amend the existing statute which provides discretionary authority to the Attorney General to pay rewards for information concerning terrorism, to permit him to provide similar rewards for information leading to an arrest or conviction for espionage or the prevention of espionage.

Section 14 would extend the court order procedure for electronic surveillances, established by the Foreign Intelligence Surveillance Act of 1978, to physical searches done for national security purposes which are now undertaken without a court order under a claim of inherent presidential authority.

As I said at the time the Panel appeared before us, I believe they performed an extraordinary public service in developing these proposals for us. I congratulate them and want to thank them once again for their fine effort.

We are pleased to have with us this afternoon three witnesses, each of whom will testify separately and provide us with his or her views on this bill. We will hear first from Mary Lawton, Counsel for Intelligence Policy at the Department of Justice. After Mary Lawton, we will hear from the Director of the Washington Office of the American Civil Liberties Union, Morton Halperin, as I have mentioned. And our final witness will be Kenneth E. deGraffenreid, who handled counterintelligence matters as a former member of the National Security Council staff under President Reagan, and who continues to write on such matters in the context of his association with the National Strategy Information Center in Washington.

I welcome all of our witnesses. We appreciate your taking the time to be with us today and share your very special expertise in this area with us. We are seeking constructive suggestions as to how we can improve the proposals that have been made and we are certainly open to any suggestions which you might make to us.

I'd like to ask, before we begin, Senator Cohen if you have any additional comments that you would like to make?

Senator COHEN. Just a few comments, Mr. Chairman.

For the benefit of the public, this is one of the few times that the Intelligence Committee has conducted its business in a public forum. I regret to say that we ordinarily have a much greater attendance in private than we do here today in public.

Attendance may even be diminished further, Mr. Chairman, because we have a unique situation in which the Senate Armed Services Committee is currently conducting its markup of the Defense Authorization Bill, which is of great importance to this Committee. And Senator Nunn intends to finish the markup by midnight tonight. So immediately after I make a few comments, I intend to depart this Chamber and head over to the Armed Services Committee to try and conclude the business there.

So the timing is not exactly propitious, on the one hand, and being the two-handed economists that we all are, on the other hand, it may be precisely that. Because I know that since the Berlin Wall is down, Marcus Wolfe, head of the East German intelligence is in Moscow, maybe on his way back now according to latest reports; and the Cold War is over; many are asking, "Why do we need this particular piece of legislation?"

First of all, I want to point out, as the Chairman has as well, that we have to keep an open mind on this legislation. We ought to proceed with due caution in terms of crafting any improvements in this measure. Our minds are not closed on this subject.

We think that the Jacobs Panel has really done an enormous public service. And because of the makeup and the composition of that particular Panel, I think, that we have taken into account not only our national security needs, but also legitimate concerns about the right to privacy.

But we are open to any recommended changes that would improve this legislation, not only to make it more consistent with our

needs for protection, but also to protect the needs of the citizens who would be affected.

I think we also have to move, Mr. Chairman, rather expeditiously. We shouldn't squander the opportunity that has been presented to us by the Jacobs Panel to act constructively in this area, because the evidence of spying continues to mount all about us.

Since the Jacobs Panel made its recommendations several weeks ago, we've had a former Army Sergeant First Class, Clyde Lee Conrad, convicted and sentenced to life imprisonment by a German court for having spied for the Hungarian and Czech intelligence services for more than a decade. The trial judge said that Conrad had, "Endangered the entire defense capability of the West." And the court found that his motivation was quite simple and clear, it was pure greed. He had been paid something in the neighborhood of $1.2 million.

Several days later, another former Army Sergeant, Roderick James Ramsay, was arrested by the FBI in Tampa, Florida for his part in the Conrad espionage scheme. Ramsay is charged with passing classified defense information to the Hungarians while serving as a classified document custodian for the 8th Infantry Division in Germany. And the FBI affidavit indicated that Ramsay was paid $20,000 by Conrad for his services.

So it was clear that Conrad wasn't quite as generous to his courier as the Czechs and the Hungarians were to Conrad.

On June 15, still another serviceman, this time from the Air Force, pled guilty in Dallas to a charge of attempting to sell classified information to the Soviet Union and was sentenced to 10 years in prison without parole. And on that very same day, an engineer in Los Angeles was arrested for illegally attempting to sell information regarding an SDI project to people he thought were brokers for a South African firm. Luckily, they happened to be from the FBI instead.

So, in the space of just 6 weeks since the Jacobs Panel reported to us and appeared before the Committee, we've had four cases where people were either arrested or convicted of espionage. And, as I indicated, one of them, the Conrad case, appears to have been extraordinarily damaging.

So even though the Cold War is over, we are faced with the prospect that espionage may be forever. And we need only to go back to Biblical days, when the first recorded attempts at spying, espionage, occurred to find that the reason for it is quite clear. Even though we have a reduction of tensions, the fact of the matter is that information confers power. The ability to know of another's capabilities or indeed more importantly perhaps, intent as well, can be the very basis for survival. So knowledge is power. And that is not going to diminish in the future, no matter what the nature of our relationship might be with any given country. There will still be an effort to attempt to gather information about our capabilities and our intentions.

I think it is critically important that if there are steps that Congress might take to help cope with this situation, as the Jacobs Panel suggests that there are, they ought to pursue them. And I mention that it is particularly propitious at this particular moment because I am going to be spending the next 6 to 9 hours in the

Senate Armed Services Committee dealing with classified projects, classified programs that we are spending millions, indeed billions of dollars of the taxpayers' money to construct and to deploy. It would be ironic indeed if we said that, just because tensions have been reduced, therefore we have no need for any legislation which might tighten the laws that are currently on the books in an effort to diminish the size of the net that these traitors have been able to slip through.

I don't think anyone seriously thinks that espionage is going to be eliminated entirely. The purpose of the legislation is threefold.

To deter individuals from engaging in espionage.

To detect them more easily if they are not deterred.

And to convict them more easily if in fact they are detected.

Those are the three main goals of the legislation. I think these objectives remain valid today and perhaps even more so than ever. We ought to take advantage of the opportunity presented to us by the Jacobs Panel, Mr. Chairman, and make what I hope and believe will be a constructive contribution toward dealing with this very difficult problem.

Chairman BOREN. Well, thank you very much, Senator Cohen.

I will place two documents into the record without objection. These two items have been provided to the Committee. The first is a letter dated June 27, 1990, from the FBI Director William Sessions relating to the two FBI provisions contained in S. 2726. The second is a prepared statement by Theodore S. Wilkinson, President of the American Foreign Service Association regarding S. 2726.

U.S. DEPARTMENT OF JUSTICE,
FEDERAL BUREAU OF INVESTIGATION,
WASHINGTON, DC 20535,
June 27, 1990.

HON. DAVID L. BOREN,
Chairman,
Select Committee on Intelligence,
U.S. Senate,
Washington, DC.

DEAR MR. CHAIRMAN: Thank you for your letter of June 13 enclosing a copy of S. 2726, the Counterintelligence Improvements Act of 1990. I commend you and the Committee for empaneling the Jacobs group and for the important work done over the last several months in reviewing the laws and policies affecting the counterespionage efforts of the United States. The collective expertise of the participants is clearly reflected in their product, and I applaud your swift introduction of a bill to implement the recommendations.

In regard to the legislation, the FBI supports the position of the Administration, which I understand will be presented before the Committee at a public hearing in the near future. In the areas of access to consumer credit reports and non-published telephone number subscribers, I offer the following additional comments.

An amendment to the Consumer Credit Protection Act to permit the FBI to obtain consumer credit reports on persons believed to be agents of foreign powers has been requested by the Administration as part of the Intelligence Authorization Act. While the Right to Financial Privacy Act allows counterintelligence investigators access to bank records of any individual who is the target of an investigation, the Consumer Credit Protection Act does not allow similar access to records which would serve to identify the banks being utilized by these same individuals. This impedes our counterintelligence investigations and severely lessens the investigative value of the current method of accessing financial records. Accordingly, I strongly recommend the provision which you have included in S. 2726, and which is comparable to that found in the Right to Financial Privacy Act. It would permit access to consumer records under the same controlled circumstances and be of great assistance to the FBI.

The Administration also supports an amendment to the Electronic Communications Privacy Act (ECPA). This amendment would resolve a problem not anticipated at the time ECPA was passed. Currently, the ECPA permits the FBI to obtain toll record and subscriber information concerning subjects of foreign counterintelligence investigations, based upon the specific certification detailed in the ECPA. However, if the toll records obtained under this provision, or other information obtained from pen registers or trap and trace devices, show calls to or from an unlisted telephone number, the FBI is currently unable to obtain from the telephone companies information identifying the subscriber. This is so because the FBI cannot certify, as required by the ECPA, that the subscriber is a target of investigation. Identification is the threshold the FBI must cross to determine whether further investigation of the individual is warranted or would obviously be irrelevant. It is important to stress that the information sought is identification information only. Toll records would continue not to be obtainable unless and until the individual can be appropriately certified to be the target of an investigation. Subscriber identification would not be available unless there was specific information that the subscriber had been in contact with a counterintelligence target. The intrusion involved would be minimal. The passage of this proposal is critical to the FBI's counterintelligence and counterterrorism programs and I would appreciate having it included in the Authorization Act.

John E. Collingwood, Inspector in Charge, Congressional Affairs Office, may be contacted at 324-2727 for whatever assistance the Committee may need as it deliberates S. 2726 and the Intelligence Authorization Act.

Sincerly yours,

WILLIAM S. SESSIONS,
Director.

AMERICAN FOREIGN SERVICE ASSOCIATION,
Washington, DC.

HON. DAVID L. BOREN,
Chairman,
Select Committee on Intelligence,
211 SHOB,
U.S. Senate.

DEAR SENATOR BOREN: Please find enclosed 21 copies of a statement by Theodore S. Wilkinson, President of the American Foreign Service Association regarding the proposed Counterintelligence Improvements Act of 1990. The American Foreign Service Association thanks the Committee for the opportunity to submit this statement in connection with the hearing scheduled for July 12.

Sincerely,

TURNA R. LEWIS,
General Counsel.

STATEMENT OF THEODORE S. WILKINSON, PRESIDENT, AMERICAN FOREIGN SERVICE ASSOCIATION

As the professional and labor organization representing the members of the United States Foreign Service, the American Foreign Service Association (AFSA) is concerned by certain aspects of the proposed Counterintelligence Improvements Act of 1990. While the AFSA agrees that all reasonable precautions against espionage must be taken, we do not agree that the proposed Act, as presently drafted, will contribute uniformly to the goal of protecting and preserving our national security.

Even if the proposed Act provided marginal improvements in security, certain draft provisions are unreasonable and overly intrusive on the rights and privacy of Americans. We urge this Committee to reconsider these provisions.

Government workers in general, and Foreign Service employees in particular, have suffered a substantial loss of privacy over the past few years. A panoply of preemployment forms demand ever-growing amounts of personal, medical, and financial information as a prerequisite to government employment. In addition, many Foreign Service employees are required to possess a TOP SECRET clearance as a condition of employment, and while background checks on these individuals are clearly necessary, the procedures often involve further loss of individual privacy.

The purpose of the Counterintelligence Improvements Act of 1990 is ostensibly to strengthen the ability of the United States to deter, detect, and prosecute persons

who turn to espionage. The American Foreign Service Association has reservations about the utility of some features of the proposed Act to accomplish these goals.

In some respects the proposed legislation does no more than codify existing practiced. Some of the procedures called for in the proposed act are already in effect. Section 801, for instance, would establish procedures to strengthen the security clearance process, but Standard Form 86 already fulfills the same requirements by asking questions relating to credit history, foreign travel for business and/or personal reasons. Section 802 of the proposed Act establishes authority for periodic clearance updates on a 5 year basis. Within the Department of State, current regulations already provide authority to the Diplomatic Security Service to "update security clearances of all employees periodically, or as required by changing circumstances . . ." (3 Foreign Affairs Manual (FAM) 162.4).

The Proposed Act does not adequately balance the government's interest in preserving and protecting our national security against the public's interest in civil liberties and the privacy rights of citizens. Section 801 of the Proposed Act would allow access to personal and financial information for a 5 year period after termination of a security clearance. We would urge the Committee to reconsider this blanket intrusion into the personal affairs of private citizens and to base access on a reasonable cause standard. Section 901 of the Proposed Act would subject individuals with access to crytographic information to periodic polygraph exams. These exams have been found to be unreliable indicators of veracity. Again, while the American Foreign Service Association supports measures which strengthen protection of national security, we oppose provisions in the Proposed Act which rely on questionable measure such as the polygraph exams. Until the accuracy of polygraph examinations improves, the American Foreign Service Association will oppose widespread use of this test among the personnel that we represent. Members of the Committee will recall that former Secretary of State Shultz took a similar position when broad polygraph authority was sought for State.

The American Foreign Service Association does not challenge the government's authority to conduct background investigations for employees with access to classified information. We think the intent of the Proposed Act is laudable; however, overall, there is a need for more due process protection for individuals and less discretion in the hands of federal agencies. We do not believe that federal employees should be asked to give up their constitutional rights, including their right to privacy, so that security investigation authorities may obtain complete access to information on the employee, regardless of its relevance.

In previous testimony before other committees we have expressed our concerns about the encroachment of government into the personal lives of government employees and asked for specific legislative relief to address the serious erosion of individual due process rights. Specifically, AFSA has proposed the institution of periodic reports to the employee on the status of any adverse action regarding his clearance, as it is not uncommon for employees to have their clearances suspended for an unlimited period of time. AFSA has also proposed that the recommendations of security agents in the areas of assignments, promotions, and tenuring decisions be presumptive at best, and that they not control agency personnel determinations. Finally, we have proposed review by the Service Grievance Board of security clearance reductions or revocations, to ensure that those decisions are not arbitrary, capricious, do not constitute an abuse of discretion, or are not otherwise contrary to law or regulation.

We see no reflection of these desirable additional bulwarks to employee rights in the Proposed Act. We see only one further step in the exonerable march toward cradle-to-grave security investigations.

AFSA urges this Committee to reconsider its provisions for the Proposed Act which would allow broad unfettered intrusion into an employees life, and to adopt provisions which reflect our adherence to the standing principles of civil liberties and due process.

Chairman BOREN. At this time, I would like to welcome Ms. Mary Lawton if she would come forward to testify for us. She is the Counsel for Intelligence Policy, as I mentioned, at the Department of Justice. She has appeared before us many times, though usually in closed session, I would say, in the Committee. We certainly value her advice and her counsel and have asked her to provide the views of the Administration on this bill, recognizing that it would affect many departments and agencies should it be enacted.

Mary, we welcome you to the Committee and ask that you would proceed with your remarks and suggestions for us.

Ms. LAWTON. Thank you, Mr. Chairman. If I may, I would like to be joined by John L. Martin, our Chief of Internal Security.

Chairman BOREN. Mr. Martin, we are glad to have you.

TESTIMONY OF MS. MARY LAWTON, COUNSEL, OFFICE OF INTELLIGENCE POLICY AND REVIEW, U.S. DEPARTMENT OF JUSTICE; ACCOMPANIED BY, MR. JOHN MARTIN CHIEF, INTERNAL SECURITY DIVISION, U.S. DEPARTMENT OF JUSTICE

Ms. LAWTON. Mr. Chairman, it is a pleasure to appear before you today to give the Administration's views on S. 2726, the legislative proposals developed by the Jacobs' Panel to enhance our ability to detect and prosecute persons who commit espionage. In commissioning the Panel, the Committee demonstrated its awareness of the threat to our national security posed by those who would provide highly sensitive information to foreign adversaries. The United States has great reason to be proud of the thousands of dedicated, absolutely loyal citizens in sensitive positions who daily deal with matters effecting the gravest national interests. Unfortunately, there are also a very few who, for whatever reason, choose to betray their country, the American people, and their loyal comrades and colleagues.

Since 1980, the Department of Justice has prosecuted 45 individuals for espionage and related offenses. At no time since the enactment of our Nation's first espionage laws in 1917 have there been more espionage prosecutions. No agency of the Intelligence Community, no arm of the military, no category of information has been left unsullied by the predations of hostile foreign intelligence services, and by the act of those very few American citizens who have volunteered to breach the trust reposed in them.

The 13 Jacobs Panel proposals address three distinct areas of concern, as you have outlined. Improvement in the personnel security system. Penalties for espionage-related activities. And enhanced Counterintelligence Investigative capabilities. I should like to discuss in detail each proposal as it relates to each broad category. Before proceeding, let me say on behalf of the Administration that we welcome the Jacobs Panel's proposals as evidence of a bipartisan effort to improve counterintelligence measures. We are very appreciative of the Panel's hard work and their thoughtful proposals. For the most part, our suggestions reflect either an effort to fine tune proposals or our views on the proper framework within which Congress and the President can work together in this area. We welcome the opportunity to work with the Committee and its representatives on these important proposals.

The Panel made four proposals to improve the personnel security system. The first 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 clearances would be required, among other things, to consent to access to their financial records, consumer 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 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 eligibility for access to TOP SECRET information. Waivers of the minimum requirements may be granted, but must be recorded and reported to both the Senate and House Intelligence Committees.

We think it is reasonable that persons whose position afford them access to the most sensitive information be subject to heightened security to determine their eligibility for access 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 Administration is actively addressing the issue of uniform standards. We will certainly carefully consider the Jacobs Panel's recommendations as we move forward with this process.

The concept of allowing continuing access to financial records of those who hold security clearances, which is contained in the Panel's second proposal, rather than the limited access now provided under the Right to Financial Privacy Act's consent provisions, is helpful, at least during periods of employment. Those who have sold secrets in order to get out of financial difficulties generally got into difficulty some time after their initial personnel security investigation was completed. We have some specific suggestions to fine tune this useful proposal, and we would be happy to share them with you.

The Panel has also proposed adding 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 during the period personnel are granted access to cryptographic information or material. Briefly stated, only individuals granted access to classified information regarding the design or operation of cryptographic devices, having routine access to places where classified cryptographic key is produced, or assigned responsibilities as custodians of classified cryptographic key would be subject to the requirements of this section.

The spate of espionage cases in the last decade demonstrated that personnel with access to U.S. cryptographic information and keys are targeted by hostile intelligence services. This comes as no surprise. Knowledge of the cryptography employed by the United States, or possession of U.S. cryptographic keys, enables those who have it to read U.S. encrypted communications and, thereby, provides them access to the wide range of secrets the cryptography was intended to secure. The Panel has rightly recognized that such information and material is uniquely important to the national security. Our principal concern here, as with the Panel's proposal on uniform standards for access to TOP SECRET information, is that we believe that such standards should be set by the President, not Congress. In that way, the individual needs and circumstances of the various agencies affected can be considered and accommodated. In particular, our past experience has been that decisions and policies concerning the use of polygraph examinations are best left to

the discretion of each agency. We will carefully consider the Jacobs Panel's recommendations in this regard.

The Panel has also proposed amending the National Security Agency Act of 1959 to authorize the Director of the National Security Agency to expend Agency funds to assist current and former NSA employees who have been found to be ineligible for continued access to Sensitive Compartmented Information and employment with NSA. Assistance would be authorized for up to 5 years and could include help in finding employment, treatment of medical and psychological disabilities, and financial support. Such assistance could be provided, apparently without dollar limit, when in NSA's judgment it would be essential to maintain the employee's judgment and emotional stability. The purpose of this proposal is to provide NSA authority to assist current and former employees who have personal problems that may lead them to turn to espionage. An agency determination as to when personal problems may lead current and former employees to turn to espionage presents considerable practical difficulties. If these practical difficulties can be resolved, we can consider extending this authority more broadly to other segments of the Intelligence Community as well as to personnel in similar sensitive positions elsewhere throughout the Government. If upon further review and evaluation this proposal appears to be workable, we will work with the Committee to attempt to fashion appropriate coverage and conditions for implementation.

Five of the Jacobs Panel's proposals would either create new criminal offenses, or enhance the penalties of existing provisions. The Panel proposes to criminalize the possession of espionage devices which are, "primarily useful for the purpose of surreptitiously collecting or communicating information". For the crime to be complete, possession of the device must be accompanied by the intent to use it to commit espionage.

This provision would be potentially useful where a spy has been provided exotic tools of the trade by a foreign intelligence service. In this regard, we recommend broadening the proposal to include the use of such devices to undertake actions in violation of 50 U.S.C. 783(b), the Scarbeck Act.

We are compelled to note, however, that as drafted, the proposal requires the Government to prove that a device is primarily useful for the surreptitious collection or communication of information. This essential element of the offense may be quite difficult to establish. Moreover, it could appear that the gravity of the offense is the possession of paraphernalia with requisite intent, regardless of whether the items have an innocent primary purpose. Given the stringent intent requirements of this provision, the knowledge of primary purpose requirement is gratuitous. The statute applies to possession in the United States or in areas within the jurisdiction of the United States. It would be useful to clarify whether this phrase is intended to cover geographic locations or subject matter areas. If the latter, the statute may appear to have extraterritorial application to which foreign governments may take exception. We would like to work with the Committee to strengthen this provision.

The Panel has also proposed making it a crime knowingly to sell, or otherwise transfer for valuable consideration to representatives

of a foreign power, TOP SECRET information. Significantly, the propriety of the TOP SECRET classification could not be an element of the offense. Through this formulation, the Panel has sought to eliminate trial testimony about the nature of the information compromised as now required by 18 U.S.C. 793 and 794, to prove its relationship to the national defense. By covering only saleslike transactions, the provision would not apply to leaks of information. The proposal does not include attempts or conspiracies to violate the provisions and we believe it should.

We also note a possible ambiguity in intent within this proposal. 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 appreciate the difficulties the Panel identified in balancing national security interests in the requirements of proof—at trial in prosecutions involving unauthorized disclosure of national security information. We are anxious to explore new options in this regard, but we have not resolved at this time relevant competing considerations. There are technical and practical aspects of this proposal that deserve fuller exploration. And we look forward to working with the Committee on the further development and refinement of this aspect of the proposed legislation.

The Panel has also proposed an offense punishable by imprisonment for not more than a year or removal from employment or both for the unauthorized removal and retention of TOP SECRET material. In this instance also, the propriety of the TOP SECRET classification is not an element of this offense. While we fully understand the Panel's motivation in making this proposal, as currently drafted we do not think it could achieve its intended benefits. Under current law, individuals who retain without authority national defense information classified at any level are subject to up to 10 years' imprisonment. Neither existing law nor the Panel's proposal requires proof that the unlawfully retained materials were to be communicated to a foreign government.

The Panel has correctly recognized that the penalty for this conduct under 18 U.S.C. 793(e) and related provisions is severe, and may, where the conduct is not aggravated, contribute to a decision by the Department of Justice to decline prosecution. I should like to make it clear, however, that the potential penalty is never the sole or dominant reason for which a prosecution in this important area may be declined. Through our charging decisions, and now by appropriate use of the sentencing guidelines, we are able to fashion prosecutions for retention of materials where the potential punishment fits the crime.

It should be noted that enactment of this proposal, without substantial amendment to 18 U.S.C. 793, would create the anomaly of subjecting the individual who retains confidential material to a potential 10 years' incarceration, while the offender who retains far more sensitive TOP SECRET material may be imprisoned for not more than 1 year. Also, it is unusual for a Federal criminal statute to have, as a penalty provision, removal from office or employment. We believe it to be better practice for the statutes to simply make it clear the conviction would provide the basis for the employing

agency to terminate the offender's clearance and employment. Recognizing there are a number of issues with this section of the bill, we nonetheless support the thrust of this effort.

The Committee has also recommended amendments to 18 U.S.C. 3681, which provides for forfeitures of collateral profits of certain enumerated offenses, so as to include violations of 18 U.S.C. 798, as well as court-martial and foreign convictions for espionage. The ministration fully supports this proposal. We suggest adding to the offenses covered 50 U.S.C. 783, which prohibits the communication by Government employees of classified information to foreign agents.

Similarly, the Committee has proposed an amendment to 5 U.S.C. 8312 that individuals who are convicted of espionage in foreign courts can be denied Federal annuities or retirement pay. The amendment would require the Attorney General to certify, presumably to the agency where the offender was employed, that the conduct underlying the conviction would have violated U.S. law and that the offender was afforded due process. The Administration also supports this proposal, but asks that Congress consider expanding this provision to provide a means of denying retirement benefits to individuals whose employment is terminated for national security grounds pursuant to 5 U.S.C. 7532. This could be a benefit to the Intelligence Community by removing a distinction now made between individuals terminated under that statute and those separated from the Foreign Service under 22 U.S.C. 4010, who may be denied Government retirement benefits.

The remaining proposals are designed to enhance Counterintelligence Investigative capabilities. One welcome proposal would amend the Consumer Credit Protection Act to permit the Federal Bureau of Investigation to obtain consumer credit reports on persons believed to be agents of foreign powers. As you are aware, Mr. Chairman, the Administration has already requested, as part of the Intelligence Authorization Act, a similar provision permitting access to consumer credit information. There is an anomaly in existing law. The Right to Financial Privacy Act allows Counterintelligence Investigators access to bank records of an individual who is the target of an investigation, but the Consumer Credit Protection Act does not allow similar access to records which would serve to identify the bank the individual uses. This frustrates Counterintelligence Investigations. Accordingly, we favor a provision, comparable to the Right to Financial Privacy Act, which would permit access to consumer records on the same controlled basis.

We also fully support the proposal to amend the Electronic Communications Privacy Act, which is similar to a provision requested by the Administration as part of the Intelligence Authorization Act. It would resolve a problem not foreseen at the time ECPA was passed. Currently the Act permits the FBI to obtain toll records and subscriber information on targets of foreign Counterintelligence Investigations, upon a specific certification. However,if the toll records obtained under this provision, or other information obtained from a pen register or trap and trace device, show calls to or from an unlisted number, the FBI is unable to obtain information identifying the subscriber of this number. The subscriber, who is not yet identified, cannot be certified to be a target of investigation

because so little is known. Yet identification is the threshold the FBI needs to determine whether further investigation of the individual is warranted or is obviously irrelevant.

It is important to stress that the information sought under both the Authorization Act and the provision suggested by the Jacobs Panel is identification information only. Toll records would not be obtainable unless and until the individual can be appropriately certified to be the target of an investigation. Nor would subscriber's identification be available unless there were specific information that the subscriber had been in contact with a counterintelligence target. Thus, the intrusion involved is minimal.

With respect to the proposal to authorize rewards in espionage cases, we are in agreement with the Panel's concerns. We note that individuals with security clearances are, by regulation and practice, now required to not only safeguard information entrusted to them, but also to report to appropriate authorities suspected breaches of security. Security awareness briefings are routinely held for both cleared Government employees and contractor personnel. We must be cautious not to undermine the importance of this obligation through a system that may be viewed as an entitlement to a reward as of right. However, we support the proposal to make rewards available, but suggest that substantial administrative discretion be afforded in making such determinations. Specifically, we envision the inclusion of a pre-existing obligation to report as an important factor to consider in determining if a reward is appropriate.

The final provision of S. 2726 would amend the Foreign Intelligence Surveillance Act to include physical searches as well as electronic surveillance within its provisions. This would have the effect of mandating court approval for physical searches conducted for intelligence purposes.

As the Committee is aware, the existing authority to authorize physical searches for intelligence purposes is section 2.5 of Executive Order 12333 which delegates to the Attorney General the President's inherent authority to approve such searches. This authority has been upheld by the courts; not only in the pre-FISA case law relating to electronic searches but also by direct ruling on physical search.

The Supreme Court, of course, has not directly addressed the issue, but when it determined that warrant requirements applied to electronic surveillance for domestic intelligence purposes in *United States* v. *United States District Court*, it specifically declined to apply this holding to foreign powers or their agents.

We are fully satisfied that the President's authority in this area is adequate to meet our intelligence needs. Nevertheless, we maintain an open mind on the question whether legislation which supplements this authority would be useful. Upon review of the proposed language in S. 2726, however, we have concluded that amendment to the FISA statute is not the best vehicle for such supplementary authority. That statute is so thoroughly directed at electronic surveillance that provisions such as the emergency authority and the minimization procedures do not readily lend themselves to adaptation to physical search. We are, of course, willing to discuss these drafting problems with your staff.

I close as I began, Mr. Chairman, by commending the Committee for commissioning this inquiry and the Members of the Jacobs Panel for their conscientious and valuable efforts. I would like to emphasize the Administration's willingness to work with the Committee and the Jacobs Panel to achieve, improved counterintelligence measures. I should also note that some of the proposals may require additional resources to implement effectively, and we will work cooperatively with Congress to accomplish this.

Thank you.

Chairman BOREN. Thank you very much, Ms. Lawton. We appreciate your comments and willingness of the Administration to work with us in developing and refining these proposals. We certainly will take you up on your offer to do so.

I want to raise just a few questions. You indicate that while you are not quarreling with the move toward uniform minimum standards for TOP SECRET clearances, you think it is more appropriate to leave that to the Executive branch for action. And you make the point the Administration is actively addressing the issue of minimum standards.

I wonder if you can tell us how long the Administration has been actively addressing this issue? I believe that it may have begun in 1983 at the direction of President Reagan if my memory serves me correctly. So we've been actively addressing for about 7 years at the minimum. Why has this been so difficult? Am I right in my memory that we are now into the seventh year of actively addressing this and why shouldn't we decide to push ahead if it has taken this long?

Ms. LAWTON. Seventh year of the Executive branch looking at it, Mr. Chairman, but certainly not of this Administration.

Chairman BOREN. If we could begin this over again every 4 years, we can maybe be up to a 100 years before it's certain of actively addressing.

Ms. LAWTON. No, actually after the inauguration, President Bush decided to take a fresh look, using his appointees and the perspective of the new Administration, at the efforts that had gone before. The Committee working on that, as I understand it, has completed its process in a lot less time than it took the first time around, and has sent forward a recommendation to the National Security Council, is my understanding.

Chairman BOREN. Well, should we then expect a new Executive Order on security clearances fairly soon from the Executive branch?

Ms. LAWTON. I can't answer you with certainty, Mr. Chairman. I'm not involved in the process right now. And so I don't honestly know. I do know that the Committee working on it has finished and sent forward a proposal.

Chairman BOREN. Do you know if it would include access to financial records, travel records, and consumer credit records along the lines of the Jacobs Panel recommendations or not?

Ms. LAWTON. Those things, Mr. Chairman, an Executive Order could not do, because there are statutes barring that access and only with the statutes changed could that access be provided.

Chairman BOREN. So we would have to actually have legislation to amend the Right to Financial Privacy Act so the Government could go in and request——

Ms. LAWTON. Oh yes.

Chairman BOREN. That would require legislation?

Ms. LAWTON. That, and consumer credit and so forth, yes. It needs legislation and we support the proposals.

Chairman BOREN. What about the Legislative and Judicial branches? I would assume an Executive Order could not cover the other two branches of Government. Do you think there is some wisdom in trying to have an action taken that would cover the other two branches of Government as well?

Ms. LAWTON. Well, it becomes awkward always of course, for example, for the Congress to try to cover the Judicial branch, which historically, of course, has been the least troublesome branch in this area. We've never even had an allegation of a leak from them that I know of.

This body, of course, has already taken action which we think is just wonderful to set up a security system. We'd like to see the other body do as well. But certainly Congress could legislate across-the-board for itself. In theory, it could in connection with court employees. But as I've said, that's a bit problematic. And that is not an area that has been proved difficult.

Chairman BOREN. On the polygraph provision, I gather you take the same position, that it would be better to leave it up to the Executive branch and Executive Order which would allow for greater flexibility. But isn't it the point of the Jacobs Panel that if we do leave it up to the Executive branch, there are simply going to be many agencies, perhaps some of those where the need is greatest, that will simply decide not to take any action in this area?

Ms. LAWTON. Well, without some specific directive from the Executive, agencies are under no obligation to adopt their own policies. If the Executive were to issue such a directive they would comply with it.

It is a difficult problem in part because, as you know, for a while, Mr. Chairman, the Department of Defense was under statutory limitations. No matter what the President said, they could only do so many polygraphs because Congress had said they could only do so many.

Like the problem on reporting foreign contacts, which we dealt with and which I was involved with, it is very hard to issue a uniform rule for all agencies. Some agencies have foreign contacts as their mission. And a reporting requirement too strenuous for them might be all right for an agency that does that rarely.

So with the difference in mission of the various agencies, we really think that it, in practical terms, has to be that way, however strongly we might wish to increase the base standards for certain clearances.

Chairman BOREN. Well, in our discussion of the polygraph, we've talked only about communicators, very strictly constrained, only security type questions and not lifestyle questions. That's a bare minimum really. We're not talking about covering all the people in a department with TOP SECRET clearance or even those in most sensitive jobs, but strictly limited to security type questions for

those that are communicators. Do you still see the problem of those that deal with codes and ability to communicate in code? Do you still see a problem, since we are dealing in such a constrained area, with some uniform procedures for those particular people even though they are in different agencies?

Ms. LAWTON. There may well be sufficient differences. Most of the time when we think of cryptographers, we think of certain aspects of the military services and the National Security Agency. But there is indeed an increasing use of encrypted communications in other areas. Law enforcement, for example, is looking toward encryption of certain types of devices. And the standards might well be different depending in the type of encryption and the purpose of the encryption.

Chairman BOREN. Let me ask about the three new criminal provisions in the bill. Possession of espionage devices, the sale of TOP SECRET documents so designated and retention of TOP SECRET documents. I gather you feel, as the agency responsible for prosecuting these cases, there is a need for additional legislative action in this field?

Ms. LAWTON. Well, we are a little torn there, Mr. Chairman, and I'll defer to John. After all, we think we've got a pretty good record in the last 10 years with the existing laws, with the old laws.

On the other hand, there could be instances where some of these would come in handy. The unique sort of fact situations. We know that the Jacobs Panel, in working on these, was looking at specific cases as they looked for ways that the law could be enhanced that it might help. And you never know what the next twist or turn might be. But I——

Mr. MARTIN. Mr. Chairman, if I may? We discussed this at some length with representatives of the Jacobs Panel and had an opportunity to talk to your staff about it.

With regard to the criminal provisions, there is—while these provisions would be helpful, the unique nature of the crime of espionage makes it very, very difficult, not only to define but also to enforce. It is a crime that leaves no footprints. It is not like the ordinary, street crime, the ordinary theft or homicide. And while these provisions are helpful, they do not solve, and they are not intended to solve, the very difficult and complex evidentiary problems that we have when we face trial. But as Mary said in her testimony, and as we've told the staff, we want to study this more closely and see if we can come up with something that will definitely benefit our efforts, our prosecutive efforts.

Chairman BOREN. I'd like to turn to those FBI recommendations concerning information on unlisted telephone numbers, contact with agents of foreign powers and the access to consumer credit reports. As I understand it, the FBI proposal would allow the FBI to identify people with unlisted numbers whose phones are used in communication with foreign powers. And I suppose this would apply to everyone that called a foreign embassy. A number of these calls might well be legitimate calls for purely legitimate reasons. ACLU proposes changing the language of the amendment to allow the FBI to identify people with unlisted numbers only if the Bureau has probable cause to believe that the foreign agent, so called or was called from an unlisted number, is involved in clan-

destine activities. Would the probable cause standard create a problem for the FBI if we were to add that to the legislation?

Ms. LAWTON. It certainly would, Mr. Chairman. Access now under the ECPA statute doesn't require probable cause. It requires specific and articulable facts, a lesser standard, and that to get the toll records of an individual, to track all their calls.

A probable cause standard for unlisted numbers would be even higher than what we would need to get toll records, a far more intrusive inquiry.

Yes, it would be impossible to live with.

Mr. MARTIN. And it might frustrate some very significant investigations. You may recall, Mr. Chairman, that defendants such as Ronald Pelton, John Walker, Christopher Michael Cook had open contacts with foreign embassies.

Chairman BOREN. On the consumer credit reports, there has been concern voiced that financial information from these credit reports could be misused. Could you accept a restriction against the use of the substantive financial information from the consumer credit reports beyond the names of the financial institutions where the FBI already will be able to go to get the underlying information? Would that be a problem?

Ms. LAWTON. Well in certain circumstances, it might, Mr. Chairman. I'm thinking for example of the *Cavanaugh* case. Cavanaugh did what he did in offering to sell information primarily because of a debt load he was carrying and he was trying to recover. The price he asked for what he was selling was exactly what he needed to clear off the debt load on his consumer credit records.

Chairman BOREN. Although if you got the names of the institutions with which he was dealing, couldn't you then go to one of those institutions and get the underlying information as opposed to the summary of that information in a consumer credit file?

Ms. LAWTON. You could get the identity of his bank. But his debt problems may not have been limited to the bank. He could have been running a float on credit cards. The debts where probably scattered around.

Chairman BOREN. You can't get that information now, for example, from credit card balances or consumer debt from let's say a merchandise institution as opposed to a bank?

Ms. LAWTON. Well, the prime source though to identify all of that is your consumer records. The example that the FBI always cites to me—and it's a bit of an irony, it doesn't quite answer your question—but it's that as a businessman in Norfolk, John Walker could have gotten credit records by paying a fee, of anybody he inquired about. The FBI could not get his.

Chairman BOREN. I see your point.

Let me just ask one last question. The ACLU also, of course, strongly opposes secret searches with or without a court order. We get into the whole question of what the inherent authority is or is not without a court order. Is the Administration opposed to any kind of notice, even after the fact, of a search having been made, so that perhaps the person against whom a search was made could test at some point in time the legality of the search?

Ms. LAWTON. Yes, Mr. Chairman. I believe the Committee has some knowledge of the sort of targets that are involved. And focus on it for a while and I think you will see why we it gets——

Chairman BOREN. I assume that at the time of prosecution there would be access to the fact that these searches had taken place.

Ms. LAWTON. If there is prosecution——

Chairman BOREN. If there is prosecution.

Ms. LAWTON. There was in the TRONG case—and that was a case where, which John's far more familiar than I—in which the defendant had the full opportunity to challenge the search and did.

Chairman BOREN. So you might have a closed case, for example, where a search, perhaps an electronic search with a court order or a physical search without a court order, was made. Then a decision was made not to prosecute possibly because there were insufficient grounds. The person, even though the case had been closed, would not necessarily have ever been aware of a search.

Ms. LAWTON. That's right. That's the way it operates now under the Foreign Intelligence Surveillance Act.

Chairman BOREN. Senator Specter has joined us. Senator Specter, are there any comments or any questions that you would like to ask at this point?

Senator SPECTER. Thank you very much, Mr. Chairman.

First, I do have an opening statement which I will just insert in the record.

[The prepared statement of Senator Specter follows:]

PREPARED STATEMENT OF SENATOR ARLEN SPECTER

I want to thank the Chairman and Vice Chairman for their initiative in constituting a special panel—the Jacobs panel—to assess the need for and remedies to our security and espionage laws.

In the past five years especially, there has been a near hemorrage of espionage in the United States which according to Defense Department estimates has cost tax payers billions in terms of lost defense capabilities and in terms of necessary countermeasures. The Jacobs panel has served a useful purpose in pointing out where our current espionage statutes are in need of strengthening.

While the world is on the verge of a new order based on principals of democracy, no nation or responsible leader can ever abrogate responsibility for national security. Every American and indeed, every sane individual should welcome the efforts to reduce or eliminate arms but not simply for the sake of disarmament, for the greater goal of peace and harmony can realistically be achieved only through cooperation and vigilance. For the latter this equates to deterrence and defense in consonance with the threat.

The history of mankind has shown that no matter the level of cooperation and defense, nations will always want access to other nations' defensive posture. Unfortunately, while this country has not been immune to the scourge of treason, the more recent past has demonstrated a shift in motivation from ideology to profit and personal gain. The results are equally devastating.

I applaud the efforts of Eli Jacobs and his panel. Their efforts have been expansive, thorough and thoughtful.

However, I am sure that the members of the panel and this Committee will agree that in our quest to preserve national security, we do not erode basic human and civil rights guaranteed by the Constitution and Bill of Rights.

In our hearing today, I shall be mindful of the need to strike a balance between security and these basic rights. In reviewing the Panel's proposals, I find myself in full agreement in principal. I therefore look forward to clarifications and opposing views on several provisions which will allow me to support them or recommend modifications.

Chairman BOREN. Let me say that Senator Specter has been a very active Member of the Committee in this area.

Senator SPECTER. I start by joining in the commendation of the Jacobs Panel for all the very important work which the Panel has done.

With respect to the provisions under the Foreign Intelligence Surveillance Act, and the current proposal that there be a warrant if there is to be an electronic surveillance, I understand your position to be that you think there should not be an additional statutory requirement for search and seizure of physical evidence. Is that right, Ms. Lawton?

Ms. LAWTON. Well, the problem, Senator Specter, is that we would not want an exclusive statute, a supplementary warrant requirement or warrant authority we would not object to. We would not want an exclusive requirement. The FISA statute, as you know, is crafted in such a way that by definition a number of items fall outside its mandate. And indeed even with——

Senator SPECTER. Would you enumerate those, please?

Ms. LAWTON. I can't in open session, Senator.

Senator SPECTER. Excuse me?

Ms. LAWTON. I can't in open session.

Senator SPECTER. OK. But the physical——

Ms. LAWTON. But in the statute there is a provision for certain types——

Senator SPECTER. But the statute is public.

Ms. LAWTON. The statute is public. But——

Senator SPECTER. But the statute does not contain the exclusions, you say?

Ms. LAWTON. What I am saying, Senator, is in the definitions of the statute, certain things are included and those are public. What those definitions leave out——

Senator SPECTER. Is not public? Can't figure it out from what is in the definitional section? I would doubt that, but let's not——

Ms. LAWTON. Not without a considerable body of knowledge, no.

Senator SPECTER. Well, I question that. But let's not pause on to that unduly.

Let's come to the central point as to why you shouldn't have a warrant requirement for physical searches as well as a warrant requirement for electronic surveillance. Currently, the satisfaction of appropriate privacy standards are met so long as you gather the evidence on the warrantless searches only for intelligence purposes. But not if they are for prosecutorial purposes. Correct?

Well, it seems to me as a former prosecutor that that puts a very important factor at risk. And that is whether you are able to prove at trial that the prosecutorial purpose was secondary and that you are really looking for an intelligence purpose. And why not use the special court which has been set up under the Foreign Intelligence Surveillance Act on searches as well as on electronic surveillance?

Ms. LAWTON. Well, the issue of the primary purpose preceded the FISA statute and has carried over since the FISA statute. We have had to fight that battle in every one of the cases in which there has been a prosecution, with or without the court order process.

Senator SPECTER. But if the physical search were under the Foreign Intelligence Surveillance Act, under the FISA statute, there would be no question about the usability of the tangible evidence seized in the search and seizure.

Ms. LAWTON. Oh, there are always questions, Senator Specter. Every time it is used, it is litigated.

Senator SPECTER. Well, it wouldn't be stricken summarily. Let me put it that way. Of course, you've got to satisfy the requirements of probable cause and sufficiency of the warrant and the requirements which now attach.

Let me approach it from a different angle because I want to move on to some other questions.

The requirement for a warrant under the Foreign Intelligence Surveillance Act as it relates to electronic surveillance is essentially the same reason that we require warrants in other lines for search and seizure where you have time to get a warrant. The privacy interest. And now the Presidential authority is delegated to the Attorney General. But why not take that extra step and have the Attorney General submit a warrant for a physical search to the Foreign Intelligence Surveillance Act court?

Ms. LAWTON. There may be circumstances where it would be useful to do that. But our concern is in derogating the authority that the President now has. It's essentially a separation of powers concern.

Senator SPECTER. Well, but why not? Is there any practical problem? Are you concerned about speed? Why not take it to the court? Because that's what you have, that's what you have on search and seizure generally. Why not, in this situation, especially where you have the parallel of the warrant for electronic surveillance?

Ms. LAWTON. Well it's a debate that goes back to that original requirement. If you recall, at the time the Foreign Intelligence Surveillance Act was debated, this tension between withdrawing certain powers from the President and transferring them to the Judiciary was an element on which many opposed the Foreign Intelligence Surveillance Act. The Administration at the time did not, in part because of a practical imperative. Electronic surveillance can only be done with phone company cooperation and we weren't getting it.

That practical imperative which overrode the separation of powers argument with the then Administration doesn't exist here.

Senator SPECTER. All right. I think I understand your position. But it seems to me that the same public policy considerations which weighed in favor of Judicial approval on electronic surveillance would weigh equally on search and seizure and then from a prosecutor's point of view, it could eliminate a very major obstacle to a successful prosecution. Because if you have the warrant in advance, then you don't have to worry about being able to establish the primary purpose being intelligence with the prosecution only secondary.

Mr. Martin, I'd be interested in your view on that, considering your career prosecutorial position in this field.

Mr. MARTIN. When you get into this very delicate area, Senator, you don't always know where the investigation will take you. And the counterintelligence aspects oftentimes are primary. That is to detect who is committing the espionage, to determine what country may be involved, how the—what information is going over to the other side, and how it is going.

And there are numerous times, during the course of an investigation, where we wrestle with this problem. And, in the last decade, what you have seen in the 45 or 46 cases that we have taken so far, you have seen decisions where we have gone forward with a prosecution. There are times when we decide not to and for very good and sufficient national security reasons.

So, retaining that option is important, I think, to the Community and to the people who have to make those decisions.

So, I understand what you are saying——

Senator SPECTER. You always have the option. You don't have to bring the case. The only point is that if you do bring the case, you've eliminated the potential impediment. Perhaps there are some of those cases that you haven't brought because you feel you couldn't prove that intelligence gathering was the primary purpose.

Mr. MARTIN. No. There have not been those situations. And I might point out to the Senator, I know your concern for judicial oversight of these activities, but in reviewing the cases, for example, that we have taken over the last 15 years, there have been no illegal searches that have been suppressed by any court, no involuntary confessions, no prosecutorial investigative misconduct found in any of these cases. So that the standards that the Department has been applying over the years have been very strict and very high and very much in keeping I think with what you are proposing in connection with your suggestions.

Senator SPECTER. Let me move to another question and that is whether the issue as to the proof of damaging national security would be eliminated by the Jacobs Panel recommendation.

Mr. MARTIN. It may or may not. We, again, wrestle with this problem. We have never had a situation where we have been able to go into court and say because there is a classification stamp on this particular document and it has been illegally retained or transmitted, that a jury would convict and a court uphold that conviction. We have always had a combination of charges which would require us to explain to a jury and to a court the national defense character of the documents.

I'm not sure, and I don't feel that confident that you can just go into court and say it is classified and therefore meet the standard.

Senator SPECTER. Well, if the Congress enacts a statute which says that it is illegal to sell TOP SECRET information and omits a requirement that there has to be proof of injury to national security, do you have a doubt that the Congress can make a criminal statute which says only——

Mr. MARTIN. No, no doubt.

Senator SPECTER. —it is unlawful to sell TOP SECRET material?

Mr. MARTIN. I think though it would depend on how it was first applied. And that is that you would have to make awfully certain, as you do now, that the document that you used to persuade a court and jury that a criminal offense has taken place is a document that indeed warrants a legitimate classification of TOP SECRET.

Even though you have removed that from the purview of the court, I think it is the responsibility of the prosecutor to make sure

that before a case is taken under such a statute that it is a bona fide classified document.

Senator SPECTER. Well, I don't agree with you about that at all. But, if you are correct, I think that if it is classified TOP SECRET and the Congress says that once so classified and then sold, it's a violation of law, I think that's sufficient. It would be pretty hard for somebody to defend on the ground that it was an erroneous classification or a wrongful classification.

But even if you are correct on that, it would be a lot easier to justify the TOP SECRET classification than to go beyond and prove injury to national security.

Mr. MARTIN. Perhaps. But I think that if you went into court with a document that was clearly—did not warrant the classification that it bore, that you would have some difficulty in upholding that conviction, Senator.

Senator SPECTER. Where someone sells a document which is labeled TOP SECRET?

Mr. MARTIN. If it did not warrant—Senator, I have seen—and I think perhaps you have a number of documents that——

Senator SPECTER. I'm not totally unfamiliar with criminal prosecutions.

Mr. MARTIN. I know that, sir.

Senator SPECTER. Let me move on to the issue of procedure on taking away security clearances. I understand that there is some concern about the absence of the Jacobs Panel Commission in addressing the subject of due process of procedures for determining where someone has failed to disclose travel or contact with foreign officials, etc.

Do you think that we ought to provide for a hearing process to make that determination in the statute?

Ms. LAWTON. Well, as we indicated in the testimony, Senator, we're not really sure that it ought to be the Congress that is dealing with this area at all.

Senator SPECTER. You are pretty sure that the Congress shouldn't deal with this area at all.

Ms. LAWTON. Well, Congress has its own responsibilities in its own area. And, as I've said before to the Chairman, the Senate has dealt with that in setting up its own security procedures in just relatively recent years.

But in terms of the Executive branch, historically, as you know, this has always been handled by Executive Order and the procedures have been laid out. They are obsolete. I think it is generally recognized that they are. But the Executive branch is working on an effort to update and modernize them. And——

Senator SPECTER. Do you currently have a procedure for making that determination when you take away a TOP SECRET clearance?

Ms. LAWTON. It varies from agency to agency now. There is no uniform baseline and no uniform procedure. The Justice Department has its regs, the State Department has their own regs.

Senator SPECTER. Some have none?

Ms. LAWTON. It's very possible that there are agencies that have none.

Senator SPECTER. Well, if Congress does decide to impose this standard for TOP SECRET, do you think that Congress ought to take the corollary step of establishing procedures for taking TOP SECRET clearance away?

Ms. LAWTON. If Congress were to occupy the entire field, procedure becomes part of it. Yes, I think the Congress needs to consider whether what is required is a baseline with the flexibility to go further on the part of agencies, or whether an absolute, across-the-board standard with no deviation from anyone, by anyone, is to be required.

This is, as the Chairman pointed out earlier, an area I've been involved in more than I wish. And one of the things you discover when you start looking at it over the entire breadth of the Executive branch is that the resources, the numbers, the ability to handle procedures varies widely from agency to agency. We once got in a discussion of whether polygraph ought to be required for all TOP SECRET. And I remember saying to one of the people I was discussing it with, how many polygraphers do you suppose the Department of Agriculture has? Because they almost certainly have some people with access to TOP SECRET information. But I doubt they have polygraphers.

We have others talking about the necessity of holding formal hearings to remove a clearance—one proposal—before administrative law judges. FBI doesn't have any administrative law judges. A lot of agencies don't.

So, when you start talking about a standard across-the-board, you have a problem. If you're talking about a baseline on which different agencies can build, you come to a different conclusion.

Senator SPECTER. I have a very brief, final question to you Mr. Martin.

The Senate passed a death penalty bill yesterday including espionage. I had introduced legislation on this subject in a separate bill last year and got very deeply involved in the statistics of espionage cases and espionage for money. And there has been a very significant increase in such cases. And, taking the last three decades, there's been an enormous increase in espionage cases and it appears to be a pretty sharp correlation with the amount of money involved on an analysis of these cases.

Do you think that the death penalty would have a significant deterrent effect on espionage cases where people appear to be more and more into it for the dollar value as opposed to some ideological reason which might have been present on past espionage cases? Do you think the death penalty is an effective deterrent?

Mr. MARTIN. I would hope so, Senator. You are absolutely right that you see more people committing espionage for reasons of greed rather than ideology. And I would hope that there would be a deterrent and I expect that it might be.

Senator SPECTER. Thank you very much. Let me compliment you, Miss Lawton, and you, Mr. Martin, on your work with the Government. We've seen you here before on many occasions. And it's very reassuring to have this kind of professionalism that both of you display on these important subjects even if we might not agree on all of the legal consequences.

Mr. MARTIN. Thank you, Senator.

Ms. LAWTON. Thank you, Senator.

Chairman BOREN. Thank you very much, Senator Specter.

And again let me thank both of you for being with us today. We value your comments.

Ms. LAWTON. Thank you, Mr. Chairman.

Mr. MARTIN. Thank you, Mr. Chairman.

Chairman BOREN. Thank you.

Our next witness is Morton H. Halperin, Director of the Washington Office of the American Civil Liberties Union, who is very well known to us on this Committee as are his many constructive efforts to ensure that our civil liberties are preserved and protected. Legislation in this area inevitably raises questions of balancing such rights and liberties against the needs of Government for maintaining adequate security. So we look forward to your counsel in this regard.

I note that the statements of our remaining two witnesses are rather lengthy and I might suggest that we insert them in full into the record and then perhaps you could summarize for us and hit the high points of your testimony and direct us to the major areas of your concern.

Mr. HALPERIN. Thank you, Mr. Chairman. I was going to suggest doing that and I am glad to do that.

[The prepared statement of Mr. Halperin follows:]

PREPARED STATEMENT OF MORTON H. HALPERIN

Mr. Chairman:

I very much appreciate this opportunity to testify on behalf of the American Civil Liberties Union (ACLU) on S. 2726 and the Jacobs' Panel legislative recommendations to improve counterintelligence. The ACLU is a non-partisan organization of over 275,000 members dedicated to the defense and enhancement of civil liberties guaranteed by the Bill of Rights.

INTRODUCTION

Since 1985, the "year of the spy", the American Civil Liberties Union has made clear its belief 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 were therefore encouraged by the formation of the Jacobs' Panel and find much to commend in its activities and recommendations. We appreciate the efforts of the Panel to strike a balance between the needs of national security and civil liberties concerns. At the same time we regret that the Panel, despite the well known interest of the ACLU in these issues, did not choose to consult with us in the course of its deliberations. While we find much to support in the recommendations of the Committee, we cannot support the overall bill embodying its proposals. There are some items that we simply cannot accept and some other proposals which we could accept only as part of a more balanced package. We also regret that the Panel did not recommend any legislation to require changes in the current system. We believe that such changes are needed to make the process more consistent with the individual rights of those affected.

Before turning to a specific discussion of these issues, I would like to make some general remarks about the Panel's approach. The report adopts many of the basic points that we believe should guide any reorganization of the counterintelligence efforts of the United States. Let me try to make each of these points explicit.

The first fundamental insight of the report is that economic and not ideological motives lead people to espionage. Moreover, the decision to become a spy occurs *after* a person has obtained a security clearance and gained access to high-level classified information; people do not get clearances in order to be able to provide information to a foreign power. Thus, the focus of attention should be on economic incentives and job dissatisfaction and not on ideology or other extraneous factors. The present system of concentrating resources on an unnecessarily intrusive initial

clearance should be replaced with a system which gives equal priority to the initial clearance and subsequent reclearances for those persons who most likely would be targeted by foreign intelligence services.

The security clearance process and counterintelligence efforts should focus on the nexus between the behavior and attributes of the person, and the likely causes of the decision to become a spy. The Jacobs' Panel does a good job of redirecting these efforts towards economic and other relevant concerns. The Panel does not, however, propose specific legislation that would require the Executive branch to stop focusing on irrelevant concerns. The ACLU believes that this must be done for two compelling reasons. First, these other inquiries frequently lead to violations of civil liberties. Second, bureaucracies change their patterns of behavior slowly and with great reluctance. The national security bureaucracy will continue to spend its time compiling irrelevant personal information until it is ordered to address the true security risk—cleared employees who become spies out of greed or job dissatisfaction.

The current failure to focus on the appropriate nexus shows up most clearly in the emphasis on "left" political ideology and the special attention given to gay men and lesbians who seek security clearances. Both of these trends persist despite the evidence that people do not spy because of their ideology or their sexual orientation, and that neither marxists nor gays are more likely to become spies than anyone else.

The government continues to ask security clearance applicants about their political beliefs, and specifically if they are members of the Communist Party. It also discriminates based on sexual orientation.[1] We believe that any statutory reform of the process must explicitly prohibit such practices. We do not mean to exclude all inquiry into political beliefs or associations or sexual practices. We do, however, argue that such questions are improper unless there is some reason to believe that they are relevant based on a specific security concern arising out of the particular circumstances of the individual being investigated. There is no basis for treating one ideological group (leftists or marxists) or those who have one particular sexual orientation (gay men and lesbians) any differently from others.

A second issue raised by the report is the scope of counterintelligence statutes. Because too much information is classified and too many people have clearances, counterintelligence can only be effective when the government focuses on the relatively small group of people who have access to the truly critical information that is likely to make them targets of the intelligence efforts of foreign governments. The Panel understood this principle and singled out those with TOP SECRET clearance for special treatment.

Although a step in the right direction, this does not go far enough. The number of people with TOP SECRET clearance is simply too large to permit the counterintelligence effort to be properly focused. Moreover, most people with TOP SECRET clearance are unlikely to be targeted by a foreign intelligence service. For one thing, many people have TOP SECRET clearance only because they occasionally handle such material. For another, much TOP SECRET information is not in fact of great value to a foreign intelligence service if acquired clandestinely. For example, much foreign policy information is TOP SECRET only because of the harm to diplomatic

---

[1] The government continues to single out homosexuals as a high security risk. *See High Tech Gays* v. *Defense Industrial Security Clearance Office (DISCO)*, 895 F.2d 563 (9th Cir. 1990). Its argument, however, has shifted somewhat in recent years. Homosexuals are now deemed a security risk not because they are vulnerable to blackmail, as once perceived, but because the Soviets target homosexuals on the belief that "the homosexual frequently is shunted by society and made to feel a social outcast. Such a person may seek to retaliate against a society that has placed him in this unenviable position." *Id.* at 575, citing a DIA report in *Federal Government Security Programs, 1985: Hearings Before the Permanent Subcomm. on Investigations of the Senate Committee on Governmental Affairs*, 99th Cong., 1st Sess. (1985).

The Ninth Circuit upheld the Defense Department's discriminatory security clearance approval process against homosexuals on the grounds that "hostile intelligence efforts are directed at homosexuals," and dismissed as "irrelevant" the plaintiffs' assertion that the "reasons for targeting homosexuals [are] based on continuing ignorance or prejudice." 895 F.2d at 578 (citing a 1975 Resolution of the American Psychological Association which states that homosexuality "implies no impairment in judgment, stability, reliability or general social or vocational abilities").

By logical extension, the government could advocate, and the courts would presumably allow, the same discriminatory practice if it found that the Soviets targeted blacks, women, Jews, or any other group under the same ignorant and prejudicial belief that they too were shunted by society and made to feel social outcasts, and therefore might seek to retaliate against a society that has placed them in this unenviable position. Obviously, practices of the KGB could not justify policies so inconsistent with our fundamental principles.

relations that would occur if the information were to become public not because the information is inherently valuable to foreign countries.

We believe that the group that is singled out for special treatment should be limited to individuals with specifically designated clearances beyond or in addition to TOP SECRET where the managers of such special access programs certify that the program is likely to be targeted by foreign intelligence services. Obviously, this would include communications and intelligence activities.

The Committee will know, or can find out, if any of those who have become spies in the last ten years had only a TOP SECRET clearance. If not, it would make sense to limit these reforms to those with special clearances. If some of those who have spied only had TOP SECRET clearances, it may be possible to identify the sub-category of such people who need to be included in the program, and then to require the head of the agency to include in this program those individuals who have only a TOP SECRET clearance based on a specific finding that because of their positions they are likely to be targets. By limiting the statute to the likely targets of foreign intelligence services, Congress can ensure both that counterintelligence efforts are most effective and that the civil liberties of those who pose little security risk are not abridged.

Turning to another basic issue, we agree with the Panel that the end of the cold war does not mean that there is no foreign intelligence threat and no need for security clearance and counterintelligence programs. The American Civil Liberties Union does believe, however, that we need to end the cold war at home as well as abroad. That means that we need to consider whether the restrictions that were accepted in the past in the name of national security remain necessary and appropriate.

In particular, there is a need to consider both the definition of what should be classified and the process of classifying information. As Senator Metzenbaum indicated in his statement when the Jacobs' Panel presented its findings to this Committee, the time is ripe, indeed overdue, "to revisit the entire fundamental definition of what is national security information" and to consider "a complete overhaul of the classification system."

As Senator Metzenbaum noted, the Information Security Oversight Office (ISOO) found a high degree of overclassification, for reasons "including sheer ignorance of the standards for classification, overcaution, and a desire to give more prestige to one's work or to avoid routine oversight." Drastically limiting the amount of classified information, and the number of people who have access to it, will greatly facilitate the protection of information that needs protection and will do so in a way that minimizes constitutional infringements.

Again, Senator Metzenbaum: "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." We heartily concur.

A 1985 House Committee Staff report found that roughly ninety per cent of the classified information was classified needlessly. It recommended a two-tiered reform of the classification system: "Four types of information deserve the strongest protection: high technology products, codes, operational plans, and sources and methods (narrowly defined) of intelligence. A definition limiting classified information to these four categories rules out nine-tenths of what is now classified." Everything else that the government wants to keep secret should be labelled "administratively controlled information." Thus, "[t]he security clearance process and espionage penalties should apply only to high level national security data, while the category of administratively controlled information should be subject to much the same protections that businesses accord their proprietary information." *Preliminary Joint Staff Study on the Protection of National Security Secrets,* House Judiciary Subcommittee on Civil and Constitutional Rights and House Post Office and Civil Service Subcommittee on Civil Service (Oct. 25, 1985). Although the ACLU does not agree with everything in this report, we support this recommendation.

Any effort to reform the system must also include provisions that insure that those who are denied security clearances are afforded appropriate due process. As the Committee knows, the Administration circulated a draft Executive Order last year that contemplated drastic reductions in existing protections.

Procedural due process standards should be spelled out by statute and included in any comprehensive legislation.

There is one assumption of the Panel with which we profoundly disagree: its emphasis on future economic and industrial "espionage." We recognize that economic

issues will become more important and that foreign governments may join others who now seek to learn the secrets of American companies. However, we see very serious dangers in any governmental effort to use the procedures and apparatus designed to protect the national defense and foreign policy secrets of the American government to protect the secrets of American business. The many restrictions on individual rights that have been justified by the compelling governmental interest in protecting military and foreign policy secrets should not be extended to economic information, which, although important, is not critical to the physical security of the United States. Any attempt to focus on protecting American economic information seriously risks further erosion of basic rights.

The Intelligence Community itself has advocated the need to change its mission to combat an increased foreign threat to United States economic interests. Director of Central Intelligence Webster, in an address last fall to the National Press Club, charged that the Soviet clandestine intelligence threat to the U.S. was, if anything, increasing, but that it has refocused away from military targets towards economic targets. Accordingly, Webster asserted that the U.S. should refocus and increase its counterintelligence efforts in the economic arena. We believe that Congress, and in particular this Committee, should concentrate on inhibiting the Intelligence Community from moving in this faulty direction, rather than on encouraging or authorizing such conduct.

At the same time, we would not object if the Intelligence Community were tasked to collect additional economic intelligence as long as the collection process focuses on foreign governments. Without this limitation, however, there is a danger that the Intelligence Community will seek to gather economic information from American business firms that have this information but have chosen not to share it with the government.

The Panel report is not entirely clear as to whether the government should assume greater responsibility in preventing foreign governments from gaining access to the secrets of American firms. Apart from providing such firms with information about secure communications, we do not believe that this is an appropriate task for the Intelligence Community. We urge the Committee to monitor closely the work of the Intelligence Community on economic issues.

With this background let me turn to the specific proposals of the Panel as presented in the bill. For the convenience of the Committee, I will consider them in the order in which they appear in the bill, although some obviously raise much more serious civil liberties problems than others.

I. Section 2: Amendment to the National Security Act of 1947, providing uniform requirements for persons granted TOP SECRET security clearances.

As stated in the introduction, the ACLU believes that the authorities and restrictions granted under this bill should apply only to persons with TOP SECRET and above clearances who have been specifically designated by the managers of special access programs, or by the agency head, on the grounds that the program, or the position is likely to be the target of intelligence services. Thus, the sections concerning "Minimum Requirements" and "Requirements for Additional Investigations" should be amended to apply only to this smaller group of individuals.

For the reasons outlined above, we think the bill's focus on financial and travel information concerning individuals with these high level clearances is appropriate and should be helpful in curbing espionage. At the same time, we think the statute should explicitly prohibit the government from asking questions about political beliefs or sexual orientation, unless it can establish that such questions are directly related to a specific security concern about the particular individual under investigation. The statute should also affirmatively require that denials or revocations be based on reasons that have a nexus to a demonstrated security concern.

For example, sexual conduct could be a legitimate subject of investigation where such conduct could result in making an individual susceptible to blackmail, coercion or other financial pressures. But the fact that conduct is homosexual rather than heterosexual does not in itself justify subjecting an individual to heightened scrutiny or investigation. The current practice of subjecting individuals with certain political beliefs or sexual orientations to intrusive questioning and discriminatory treatment infringes their constitutional rights. Moreover, as the Jacobs' Panel recognized, it is unrelated to any effective program of preventing and detecting espionage. We would be willing to work with the Committee on language to incorporate this limitation.

We also think that it is both undesirable and unnecessary to limit such access only to United States citizens. The 1986 Immigration Reform and Control Act points in this direction by prohibiting discrimination based on national origin or citizen-

ship status. 8 U.S.C. § 1324b.[2] We are aware of no evidence in the last twenty years that a permanent resident alien imminently intending to become a citizen poses a higher security risk than a citizen. Indeed, we think it would be detrimental to United States interests to deny a clearance to a clearly qualified person who intends to become a citizen based solely on citizenship status.

We are also concerned that the proviso in proposed § 802(1) does not adequately protect employees from losing a clearance due to the government's delay in completing an investigation. We believe it should be amended by adding the word "solely" before "attributable," to make clear that loss or denial of a security clearance can only be based on a failure to complete an investigation that is "solely attributable to the subject of the investigation." This is necessary to prevent de minimis actions by an employee—such as turning a form in a few days late—from being used against him or her.

We also believe that as drafted the bill is unconstitutionally overbroad because it applies to employees of the judiciary and the Congress as well as to employees of executive agencies. Although the bill states that Article III judges and elected officials are entitled to access to information without obtaining a security clearance in accordance with the statutory procedures, proposed § 804(a), it goes on to provide that the President shall issue regulations that shall be binding upon the legislative and judicial branches as well as the executive. Proposed § 805. We believe that each branch should establish its own procedures. Such a distribution and balance of power in this area is more likely to protect individual rights and prevent abuses of power.

We are also concerned about the use of the term "national security" in the definition of covered information in § 803(3), because the term is overbroad and vague. Everything that contributes to the strength of our country has an effect on our national security. We think the term "national defense or foreign relations of the United States," which is the definition of national security in Executive Order 12356, should be incorporated in the bill.

Finally, we think that in addition to creating uniform requirements for high level security clearance determinations, the statute should provide minimum due process procedures for all persons who are denied security clearances, either for an initial clearance or for an upgrade, and for persons whose clearances are revoked.

While we agree that no one has a "right" to a security clearance, we strongly disagree with those who maintain that clearance denials are not subject to the basic due process requirement that the government not act arbitrarily, but only for good reason after giving the affected individual the opportunity to be heard. Despite the government's disclaimer, clearance denials are in fact viewed as an assessment of an individual's character, integrity, loyalty, trustworthiness, and judgment. A clearance denial or revocation can have a devastating impact on future job opportunities, both within the government and in the private sector.

For this reason alone, no clearance should be denied or revoked unless the person is given an opportunity for a full and fair administrative hearing with a right to judicial review. A fair hearing requires that the employee be permitted to confront all witnesses and review all relevant documentary evidence.

Recent events make clear that the right to these fundamental safeguards is under attack. As we noted in the introduction, last year the Administration circulated a draft Executive Order that would have stripped away many of the due process procedures that have been in place for the last thirty years. Executive Order 10865, DOD Directive 5200.2-R, and other agency regulations currently provide minimum due process standards for most government and government contractor employees and applicants. The draft Order would have eliminated these due process standards for clearance denials, and would have significantly lowered the standards for revocations. In the face of significant public and congressional opposition, the Administration withdrew its proposed Order for further study.

Moreover, many government agencies are interpreting the Supreme Court's decision in *Department of the Navy* v. Egan, 484 U.S. 518 (1988)—which held that the Merit Systems Protection Board has no authority to review the merits of a security clearance determination—to mean that they do not have to afford their employees

---

[2] "(a)(1) It is an unfair immigration-related employment practice for a person or other entity to discriminate against any individual (other than an unauthorized alien, as defined in section 274A(h)(3)) with respect to the hiring, or recruitment or referral for a fee, of the individual for employment or the discharging of the individual from employment—

(A) because of such individual's national origin, or

(B) in the case of a citizen or intending citizen (as defined in paragraph (3)), because of such individual's citizenship status."

any review of such determinations. And just last month, in an analogous case involving due process in a job termination for national security reasons of a USIA employee deemed an " 'intolerable' security risk" because he was a homosexual, the Court of Appeals for the District of Columbia urged Congress to use its authority "to provide substantive review of security clearance determinations." *United States Information Agency* v. *Krc*, No. 89-5220 (D.C. Cir. June 5, 1990) (Wald, C.J., concurring), (*see also id.*, Mikva, J., concurring).

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 national security cases. We view such a provision as a necessary component of any proposed legislation the Committee might approve.

II. 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, a violation of the prohibition against self incrimination and an unlawful search and seizure. We do not think that Congress, in this or any other instance, should be passing laws authorizing their use. Rather, we think Congress should legislate a prohibition on the use of polygraphs for government employees, just as it did in the last Congress for most private employees by passing the Employee Polygraph Protection Act of 1988, 29 U.S.C. § 2001.[3]

Furthermore, we are particularly concerned with Congress legislating a polygraph requirement aimed primarily at State Department employees when the Secretary of State has declared that these tests are neither proper nor effective.

The polygraph test basically depends upon simple mechanical recordings of the fluctuations in an individual's rate of respiration, blood pressure and skin perspiration during a prescribed plan of interrogation. Polygraph advocates claim these recordings can be interpreted by "trained" examiners to provide conclusive evidence of the truth or falsity of the individual's "yes" or "no" answers to particular questions. On the contrary, there is no known physiological response that is uniquely identified with the act of deliberate deception.

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.

The leading medical authorities have also warned against the use of polygraphs. The American Psychological Association has adopted a policy resolution recognizing that scientific evidence for polygraph test validity is "still unsatisfactory." In 1987, the American Medical Association and the American Psychological Association both testified against the use of polygraphs for private employees. In 1986, one of the foremost researchers on the validity of polygraph examinations, Dr. David Raskin, testified that the degree of reliability of the polygraph as a detection device falls *below 50%* whenever the number of guilty people in a group to be tested is less than 20%, even when it is used to investigate specific incidents.

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.

Twelve years ago, Sam Ervin's staff on the Senate Judiciary Subcommittee on the Constitution in its study on "Privacy, Polygraphs, and Employment" reached a reasoned conclusion that is still valid today:

---

[3] 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).

Compulsory submission to a polygraph test is an affront to the integrity of the human personality that is unconscionable in a society which values the retention of individual's privacy. . . . Expediency is not a valid reason for pitting individuals against a degrading machine and process that pry into their inner thoughts. Limits, beyond which invasions of privacy will not be tolerated, must be established.

For these reasons, we oppose this provision of the bill, and urge the Committee to remove it from the legislative package.

III. Section 4: After-care for National Security Agency employees.

The ACLU does not oppose the concept of "after-care" for NSA employees who may be targets of foreign intelligence services. We suggest, however, that the Committee amend the language in the bill to make clear that the provision applies only to the *unlawful* disclosure of classified information. Otherwise, there may be an unintended implication that there is no such thing as a lawful disclosure of classified information.

IV. Section 5: Amendment to the Right to Financial Privacy Act (RFPA) to permit access for purposes of security clearance investigations.

The ACLU does not oppose requiring individuals with high level security clearances to consent to access to their financial records. We do, however, have two concerns with the proposal as currently drafted. First, we think that this proposal, like the others, should apply only to persons with TOP SECRET and above clearances who have been specifically designated by the managers of special access programs, or by the agency head, on the grounds that the program or the position is likely to be the target of intelligence services.

Second, 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. Affirmative notice is necessary because of the length of time for which the bill allows access after the individual has given consent—anytime during which the employee has a high level clearance and up to five years thereafter, which could last longer than one's entire career.

Under current law, an individual must be informed upon request "of all instances in which [his or her] record is disclosed . . . including the identity of the government authority to which such disclosure is made." 12 U.S.C. § 3404(c). The purpose of this notice requirement is to give the person an opportunity to clarify any transactions that might appear suspicious to a government investigator but can easily be explained, thereby avoiding a more probing and unnecessary investigation. This purpose is reasonably accomplished under the present statute. Because the information can only be disclosed after the individual consents and because that consent is valid for only three months, 12 U.S.C. § 3404(a), the individual is on notice that a disclosure may occur within a three month period and can check the accuracy of his or her records and monitor whether a disclosure is made within this relatively brief time frame.

The longer period covered by the employee's nonrevocable consent under the proposed bill, however, makes effective monitoring impossible. When requiring what could amount to lifetime consent, it is unreasonable to impose on the individual the burden of continuously checking to see if the government has sought disclosure of financial records and whether those records are accurate. Accordingly, under the proposed bill automatic notice of disclosure is appropriate.

The ACLU also believes that the proposed statute should contain the same procedural safeguards as does the present limited national security letter exemption in the Right to Financial Privacy Act.[4] Information collected under the new provision should only be used for security clearance and counterintelligence purposes.[5] In addition, any government agency that seeks access to records under this provision should compile an annual tabulation and the Attorney General should report twice a year to both Intelligence Committees concerning all uses of the provision.[6] These established safeguards will serve to minimize potential abuse of consensual access to financial records.

V. Section 6: New Criminal Offense for the Possession of Espionage Devices.

---

[4] *See* 12 U.S.C. § 3414(a), discussed *infra* in section X at 33-34. In order for the FBI to request disclosure of financial records it must certify 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." 12 U.S.C. § 3414(a)(5)(A).

[5] 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).

[6] *See* 12 U.S.C. § 3414(a)(5)(C).

We share the concerns raised by Senators at the Jacobs' Panel hearing about the potential danger this proposal poses for innocent persons. We believe that it might be possible to write such a clear and stringent intent requirement that the provision would not be subject to abuse and would not sweep innocent persons into its orbit. However, 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.

VI. Section 7: New Offense for Selling to Foreign Governments Documents and Other Materials Designated as TOP SECRET.

This provision is obviously among the most far reaching of the Panel's proposals and one that requires the most careful consideration. It is this provision in particular that most forcefully implicates the ACLU's concern with developing a balanced bill.

We recognize that the Jacob's Panel chose to avoid the subject of leaks. Insofar as that meant that the Panel did not propose any new legislation directed at the perceived leak problem, we applaud its decision. Any effort to deal with that problem, particularly by criminal statutes, would require very careful attention and should be preceded by a very significant reduction in the number of documents that are classified.

At the same time, two urgent problems require consideration by both the Administration and Congress. One is the espionage problem that the Panel attempts to address by broadening the espionage statutes. The other problem is created by the use—misuse in the view of the ACLU—of the espionage and theft statutes when information is provided to the press. If Congress considers broadening the espionage laws it should simultaneously deal 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.[7]

As the Committee knows, in the *Morison* case the government for the second time sought to apply the general espionage statute (18 USC § 793) and the theft of government property statute (18 USC § 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 is a member of the Jacob's Panel, reached the same conclusion. *See* Edgar and Schmidt, "The Espionage Statutes and Publication of Defense Information," 73 *Colum. L. Rev.* 929 (1973). 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.

The Executive branch continues to exhibit conflicting views on this subject. On the one hand, it brought the *Morison* case. On the other hand, proposals to create new offenses would be entirely unnecessary if the theft statute covered such cases.

If this Committee gives serious consideration to the Panel's proposal, we urge you at the same time to clarify the espionage and theft statutes to make clear that they do not apply to the provision of information to the press. You will thus be dealing with the two urgent problems in this area. One change will make it easier to prosecute genuine espionage cases, and the other will insure that public debate is not chilled by the misapplication of the espionage and theft statutes.

I should add that the ACLU does not categorically oppose statutes that make it a crime for a government official to reveal information to the press. Rather, we insist that any such statute be very narrowly drawn, that it deal with a specific and clearly demarcated body of information, and that it provide protection for those who might receive such information.

VII. Section 8: Lesser Criminal Offense for the Removal of TOP SECRET Documents by Government Employees and Contractors.

The ACLU is concerned that this proposed statute could have the unintended consequence of being used against whistleblowers. As Senator Metzenbaum commented at the Jacobs' Panel hearing, this statute could be used to prosecute a government employee who sought to bring a TOP SECRET document to Congress to expose unlawful activities, misuse of funds, abuse of authority, or significant dangers to public

[7] *United States* v. *Morison*, 844 F.2d 1057 (4th Cir. 1988), *cert. denied*, 109 S. Ct. 259 (1988).

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." While the Panel insisted that this was not the intent of the proposal, as drafted it could clearly have this effect.

One possible way to deal with these concerns is to require that the material be retained at the unauthorized location for a period of two weeks or more. Another might be to provide an affirmative defense that the information was maintained at the unauthorized location as a means of providing it to Congress or the press.

If the provision is retained, we do not believe that a court should be granted the initial authority to terminate a person's employment. Obviously the Executive branch has the power to terminate a clearance or even government employment because of the mishandling of classified documents. However, we believe that such actions should be taken in the first instance by the Executive branch following normal procedures for terminating clearances or employment.

VIII. 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.[8]

IX. Section 10: Denial of Annuities or Retired Pay to Persons Convicted of Espionage in Foreign Courts Involving United States Information.

The ACLU has no objection in principle to the end result contemplated by this section. We are, however, concerned about the denial of retirement pay to an individual on the basis of an espionage-related conviction in a foreign country without affording him or her sufficient due process protections. We appreciate the concern for due process demonstrated by the proposed law's requirement of a certification by the Attorney General. We believe, however, that the determination of whether the foreign conviction is sufficiently trustworthy to justify the denial of retirement pay should be made in an adversary hearing with the opportunity for participation by the affected individual, and not by an ex parte certification by the Attorney General. We also suggest that a requirement be added that the foreign court be of competent jurisdiction as determined by U.S. law before its judgment can be the basis for a forfeiture. Thus, we suggest that "the Attorney General certifies that" should be stricken and "of competent jurisdiction as determined by U.S. law" should be added after "convicted by a court." With these changes we believe the statute would provide sufficient due process.

The denial of retirement pay represents a significant infringement of an individual's property right; it can also affect the rights of one's spouse and children. The Constitution requires due process before the government can take away this right, and that process must include notice and an opportunity to be heard.

An individual faced with the denial of an earned entitlement should be afforded at least as much of an opportunity to be heard as is an individual against whom a foreign civil judgment has been entered. Traditionally, an independent U.S. court proceeding has been required before foreign claims could be recognized and enforced here.[9]

---

[8] 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.

[9] Bishop & Burnette, "United States Practice Concerning the Recognition of Foreign Judgments," 16 *Int'l Law.* 425, 427 (1982).

The Supreme Court in *Hilton* v. *Guyot*, 159 U.S. 113 (1895), established substantive requirements that must be met in order for a United States court to recognize a foreign civil judgment. The foreign court must have proper jurisdiction, be of an impartial nature and afford the defendant procedures compatible with due process of law. These same basic requirements continue to apply today. *See Restatement (Second) Foreign Relations Law of the U.S.* § 482 (1986).

We do not believe that this requirement would in any way impede or prevent the termination of benefits to those convicted in foreign courts where fair and just procedures were used such that all would agree that it is fair for the United States to impose an additional penalty based on the foreign conviction. The Constitution requires an adversary hearing to determine whether the foreign proceeding was fundamentally fair. A certification by the Attorney General, however well-intentioned, is not an adequate substitute for that opportunity.

X. Sections 11 and 12: Authorizing FBI to Obtain Consumer Reports on Persons Believed to be Agents of Foreign Powers and Authorizing FBI Access to Subscriber Information of Persons with Unlisted Numbers who Call or are Called by Foreign Powers or Agents of Foreign Powers.

The ACLU opposes the proposals in Sections 11 and 12 of the bill to amend federal law to grant the FBI additional national security letter exemption authority to obtain credit records and telephone subscriber information of non-Published telephone numbers.[10]

The proposed exemptions 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. This drastic departure from the current procedures set forth in federal privacy protection statutes would give the FBI virtually unchecked power to obtain personal information on individuals.

The FBI has sought the authority to obtain these records for several years without success, and is currently pressing to have the same national security letter exemptions attached to the 1991 Intelligence Authorization Bill. The ACLU has consistently opposed granting the FBI this power and our concerns remain the same as we have previously expressed. In enacting privacy laws, Congress sought to protect the significant interest individuals have in personal, sensitive information held by others. The FBI has failed to demonstrate an adequate need for undermining these protections.

Section 11 would amend the Fair Credit Reporting Act to 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 information without following the statutorily prescribed procedures.[11] Absent such a showing, this highly personal and sensitive information should not be added to the narrow category of records subject to the national security letter exemption.[12]

In section 12, the FBI seeks to expand significantly the existing national security letter exemption to the ECPA. If this section is enacted, the FBI would be able to obtain subscriber information on all persons with *non-published* telephone numbers who call or are called by someone the Bureau has "reason to believe is an agent of a foreign power." The ECPA currently gives the FBI authority to obtain information in these circumstances only where the subscriber has a published or listed telephone number. But as recent court decisions have recognized, an individual who affirmatively requests an unpublished listing is specifically protecting a greater privacy interest than that afforded other telephone customers.[13]

Past experience demonstrates the problems that may arise from this kind of access by the FBI. This Committee's 1989 report on the FBI's CISPES investigation noted that the FBI "field offices were randomly setting [sic: sending] out voluminous numbers of leads to identify subscribers to telephone numbers."[14] The Report then

---

[10] 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) for published telephone subscriber information.

[11] 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.

[12] In an April 10, 1990 letter to FBI Director William Sessions, Congressman Richard Lehman (D-CA), chairman of the House Banking Subcommittee on Consumer Affairs which has jurisdiction over the FCRA, suggested that the FBI's concerns could be addressed at an upcoming hearing on the overhaul of the FCRA. The FBI declined to participate at the June 12 hearing, and we are unaware of any request by the FBI for the Subcommittee's involvement in this matter.

[13] *See, e.g., State* v. *Butterworth*, 48 Wash. App. 152, 737 P.2d 1297 (1987); *People* v. *Chapman*, 36 Cal. 3d 98, 679 P.2d, 201 Cal. Rptr. 628 (1984).

[14] "The FBI and CISPES," Report of the Senate Select Committee on Intelligence, at 106 (July 14, 1989).

noted that the "FBI's excessive use of long distance toll records evidenced in the CISPES case has been curbed by [the ECPA] legislation enacted in 1986." [15] Although the proposal applies to non-published subscriber information and not to telephone toll records, we believe the proposal would undo a major element of the protection created by the 1986 Act. We are concerned that broader and easier access to non-published telephone subscriber information will result in a substantial growth in the number of FBI investigations of, and visits to, innocent persons who are not agents of a foreign power, but who simply communicate with foreign nationals, embassies and groups.

If the Committee believes that there is a legitimate need to expand the national security letter exemption in ECPA, the ACLU urges that the language of the amendment be changed to require a higher standard for access to non-published numbers: the FBI should be allowed access to the non-published numbers *only if* the Bureau has *probable cause* to believe that the foreign agent who called or was called from the non-published number is involved in clandestine intelligence or international terrorism activities.[16]

The enactment of sections 11 and 12 would dangerously expand the narrow category of existing national security letter exemptions, a step Congress has been hesitant to take. There are only two instances in which Congress has authorized the FBI, in counterintelligence investigations, to obtain information about individuals pursuant to a national security letter. In 1986, Congress passed the ECPA with a provision requiring electronic service providers to disclose subscriber information (published only) and long distance toll records to the FBI in response to a national security letter. The ACLU opposed the national security letter in ECPA, but understood it was a necessary price for securing new protections for electronic communications. That same year, in an amendment to the Right to Financial Privacy Act (RFPA) contained in the 1987 Intelligence Authorization Act, Congress required banks to provide customer records to the FBI in response to a national security letter.

Since then, however, Congress has been unwilling to grant the FBI additional national security letter authority. Two years ago, the FBI was unsuccessful in its efforts to obtain a national security letter exemption in a bill that would have created a federal right of privacy in library and video records. The section of the legislation intended to protect library records was dropped to avoid the exemption, and the Video Privacy Protection Act passed without the exemption. In addition, last year the FBI introduced proposals similar to those under consideration today. After concerns were raised by members of the Congress and the ACLU, the proposals were dropped.

These concerns demand that the proposed exemptions be adopted only after careful consideration and upon a fully developed record. The proposed national security letter exemptions would diminish existing due process and privacy protections. Before these proposals are enacted, the ACLU strongly urges that a full and separate hearing be held to address these concerns, to hear from witnesses who have objections, and to test the FBI's case for the exemptions. Additionally, any use by the FBI of the two current exemptions, and any others that may be adopted, should be subject to vigorous oversight.

XI. Section 13: Rewards for Reporting Espionage.

The ACLU has no position on the use of rewards for information concerning criminal activity.

XII. Section 14: To Provide for a Court Order Process for National Security Physical Searches Similar to that for Electronic Surveillance.

Section 14 of the bill proposes to amend the Foreign Intelligence Surveillance Act (FISA) to apply to physical searches conducted in the United States for intelligence purposes. The ACLU opposes this provision as it is drafted. 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.

---

[15] Id.

[16] Such a higher standard is not always required under the current definition of "agent of a foreign power." *See* 50 U.S.C. § 1801(b). In addition, we are concerned that the government is interpreting the current definition too broadly to include persons as "agents of a foreign power" based solely on their First Amendment protected activities. Our concerns are spelled out in the Appendix to this testimony.

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 extra-constitutional 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 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 conducting warrantless electronic searches and the Supreme Court's creation of a national security exception for electronic searches. However, we have always had doubts about some elements of the FISA and are troubled by its implementation.

Notwithstanding the FISA and the Supreme Court's position on warrantless electronic surveillance, 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 is simply outrageous. 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.

Thus, we do not think the FISA itself should be amended to accommodate physical searches, as the Jacobs' Panel has suggested. 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.

THE FOURTH AMENDMENT, WIRETAPS AND NATIONAL SECURITY

"It is familiar history that indiscriminate searches and seizures conducted under the authority of 'general warrants' were the immediate evils that motivated the framing and adoption of the Fourth Amendment." So stated the Supreme Court in *Payton* v. *New York*, 445 U.S. 573, 583 (1980). The Fourth Amendment, by requiring that the warrant "particularly describ[e] the place to be searched, and the persons or things to be seized," absolutely prohibits general searches under general warrants. For this reason, the ACLU believes that all electronic surveillance violates the Fourth Amendment because it necessarily constitutes a general search and cannot be particularized.

The Supreme Court, of course, has determined that electronic surveillance does not violate the Fourth Amendment, so long as minimization procedures are employed to meet the particularity requirements and notice is given after the surveillance to meet the notice requirement. *Katz* v. *U.S.*, 389 U.S. 347 (1967); *U.S.* v. *Donovan*, 429 U.S. 412 (1977).

But having applied the Fourth Amendment to electronic surveillance, the Court then upheld warrantless physical entry of a home in order to install an electronic listening device, when no other means are available. *Dalia* v. *U.S.* 441 U.S. 238 (1979). The Court upheld such warrantless entry as an exception to the Fourth Amendment involving "exigent circumstances"—in this case, analogizing it to the situation where " 'an announcement would provoke the escape of the suspect or the destruction of critical evidence." *Id.* at 247 (quoting *United States* v. *Donovan*, 429 U.S. 413, 429 n.19 (1977)).

Under the FISA, Congress retreated a step further and allowed the government to dispense with subsequent notice all together for electronic surveillance conducted for intelligence purposes: i.e., to collect positive foreign intelligence and foreign counterintelligence (including international terrorism) information. The ACLU believes that this failure to require any notice is unconstitutional on its face. Whatever argument may exist for its constitutionality vanishes once the government contemplates using the wiretap information in a criminal investigation or prosecution.

THE FISA WARRANT STANDARDS AND PROCEDURES

The FISA sets forth procedures by which the government must obtain a court order for electronic surveillance of foreign powers or agents of foreign powers for intelligence purposes; such an order functions like a warrant. While the ACLU thinks that the procedures for applying for and obtaining such a warrant before the Foreign Intelligence Surveillance Court (FISC) are acceptable, we continue to be troubled, as we were initially, by certain aspects of the FISA probable cause standard, as well as by the way in which the standard is being implemented, particularly when such surveillance is used for criminal prosecutions.[1]

We also believe that the FISA is unconstitutional in all cases to the extent that it does not require notice to the party being searched. It certainly is unconstitutional once a criminal case, or other deprivation of property, such as deportation, is contemplated. If a person is indicted based on the fruits of a FISA surveillance, he must be allowed to examine and challenge all the evidence being used against him, including the FISA warrant application, which forms the basis for establishing the admissibility of the evidence. The ACLU absolutely opposes the provision in the FISA allowing the court to make an in camera and ex parte determination of the legality of the warrant and the search at the request of the Attorney General. 50 U.S.C. § 1806(f), where the search or its fruits are used in a criminal prosecution.[2] A national security charge is no grounds for diminishing the fundamental rights of a criminal defendant. *See Abel* v. *United States*, 362 U.S. 217 (1960).

Nor should the FISA be used for criminal investigations. Rather, we believe that if and when the government begins to consider a criminal prosecution, it must end the FISA search and seek a warrant under Title III of the Omnibus Crime Control and Safe Streets Act of 1968. We believe that this was the intent of Congress and that any rule that provides greater leeway would raise serious constitutional questions.

Congress passed Title III in order to establish comprehensive procedures for all domestic law enforcement electronic surveillance; it requires that notice be given to the subjects of such surveillance within 90 days after the termination of the surveillance. 28 U.S.C. 2518(8)(d). The ACLU believes that Title III is still the only means by which the government can engage in electronic surveillance for criminal investigations, even for the crime of espionage. In the last decade, espionage prosecutions have increased dramatically. Nonetheless, FISA surveillance should not be used in the investigation and prosecution of such cases because its procedures and standards are meant for intelligence investigations, it denies the target adversarial review in open court of the warrant, and in some cases it authorizes searches without probable cause of criminal activity.

First Amendment Rights

Secret searches, whether electronic or physical, not only violate the Fourth Amendment, they can violate First Amendment rights as well. Free speech and association can be easily chilled through fear of unwarranted government surveillance. The Supreme Court made particular note of this in the *Keith* case, in the context of warrantless domestic security wiretaps:

National security cases . . . often reflect a convergence of First and Fourth Amendment values not present in cases of "ordinary crime." Though the investigative duty of the executive may be stronger in such cases, so also is there greater jeopardy to constitutionally protected speech. . . . History abundantly documents the tendency of Government—however benevolent and benign its motives—to view with suspicion those who most fervently dispute its policies.

407 U.S. at 313-14 (1972). The *Keith* Court went on to note that "[o]fficial surveillance, whether its purpose be criminal investigation or ongoing intelligence gathering, risks infringement of constitutionally protected privacy of speech." *Id.* at 320;

---

[1] In the attached appendix to this testimony, we state our concerns regarding the application of the FISA probable cause standard. We also oppose the distinction the FISA makes between U.S. and non-U.S. persons. We believe that the Fourth Amendment applies equally to all persons within the United States, including non-U.S. persons. The Supreme Court accepted this principle in the context of national security physical searches when it considered the Fourth Amendment appeal of a convicted Soviet spy. *Abel* v. *United States*, 362 U.S. 217 (1960). *See infra* at page 48.

[2] 50 U.S.C. § 1806(f) requires, upon affidavit by the Attorney General, that the court "review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted." We know of no instance where the Attorney General has not provided the affidavit.

see also U.S. v. *Ehrlichman*, 546 F.2d 910, 936 (1976) ("Citizens whose views are in opposition to the Administration's may be pursued [by the government] on the ground of some relation to foreign intelligence, although that is not in fact the case.") (Levanthal, J., concurring).

A person who meets the definition of agent of a foreign power—by, for example, giving political or monetary support to a foreign country or organization deemed to be engaged in international terrorism—could reasonably fear that his office, home, mail or even luggage was being searched without his knowledge, and, accordingly, might be forced to accommodate his conduct to ensure that personal or confidential information was not exposed. Such a chill is an unacceptable violation of basic First Amendment rights and cannot be justified in the name of national security. Moreover, the government could use the information it collects against the political interests of the target, in further violation of the First Amendment.

PHYSICAL SEARCHES

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)).

This right applies to all persons in all circumstances. While the Supreme Court has recognized that there are certain exceptions [3] to the warrant requirement, including "exigent circumstances," [4] allowing for warrantless entry, these exceptions do not erode the basic rule that a warrant is required, that it must particularly describe the place to be searched and the items to be seized, and that notice must be given for physical searches and seizures. Neither should "national security" erode that rule.

Knock, Notice and Inventory

The ACLU firmly believes that the Fourth Amendment prohibits searches without providing notice to the targeted party, regardless of the purpose of the search. The Fourth Amendment protects persons' "houses, papers, and effects, against unreasonable searches and seizures." With or without a warrant, when the government engages in the search of real and personal property, it must identify itself and announce its purpose to the inhabitants, and it must leave an inventory of any items seized. This principle finds its bedrock in statutory and common law.[5] 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., dissenting). Justice Brennan demonstrated through an analysis of British

---

[3] *See, e.g., Katz* v. *U.S.*, 389 U.S. 347, 357 & n.19 (1967).

[4] For example, "(1) where the persons within already know of the officers' authority and purpose, or (2) where the officers are justified in the belief that persons within are in imminent peril of bodily harm, or (3) where those within, made aware of the presence of someone outside (because, for example, there has been a knock at the door), are then engaged in activity which justifies the officers in the belief that an escape or the destruction of evidence is being attempted." *Ker* v. *California*, 374 U.S. 23, 47 (1963) (separate opinion).

[5] *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 a 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.").

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."); [6] *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).

We also maintain that the prohibition against the warrantless and unannounced seizure of papers protects against photographing them, even if no physical property is actually seized. The Fourth Amendment protects the privacy and sanctity of the home and one's papers. Taking photographs, or even just looking around, violates that right just as much as the actual seizing of tangible property.[7] 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.[8]

National Security Exception

Many would argue that there is no way to distinguish between electronic surveillance and physical searches for purposes of the Fourth Amendment, such that the same national security exceptions supported by the Court and Congress for electronic surveillance should apply to physical searches. We disagree. The loosening of Fourth Amendment standards for purposes of electronic surveillance should not in any way affect the clear and unambiguous standards well in place for physical searches and seizures.

The Fourth Amendment has protected electronic communications for only 20 years, but it has protected one's home and papers for 200, and its antecedents reach back almost another 200 years. As Judge Levanthal commented, the fact that "physical entry into the home was the 'chief evil' appreciated by the framers of the Constitution . . . argues strongly for the proposition that the safeguard against this chief evil is not to be whittled away on abstract grounds of symmetry, merely because the new evil of electronic surveillance was possibly subject to a national security exception when, in 1967, it came to be regulated by Constitutional doctrine." *U.S.* v. *Ehrlichman*, 546 F.2d 910, 937–38 (1976) (Levanthal, J., concurring) (citing *United States* v. *United States District Court [Keith]*, 407 U.S. 297, 313 (1972)).

When the Supreme Court incorporated electronic surveillance into the Fourth Amendment, 40 years after declaring the opposite, it fundamentally changed the principle on which the Fourth Amendment was based. The *Katz* Court declared that "the Fourth Amendment protects people, not places," 389 U.S. at 351, based on the notion that people had a reasonable expectation of privacy from governmental intrusion. Prior to that decision, Fourth Amendment doctrine focussed on protecting one's property from unreasonable searches and seizures. *See id.* at 373 (Black, J., dissenting). And a warrantless search was presumptively "unreasonable." *See, e.g., Coolidge* v. *New Hampshire*, 403 U.S. 443, 470–71 (1971). Notwithstanding the useful-

---

[6] 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).

[7] *See, e.g.*, the definition of physical search in the "Attorney General Guidelines for FBI Intelligence Collection and Foreign Counterintelligence Investigations," sec. II.Q (as amended, Sept. 4, 1989) ("PHYSICAL SEARCH: any physical intrusion into the premises or property (including examination of the interior of property by technical means) or any seizure, reproduction or alteration of information, material or property).

We note that in a recent opinion, with which we do not entirely agree, a 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 seven days. *Id.* at 2610.

[8] *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."

ness of constructing the reasonable expectation of privacy test in order to bring electronic surveillance within the protection of the Constitution, we maintain that there is still an absolute prohibition against unreasonable governmental intrusion into one's house, papers, mail, or luggage, and that the Fourth Amendment continues to protect that right from warrantless and unannounced searches, without regard to the privacy interests in the particular instance.

The Supreme Court has never even hinted that it would accept 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 (1960). Rudolph Ivanovich Abel, a KGB agent, had come into the United States illegally in order to operate as a Soviet spy. While ruling that the fruits of the warrantless search could be admitted into evidence as incident to a valid deportation arrest, and thus not obtained in violation of the Fourth Amendment, the Court refused to consider the possibility that a different Fourth Amendment standard, let alone that any kind of exception, should apply because the case involved national security. As the Court noted parenthetically: "(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.)" *Id.* at 219-20.

Since *Abel*, a body of case law did develop suggesting a national security exception to the Fourth Amendment; but most of those cases concerned electronic surveillance and have since become moot upon enactment of the FISA. There is only one case in which a court of appeals upheld a national security warrant exception for physical searches. In *U.S.* v. *Truong*, 629 F.2d 908 (4th Cir. 1980), *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. 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 gathering criminal evidence, as it did, then a warrant was required. For this reason, the court upheld the suppression of the fruits of a third package search that occurred after the shift in purpose occurred. The Supreme Court declined to rule on the matter.

The ACLU, however, 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. 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.

Inherent Presidential Power

We also flatly oppose the Executive branch's contention that the President has inherent power to conduct warrantless national security physical searches. While we believe that the Fourth Amendment on its face prohibits such searches, at least one court has suggested that the normal Fourth Amendment constraints may not bind the President in national security cases. *Truong, supra.* However, this decision was made in the absence of any specific statutory restrictions on such conduct. *See Youngstown Sheet and Tube* v. *Sawyer*, 343 U.S. 579 (1951). Whatever inherent foreign affairs power the President may have to deal with foreign countries, the framers would be astounded at a claim that that power includes the right summarily to abrogate the protections of Americans in their homes or with respect to their papers as guaranteed by the Bill of Rights.

Nor does the President's power override Congress's power to legislate in this area. The door opened by the courts to the President for national security wiretaps was forthrightly shut upon passage of the FISA. Similarly, Congress can squelch the President's claimed power to search without a warrant by legislating appropriate restrictions.

New Legislation

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. 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.

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. We understand that very few warrantless physical searches are currently conducted. 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.

In conclusion, Mr. Chairman, we view the Jacobs Panel report as a basis for forging a consensus on legislation which would improve our counterintelligence efforts while at the same time enhancing civil liberties. We look forward to working with the Committee toward that result.

APPENDIX

FISA Definition of "agent of a foreign power" is overbroad under the Fourth and First Amendments because it does *not always require probable cause criminal activity.*

The ACLU is concerned that the definition of "agent of a foreign power" in FISA is being interpreted to include U.S. persons who engage in entirely peaceful and lawful political activities in support of foreign political groups that may engage in both lawful and terrorist activities. The effect of this application of the statute is that surveillance is then conducted on such persons based on their protected First Amendment right of political dissent, without the requisite probable cause to believe that they have engaged in criminal activity. Such surveillance violates both First and Fourth Amendment guarantees.[1]

Two parts of the statutory definition of "agent of a foreign power" give us concern. First, the statute defines agent as a person who "knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power," 50 U.S.C. § 1801(b)(2)(C), or who "aids or abets any person in the conduct" of such activities. 50 U.S.C. § 1801(b)(2)(D). These definitions apply to all persons within the United States including citizens and permanent residents.

We believe that the Executive branch interprets this definition as applying to persons who engage in fund-raising or other political activities in support of foreign groups labeled terrorist by the United States, even when there is no probable cause to believe that such persons have the specific intent to further the unlawful terrorist aims of the group rather than other lawful aims.[2] Such application of the statute is inconsistent with its intent and would be unconstitutional. The Constitution protects membership in, and political activities in support of, an organization that advocates violence, even when directed to the violent overthrow of the United States government, unless a person has the specific intent to further the unlawful aims of the organization. *See Healy* v. *James*, 408 U.S. 169, 187 (1972); *Keyishian* v. *Regents*, 385 U.S. 589, 607 (1967); *see also, Communist Party of Indiana* v. *Whitcomb*, 414 U.S. 441, *reh'g denied*, 415 U.S. 952 (1974).[3]

Nevertheless, we believe that the executive reads the phrase "activities that are in preparation" for terrorism in the statutory definition of agent as including just such protected activities. Instead of applying a specific intent test—that is, reading FISA as requiring probable cause to believe that a person is engaging in fund-raising or other political activities with the specific intent to further *terrorist* activities—the executive presumes that such fund-raising or other political activities are

[1] The statute requires "probable cause to believe that the target of the electronic surveillance is . . . an agent of a foreign power." 50 U.S.C. § 1805(a)(3). The requirements of the Fourth Amendment are satisfied only if the facts establishing a person as an "agent of a foreign power" include probable cause to believe that she has engaged in criminal activity.

[2] Our belief is based in part on the government's FISA wiretapping of people who support Palestinian causes, apparently without any probable cause to believe they have been or are about to be engaged in any criminal activity, or that they have any specific intent to further the unlawful aims of any organization.

[3] First Amendment protections apply to aliens living in the United States as well as to citizens. *Kwong Hai Chew* v. *Colding*, 344 U.S. 590, 596 n.5 (1953) (First Amendment does not "acknowledge any distinction between citizens and resident aliens"); *American-Arab Anti-Discrimination Committee* v. *Meese*, 714 F. Supp. 1060 (C.D. Cal. 1989) (appeal pending).

in support of terrorist activities.[4] We are concerned that the First Amendment proviso in FISA does not prevent such a position because it is too narrow and, in any case, is ignored.

The proviso states that a U.S. citizen or permanent resident cannot be considered an agent of a foreign power "solely upon the basis of activities protected by the first amendment to the Constitution of the United States." 50 U.S.C. § 1805(a)(3)(A). We are concerned that the executive reads this protection of the First Amendment rights of citizens and permanent residents too narrowly. Specifically, the government appears to take the position that the First Amendment simply does not protect even lawful political activities in support of a foreign terrorist group. Rather, it asserts that acting on behalf of a foreign power is not protected by the First Amendment, even if such acts consist entirely of writing and speaking. *See Palestine Information Office* v. *Shultz*, 853 F.2d 932 (D.C. Cir. 1988); Government's Motion to Dismiss in *Atkins* v. *Baker*, C.A. No. 89-1940 (D.D.C.). The government also asserts that, in any event, all fund-raising in support of any political organization that engages in terrorist activity is unprotected by the First Amendment. *See* Letter from Joe D. Whitley, Acting Associate Attorney General, to Congressman Barney Frank, at 2 (April 17, 1989) setting forth the Administration's position on the proposed terrorism language in H.R. 1280, the "Immigration Exclusion and Deportation Amendments of 1989."

In addition, this language, on its face, fails to protect against the application of such an unconstitutional presumption to persons who are in the United States, but who are not yet permanent residents—for example foreign students, who may have lived here for a number of years and intend to apply for permanent residency. Despite the limitation in the statute, such non-U.S. persons are also entitled to Fourth Amendment protections. *See, e.g., Almeida-Sanchez* v. *United States*, 413 U.S. 266 (1973); *Au Yi Lau* v. *United States Immigration and Naturalization Service*, 445 F.2d 217, 223 (D.C. Cir.) *cert. denied*, 404 U.S. 864 (1971).

The consequence of such a crabbed reading by the executive is that citizens in this country who engage in fund-raising and other political activities in support of an organization labeled terrorist, like the PLO, may be deemed "agents of a foreign power" within the definition of FISA, even if there is no probable cause to believe that the individual citizen has a specific intent to further the unlawful rather than the lawful aims of the organization. Electronic surveillance under FISA of such persons is a violation of both the First and Fourth Amendments. However important it is for the government to have information about such organizations, it is equally important that individual rights be respected.

The second part of the statutory definition of "agent of a foreign power" that gives us concern is the part concerning a person who "acts in the United

---

[4] At least one court has held that such a reading of the statute would be incorrect. In *United States* v. *Falvey*, 540 F. Supp. 1306 (E.D.N.Y. 1982), the court upheld the constitutionality of FISA only because it found implicit in the agent of a foreign power definition a requirement that the target is herself engaged in international terrorism, or is conspiring with or knowingly aiding and abetting those who are.

Such a reading of the statute would also be contrary to the legislative history. Recognizing that "one man's terrorism may be another's holy war," *United States* v. *Falvey*, 540 F. Supp. 1306, 1314 (E.D.N.Y. 1982), Congress was very explicit that FISA surveillance could not be based on association with unpopular groups or even advocacy of violence:

[T]he advocacy of violence falling short of incitement is protected by the first amendment, under the Supreme Court's decision in *Brandenburg* v. *Ohio*, 395 U.S. 444 (1969). Therefore, the pure advocacy of the commission of terrorist acts would not, in and of itself be sufficient to establish probable cause that an individual may be preparing for the commission of such acts. . . .

S. Rep. No. 604, Pt. 2, 95th Cong., 2d Sess 28-29, *reprinted in* 1978 U.S. Code Cong. & Admin. News at 3997. The report continues:

The committee does not intend that information concerning pure advocacy of violence should be completely excluded from consideration by the judge in making such a probable cause finding, if facts regarding other activities not protected by the first amendment, such as the purchase of a weapon, are present. Activities not protected by the first amendment, however, must be the primary basis for the probable cause finding. . . .

1978 U.S. Code Cong. & Admin. News at 3997.

The legislative history also confirms that association with foreign groups, even terrorist groups, is not sufficient grounds by itself for surveillance:

In no event may mere sympathy for, identity of interest with, or vocal support for the goals of a foreign group, even a foreign terrorist group, be sufficient. The terms "involve" and "will involve" are intended to encompass activities directly supportive of some act of terrorism, *e.g.*, the purchase or surreptitious importation into the United States of explosives for use in a terrorist incident, or the planning for an assassination.

S. Rep. No. 604, Pt. 1, 95th Cong., 2d Sess. 24, *reprinted* in 1978 U.S. Code Cong. & Admin. News at 3926.

States . . . as a member" of a "group engaged in international terrorism or activities in preparation therefor." 50 U.S.C. §§ 1801(b)(1)(A) & 1801(a)(4). This definition applies only to persons within the United States who are neither citizens nor permanent residents. As explained above, these persons are nevertheless entitled to constitutional protections. This definition on its face is overbroad and unconstitutional because it covers mere membership in an organization with both lawful and unlawful ends without being limited to membership with the specific intent to further the organizations unlawful ends. For example, the definition would permit surveillance of persons within the United States simply on the basis of mere membership in the PLO or the FMLN. Again, as explained above, such surveillance would violate both the First and Fourth Amendments.

The overbreadth of these portions of the definition of "agent of a foreign power" is a problem that Congress rather than the courts may have to remedy. Our concern is that individuals subject to unlawful surveillance will be unable to challenge the lawfulness of the surveillance in court. Such persons will likely never be notified that they have been subject to surveillance. Even if they are notified, they probably will not be allowed to examine the surveillance application, order, or even the fruits, because the Attorney General in almost all cases files a claim of privilege covering such documents pursuant to 50 U.S.C. § 1806(f). As a consequence, no adversarial challenge in court is possible and thus the usual judicial check on and enforcement of these constitutional guarantees do not exist.

TESTIMONY OF MORTON H. HALPERIN, DIRECTOR, WASHINGTON OFFICE, AMERICAN CIVIL LIBERTIES UNION

Mr. HALPERIN. When we start to prepare testimony in my office, the computer automatically produces a sentence which begins with the words, "I very much appreciate." But I want to say in this case that it is not merely rote. We do very much appreciate the fact that this Committee has recognized that these matters involve balancing civil liberties concerns against national security concerns and has sought our views on these issues and on other matters over the years.

What I would like to do is to focus on the comments that are contained in the introductory part of my statement which deal generally with the approach and basic principles that seem to us to underlie the Jacobs Panel and our own views on this subject. I want to make just a few comments at the end about a few of the specific recommendations, but since you have those in our prepared statement, I think it might be more useful to respond to any questions that you may have about our recommendations.

Since 1985, the ACLU has been making clear its belief that the counterintelligence activities of the United States can and should be reformed to deal more effectively with the real problems of counterintelligence. And it is our view, and continues to be our view, that that can be done without jeopardizing civil liberties.

And so we were encouraged by the formation of the Jacobs Panel and find much to commend in its approach and its activities. And we recognize that they did seek to strike a balance between national security and civil liberties. At the same time, perhaps because they did not choose to consult with us, we do not think they struck precisely the right balance. While there are many things in the report that we can support, there are some items which we cannot accept. There are others which we think are more appropriately a part of a more balanced set of proposals which we think and would urge the Committee to adopt. So let me just then touch on some of the basic principles that are in the report and with which we agree.

The first fundamental insight relates to why people spy and when they decide to spy. It is economic motives and job dissatisfaction and not ideology which seems now to lead people to espionage. Moreover, people become spies generally after they have obtained a clearance and they do not decide to spy and then try to get into the Government in order to be able to spy.

Thus, the focus should be on economic incentives and job dissatisfaction and not on ideology or other extraneous factors. And the present system which focuses the great bulk of its resources on the preliminary decision to give a clearance needs to be altered so that you give equal emphasis to the periodic review of people who are in particularly targeted positions. Those are common grounds on which I think we agree with the Committee—with the Panel's recommendations.

We think the Panel does a good job of telling the Intelligence Community where it ought to go. What it does not do is to tell the Committee where it ought not to go. We think it is necessary to do that for two reasons. First, we think there continue to be serious civil liberties violations arising out of the fact that the counterintelligence effort continues to be devoted to the wrong areas. And second, we think that if you are going to redirect the bureaucracy, which is a very difficult thing to do, you need not only to tell them what you want them to do, you need to also tell them what you do not want them to do. We think that, therefore, the legislation ought to redirect the energy towards greed or job dissatisfaction and away from two areas where it continues to be focused for reasons which, whether they ever made any sense, no longer do.

One is so-called left political ideology. The Government has gone back to asking people whether they are members of the Communist party. Although what "Communist party" and what "Communist" now means is of course becoming increasing difficult to understand.

The Intelligence Community continues to be focused in areas that we think are inappropriate on gay men and lesbians. We do not think that questions like that should be asked. Now that does not mean that we don't think in a particular case you should be allowed to ask people what organizations they belong to or what kind of sexual practices they have. But we think you should not single out left orientation rather than right or heterosexual activity from homosexual activity. Rather the question should investigate only if there is a nexus between political beliefs and possible spying or between sexual behavior and possible blackmail and possible spying.

A second issue that is raised by the Panel where again we agree with their basic thrust is that you cannot focus the counterintelligence effort on everybody with a security clearance. Too much information is classified. Too many people have security clearances for that to work. And while we agree with Senator Metzenbaum's observation that we ought to try to find a way to cut back on both the amount of information and on the number of clearances, we don't think you should wait to do that before you move forward with this effort.

So we think again that they go in the right direction. But we don't think that they go far enough. Because the number of people with TOP SECRET clearances is simply too large and too unfo-

cused to be the basis for this. So what we suggest is to limit it to those designated special compartmentalized intelligence clearances where the head of that program thinks that the people in his program or her program are likely to be targets of these counterintelligence efforts. This would obviously include people in communications and intelligence activities. It might not in some other special access programs.

There is also the question of whether anybody who just has a TOP SECRET clearance should be covered. What we suggest is that that should be done only in exceptional circumstances where the head of the agency determines that particular individuals who have just TOP SECRET clearances are likely to be, for special reasons, targets of a counterintelligence investigation.

I also might add that, as Mr. deGraffenreid notes in his testimony, there is a more fundamental problem. The Government does not do strategic risk assessment. It does not ask which of all the information that we keep secret is likely to be targets; who has access to that information; and what are the particular vulnerabilities of those people: is it physical security, is it communications security, is it recruitment, is it some other problem? That kind of risk assessment I think badly needs to be made. I have been advocating that in a number of things that I have written. And it is a very difficult thing to make the bureaucracy do. But it is something it seems to me that is absolutely essential.

Now, we agree with the Panel that the end of the Cold War abroad does not mean the end of the need for intelligence. Indeed, we think the case can be made that the intelligence budget ought not to decline proportionally with the defense budget. And that leads us, by the way, to believe that you ought to consider making the intelligence budget public. Because if it is kept secret, it's going to be cut proportionally because they are going to be cutting programs not knowing it's the intelligence budget. We have long advocated making the budget public, but I do think that the time has come to consider doing that.

More generally, we think that as the Cold War ends abroad, and the President announced that the Cold War was over, that we need to consider whether a variety of different restrictions that Americans accepted in the past in the name of national security before the Cold War, because of the Cold War, are still necessary and appropriate. And we think one of those areas is, as I've said, the question of whether so much information needs to be classified and so many people need security clearances.

As Senator Specter has brought out, our view is that people who are denied security clearances are entitled to appropriate due process. We are concerned that a previous draft of an administration executive order, I guess the last Administration and not this one, took away due process standards. And we would urge the Committee to include those in legislation while recognizing that there may be need for a deviation in extraordinary circumstances in particular agencies.

There's one assumption of the Panel, Mr. Chairman, with which we profoundly disagree, at least insofar as I understand what they are recommending, and that's the emphasis on future economic and industrial espionage. We recognize that economic intelligence

has become more important and we have no difficulty with the Intelligence Community being tasked to collect more economic intelligence information. But we do have two sets of problems. One has to do with the danger that if you task the Intelligence Community to collect foreign intelligence information, they will seek it where the light is good, where it is easy to do. And that is from American business firms rather than from foreign governments. Since many American business firms have a lot of information about foreign business that they do not desire to share with the American Government—and we think have a right not to share with the American Government—I think there is a real danger that if you turn the Intelligence Community loose and say find out what you can about foreign business, they will start or expand spying on American business because that is the best way to find it out.

We are also concerned with the notion that somehow these procedures ought to be used to protect information that American business has as against foreign intelligence services. We do not think it is the business of the American Government except for providing secure communications systems—which sometimes we don't do for other reasons related to NSA's concerns—but except for that, we do not think that the U.S. Government ought to be in the business of using security clearance procedures and counterintelligence investigations to protect the business secrets of private industry.

Chairman BOREN. Let me interrupt you on that point so I understand what you are saying.

Let us assume that you have a private American company that has included in its production some very, very sensitive, highly technical item that only exists in that company and only in the United States. And we learn that, not a foreign company, but a foreign country's intelligence service is engaged in practicing espionage against that American company. Are you saying that we should take no action if we——

Mr. HALPERIN. No. You certainly should tell them. And of course there are many cases in which it would be appropriate to classify the information. And indeed as you know, there are even procedures which we think should be used only sparingly to classify information that isn't developed with Government funds.

What we don't think should happen is that this should become a focus of activity of the Intelligence Community. So that you start requiring security clearances from people in private industry.

Chairman BOREN. No, I understand. But you wouldn't object to us, for example, using our intelligence sources in other countries to learn about the fact that a government of a foreign power was spying upon an American business.

Mr. HALPERIN. No, not at all. But as you know, Mr. Chairman, in fact, Senator Moynihan has complained many times publicly that the Government does just the opposite. That when we learn about such spying, we don't tell the business firms about it because we are trying to protect intelligence sources and methods.

So, I think that's more likely to be the problem and our view is that you should tell them if you find out. If the American Government knows that a country is intercepting the telephone conversations or TELEX messages of an American business firm, we cer-

tainly think the Government should tell them that. The problem as I say is that it doesn't tell them that now, not that it does, but we are concerned about providing a rationale for a whole new set of investigations.

Chairman BOREN. I understand what you are saying.

Mr. HALPERIN. And, therefore, we would urge this Committee to look very closely at this process. Just one more point on that. We do think that the only information you ought to protect is information relating to national defense.

Let me just take two specific comments on the specific proposals and then I'll be done.

One, on the financial records. Let me just point out, the distinction that we try to make between the reasonable suspicion standard and the probable clause standard, the probable clause standard does not relate to the person whose phone number the Government doesn't know. What it relates to is the person who has made the call to that phone number.

And what we are saying is that you should not be able to get the phone number of the unlisted person unless the person who, as we say in the testimony, the foreign agent who called is involved in clandestine intelligence activities or international terrorism activities.

Chairman BOREN. I see. So in other words, if they call an officer at the Embassy who is not suspected of being a spy but is simply the passport control officer, the visa granter or a commercial officer who really is a commercial officer, that's where you would apply the probable cause.

Mr. HALPERIN. Right. But we are concerned not only about the commercial attache. The Government, for example, at one time as you know was conducting a counterintelligence investigation of CISPES.

Chairman BOREN. Yes.

Mr. HALPERIN. Now, as we understand the language that the Government is asking for, if somebody in CISPES called somebody else who had an unlisted number, the Government under the reasonable suspicion standard of their definition of agent of a foreign power could then get the unlisted number of the second person. And that's the concern that we have. We are saying that they should have probable cause that the target they are investigating is engaged in clandestine intelligence activities or terrorism, not the broader definition of agent of a foreign power before you can get the second one.

Let me just say about secret searches because that is the only area in which I think we have a fundamental disagreement with both the Jacobs Panel and with the Administration. Our view is that it is unconstitutional to do searches of—take the easiest case, the homes of Americans without probable cause to believe that they have committed a crime, without knocking on the door, without presenting a warrant, and without leaving a list of what you seized.

Now I think the easiest way I can describe it, Mr. Chairman, is to suggest to you that the American Revolution did not occur because the Attorney General to King George did not write himself a note saying that the American Revolutionaries are agents of the

French. But in fact that is what the current system suggests. It suggests that the general warrants which were one of the main causes of the American Revolution would have been OK if King George's Attorney General had written himself a note, which would have been as plausible as many of the judgments raised today about foreign power, that the Revolutionaries were agents of the French. We don't think that's what they had in mind. We do not think that there is a national security exception to the Fourth Amendment.

Now it is true that the Supreme Court when it brought wiretaps under the Fourth Amendment dropped a footnote which suggested that it did not decide the issue of whether a warrant was required, not the Fourth Amendment, but a warrant was required in national security cases. And out of that has grown this exception, national security treated differently for electronic surveillance. It is true there is the one *Trung* case in which physical searches were upheld by a single court. We think that decision was profoundly wrong. And our view is that this Committee far from legitimating these kinds of searches ought to tell the President of the United States and the Attorney General that the homes of Americans, the offices of Americans, and the sealed packages of Americans cannot be subjected to a secret search which the American never finds out about unless the Government decides to tell him.

Let me say, again, we appreciate very much the opportunity to testify. I'll be glad to answer your questions. And we'd be pleased to have an opportunity to work with the staff of the Committee to try to fashion a bill which we can support. We would very much like to be in a position to support legislation that deals with what we think is a real and urgent problem.

Chairman BOREN. Well, thank you very much. Let me say, I think you've raised some excellent, excellent points. And we appreciate very much the time you've already spent, you and your colleagues working with our staff, making suggestions in a very constructive way. And it's our desire in this Committee, and I know it will be the same in the Judiciary Committee, that we try to strike this balance in the right way.

I certainly agree with many of the comments you've made and in the focus, the misdirection of a lot of our clearance procedures at the present time and the fact that we also have too many clearances, too much classified information. And that in light of the shifts in the world, the way we target our resources should certainly be dramatically changed.

Let me ask, on the last point you made about warrantless or secret searches as opposed to warrantless searches. Of course, what we are proposing here is that the practice of the Administration now be changed. At the current time, they do have a secret search electronically but it has to be approved by a court. They assert the right, as you know, to make a totally warrantless search, secret search, physical search. And, so in a sense, we would be constraining what they now claim they have the right to do by saying no you can't have any secret search, physical or electronic, without a court order.

But I gather your point of view would be that you would rather be able to take on that question of the constitutionality of their

point of view on physical searches rather than have us in a sense tighten it up but still allow secret search even with a court order. Is that a correct interpretation?

Mr. HALPERIN. That's right. We've been frankly looking for a client for this case. And we'll test that one of these days.

But our view is that what the Administration is prepared to accept is in our view so clearly unconstitutional that even though, as you say, it would put some limits on what is now being done, we think it just doesn't pass muster.

Chairman BOREN. Right.

Mr. HALPERIN. And we say that reluctantly because we should like to put some limits on this. But we just don't think that what they propose is anywhere near——

Chairman BOREN. You'd rather continue to leave that in an area where you are doing battle with them on the constitutional point? At least for now.

Mr. HALPERIN. We continue to hope that we will persuade the Congress that you ought to stop it which will then get the Administration in here in a serious negotiation.

Chairman BOREN. What about the question of the uniform standards? I gather you really don't have a problem with the concept of uniform standards?

Mr. HALPERIN. No we're for them. We support legislated uniform standards.

Chairman BOREN. But you think that in terms of some of these provisions, it should be limited only to those most sensitive and not all TOP SECRET clearances. We, by various estimates have seven or eight hundred thousand people with TOP SECRET clearances. What if it ends up we have three hundred thousand people in compartmented programs. Does that create a problem for you?

Mr. HALPERIN. What I suggest in the testimony is not all of them either. I would leave it to the head of each one of those programs to decide whether the reason there is a special compartmented program is one that is likely to make them in fact a target for the investigation.

It is also, at least when I had such clearances, which was a very long time ago, there were sub-categories within each of those and one could have easily imagined some people who had special compartmentalized intelligence to read the product of a particular collection system were unlikely to be targets as compared to the people who had access to the procedures for collecting.

Mr. Kampiles, for example, must have had access not only to the first level of clearances related to satellite communications, but to the second or third level because he had that manual. I never saw that manual.

So that I would say not everybody who has a particular special compartmentalized clearance is likely to be designated by the head of that program as a likely target of a counterintelligence investigation.

Chairman BOREN. Right. I think that you are right in terms of constraining it. It's not only a matter of trying to hold to a minimum interference with personal privacy but it's also a very practical matter that you only have so many resources. You can only target your attention on so many people and it would be better to

constrain the number of people and do an effective job with those that are really and truly in sensitive positions.

Mr. HALPERIN. It's really for both reasons. I mean because we are concerned with trying to catch the spies as well.

I think the point is, if you focus this on the people who are really likely to be the targets, and I think to really do that you need to do what's been suggested in the testimony that you are about to hear—you really need to do a more fundamental estimate than the sort of crude method which the Panel suggested and which I've suggested an elaboration on.

But the point is you want to have people in this program really be people who people think might be the target so that they take their work seriously. Which nobody does now.

Chairman BOREN. Your concept of some sort of risk assessment in advance is a very interesting concept to me as well.

On the due process question, could you make a different case for those who are already Government employees? Is there a stronger reason to give due process? For somebody who is already an employee, working professionally and who is now suddenly terminated because they are denied a clearance as opposed to those that are attempting to get a clearance on the first entry.

Mr. HALPERIN. You can. I mean and our view is there ought to be some due process rights and some hearing rights in both cases. Although we certainly agree that if you are taking somebody's clearances away, the rights are much stronger and the process ought to be more elaborate.

Chairman BOREN. I noticed in your statement you mentioned the problem with the way the intent requirement is written in terms of the possession of espionage equipment. I wonder if you might just spell that out a little bit more in terms of the problem as you see it.

Mr. HALPERIN. It may be that it is OK. But I mean our sense is that it needs to be made very clear that the Government has to prove that the purpose that one had in having this equipment is to commit espionage. And our reading of that section did not satisfy us that that was completely clear.

Chairman BOREN. Well, we'd welcome any thoughts and specific suggestions you might give us in terms of how we might tighten that up even further. We do want to write that as narrowly as we possibly can and do the job.

I notice also on the question of stockpiling information at home or someplace else. As you know, some people have used it for various reasons as an insurance policy or maybe just an idea that well, I'm going to retire, I'll take this all home and if I run short of money later on, I can sell something. Some do it to protect themselves against historians miswriting what happened in a certain period or perhaps whistle-blowers use it.

You talked about making sure we do not cover those that are giving information; for example, whistle-blowers giving information to the press. It is sort of a delicate area. We do talk about sales of information as opposed to just simply transmitting information. That's meant to constrain this somewhat. But you seem to say you wanted a two week period maybe of unauthorized duration of holding documents at some insecure place. A non-authorized place.

Would this get the Committee in the problem of approving by implication, well, that's just fine for you to take TOP SECRET information or highly sensitive information and give it to the press. I'm very aware of the fact that often Government cloaks and sometimes even classifies information—when it doesn't have the national security reason—for the very purpose of preventing discovery or accountability to the press. I certainly feel that's always a danger that the national security cloak is wrapped around all sorts of skullduggery in an effort to keep it out of the hands of the press. But on the other hand there are sometimes situations where there's a very legitimate national security interest for preventing something from going forward. Very often the press exercises its own restraint, but occasionally you could have a situation where you have an irresponsible press given information that really is highly sensitive in the national security nature that they publish.

Mr. HALPERIN. Mr. Chairman, my recollection of this section is that it is not limited to cases where you sell the information but is simply taking the information and keeping it at home. Because, remember, the person has not yet formed an intent possibly to do it.

I think those are legitimate concerns. The problem is that as the Jacobs Panel recognized, if you start getting in the area of what kind of penalties you want to put on the disclosure of information to the press, that's a very different and very complicated set of problems. It's one that this Committee dealt with in the Agents Identities Protection Act and just that one narrow piece required many years.

And as I mentioned in our testimony, we did not oppose the section of that bill that related to the release by Government employees of the identities of covert agents. We objected very strongly to the part relating to people gathering information from public documents and publishing it.

But we were concerned that the definition of what had to be released be very narrowly drawn and that the press be protected against conspiracy indictments and so on.

So that if you are going to start getting into the area of leaks, I think you are into a whole set of very complicated questions. On the other hand, I think your point is right. You don't want to pass a statute that seems to suggest it's OK to take stuff home if you are going to give it to the press.

I also think that you have Mary Lawton's point that this puts lesser penalties on TOP SECRET information than on other information. I guess my view on reflection is that there's no way to write this that it's not going to raise so many different problems that it isn't worth it. And that whatever minor additional possibilities there might be of legitimate prosecutions, that this is going to raise so many different problems that I think I'd leave it out.

Chairman BOREN. Well, let us work with you on that because I understand exactly what you are saying. I'm not sure though that there aren't situations where this practice does not become so widespread. And very often people take things for commercial possibilities, particularly if they are leaving Government employ.

Mr. HALPERIN. But as you know, there are provisions that enable you to take that material but at least if you are a Presidential ap-

pointee, put it into the Archives of the United States and then have access to it.

Chairman BOREN. But of course that's not what people are doing. We are trying to cover a situation where they don't put it in some——

Mr. HALPERIN. No. I understand that.

Chairman BOREN. Where they are taking it home and may be using it as a savings account for future sale.

Mr. HALPERIN. Well, they are sometimes using it, and I must say, I've been involved in these situations where you get attacked by people after you've left for what they claim you said in the Government.

Chairman BOREN. I think if you can do that through an Archive access or something, that would be a——

Mr. HALPERIN. You can except the Government sometimes ends up telling you that you are not entitled to see your own material in the Archives.

Chairman BOREN. Maybe we can work around with these various——

Mr. HALPERIN. They've done that to me.

Chairman BOREN. Maybe we can work around with these various procedures. Maybe something positive on that end——

Mr. HALPERIN. We would be pleased to work with you on this. But I do think one piece of it which would be helpful is to extend to non-Presidential appointees, this ability to put your stuff away and then get access to it.

Chairman BOREN. Being able to defend yourself with it later.

Mr. HALPERIN. If you needed to defend yourself.

Chairman BOREN. I think that's a very valid point.

We have a problem. There's a vote on the floor and they are now down to about 4 minutes. I'm going to have to run over there and vote.

Senator Specter is coming back. Do you know if Senator Specter wants to ask questions of Mr. Halperin?

OK, if you wouldn't mind just waiting, then he will resume the questioning and then I'll be back. We're trying to stagger our voting but I will be right back and he should be here just momentarily.

[A brief recess was taken from 3:52 pm. until 4:09 pm.]

Senator SPECTER. The hearing will resume.

We regret the interruption.

Mr. Halperin, I join my colleague, the Chairman, Senator Boren, in thanking you for appearing today. And I may cover some of the same ground which Senator Boren covered because I was not here during the entirety of his dialogue with you.

Let me begin with the issue of the warrantless searches, and ask for your opinion as to whether warrantless searches ought to be covered in the Foreign Intelligence Surveillance Act.

Mr. HALPERIN. We think that Congress should prohibit warrantless physical searches. We think they are unconstitutional.

But we think that in the case of a physical search, especially of a home and especially of a home of an American, that the requirements of knock, of notice, and of leaving behind a list of what was seized are essential components of the Fourth Amendment require-

ments. And therefore we think that any bringing of physical searches under the FISA procedures ought to add those elements to the requirements.

Senator SPECTER. Well, as you know, the requirements under the Electronic Surveillance Act to give notice to someone who has been the subject of a wiretap were not included in the Foreign Intelligence Surveillance Act, because of the national security interests.

So, it is candidly doubtful that those provisions would be met. I'm not certain about it, but there would be those policy considerations against it.

Considering the likelihood of those, of that same policy being carried forward in the search and seizure issue, would you think that it at least provides some additional protection by requiring a warrant?

Mr. HALPERIN. Well, the problem we have is that if Congress does that, it is then authorizing those searches. And we think those searches are unconstitutional. And we do not think Congress should be in the business of granting authority to the Government to break into people's houses when they are not at home, search their papers, and leave no evidence behind that they've done so simply because they conclude that the person is an agent of a foreign power.

As you recall, in the prosecution of Colonel Abel, who as an agent of a foreign power if there ever was one, the Supreme Court was unanimous in its view that he was entitled to the full protection of the Fourth Amendment. And we simply don't think that the tradeoff of having the additional protection of a warrant is worth it for the Congress to be giving its authorization to this.

Senator SPECTER. Do you think Congress should stay out of it entirely, even though——

Mr. HALPERIN. No, we think you should prohibit it. We think you should prohibit searches unless there is knock and notice.

Senator SPECTER. Well, if we don't prohibit searches, would you prefer us to stay out of requiring judicial approval if we don't go as far as you would like us to go?

Mr. HALPERIN. Yes. We—this is not an answer I give you lightly. We have thought a lot about it and that is our firm and clear position.

Senator SPECTER. Why take a position which deprives at least one additional level of protection for the privacy interest?

Mr. HALPERIN. Because we think that there—that when we get the right case in court, and I mentioned to Senator Boren before, we have been looking for the right case—we think that the court is going to find it unconstitutional and we think there is some chance that the court's decision would be effected by the fact that Congress had made the decision to authorize those searches.

Senator SPECTER. So you think if the Congress provides for judicial review that might save the constitutionality?

Mr. HALPERIN. Yes.

Senator SPECTER. Isn't that a pretty good reason for the Congress to act?

Mr. HALPERIN. Well, yes. We think you ought to act to protect the Constitution. And we also, as I said to Senator Boren, we don't

despair in persuading you that you ought to prohibit these searches.

Senator SPECTER. Well, of course we should act to protect the Constitution. The only question that leaves open is how do you act to protect the Constitution? But when you say that with the Congressional enactment that might save the constitutionality of the warrant searches even though it does not provide the provisions you want.

Mr. HALPERIN. No I didn't—excuse me, what I said was the court might uphold it. And, as you know, Senator, the ACLU's view of what is constitutional does not depend on what the court says. Our view is that those searches would be unconstitutional. And we think a way needs to be found to stop them and that Congress should not be in the business of authorizing them.

Senator SPECTER. Well, I understand that the ACLU may not change its view of what the Constitution means just because the Supreme Court says so. There are a lot of other people who don't change their views on the other side, a lot of law enforcement officials who are unhappy with the Miranda decision. But the Supreme Court, under our system, of course makes the last statement on the subject.

Let me—that is, absent a Constitutional amendment. We haven't had any of those in this field.

Mr. HALPERIN. But also Congress, as of course you know, can provide greater protections than the court says is necessary under the Fourth Amendment. And it has done so, for example, in the Bank Privacy area where when the court said you can seize bank records, the Congress said no. You did the same thing with secret searches of news rooms. The court said it was OK. And the Congress, in our view, properly said even if the Constitution permits it, good sound public policy does not do so.

Senator SPECTER. Well, we were talking of course about what the purview of the Constitutional protection was. Of course, Congress can strengthen rights of privacy beyond what the Constitution requires. But in considering to have judicial supervision on a warrant, we are considering taking a step beyond what is now required. And I understand that you don't think it goes far enough. And that you would prefer that it not be enacted even though it is an additional protection of privacy. I'm still not quite sure why you come to that conclusion.

But let me move on to one final question because——

Mr. HALPERIN. Could I make just one point about that?

We think that the Government, the Executive branch, will do it much more often if Congress has authorized a warrant system, because they will then feel that they have the protection of that warrant against the possibility of both damage actions and other kinds of procedures. So we think the practical consequences will be that there will be more secret searches of the homes of Americans.

Senator SPECTER. I'm not sure you're right about that. The witnesses representing the Government today asserted very forcefully that they feel it is a matter of presidential authority, constitutional authority. They look to the same document you do, the Constitution, to find additional Executive power as opposed to rights under the 4th Amendment.

As I was starting to say, Senator Boren would like to conclude in just a minute or two, because we have an additional witness who has an early plane, and I would like to just touch on one other subject and that is the question of the death penalty. And I know the ACLU views generally, but let me just ask why we shouldn't have the death penalty where you have espionage, and you have an increasing trend of espionage cases for pay. In this application of the death penalty you do not have the kinds of concerns which have troubled the Supreme Court in Furman versus Georgia, for example, on discriminatory application. You don't have the question of unfair treatment for minorities as opposed to non-minority members. Here you have danger to an entire country that could result in many, many deaths. Why not provide for the death penalty, especially in espionage cases? Or the possibility of the death penalty.

Mr. HALPERIN. There are several problems. First of all, as you know, Senator, the ACLU believes that in all circumstances the death penalty is cruel and unusual punishment and should be unconstitutional. Second, we think there are specific problems of applying the death penalty in cases where there isn't a homicide, where there isn't a murder committed, where there is no death. But third and I think at a more practical level, people who commit espionage think they are not going to get caught. Nobody commits espionage thinking the worst penalty that I can suffer is life in prison. And as you know, several of these people have been sentenced to life in prison and several successive sentences so there is no possibility of parole. I don't believe that Mr. Boyce or Mr. Kampiles committed espionage because they said to themselves, the worst that can happen is three consecutive life sentences, but I can never get the death penalty. I think what they said to themselves is, this system is so loose and so sloppy that I am not going to get caught, and so I am going to sell these things and get some money.

So I would say that rather than get into what is a divisive and emotional issue for our society of the death penalty, the urgent task, and one that I commend the Committee for moving forward on, is to figure out ways to change the system so that when a Boyce or Kampiles thinks about selling a document, he says to himself, I am going to get caught, or there's a 25% chance I am going to get caught, and if I get caught I am going to get three consecutive life sentences. If he thinks he is going to get caught, I don't think he is going to do it. And the fact that you add the additional item of the death penalty I think is very marginal.

Moreover, unlike people who commit espionage for ideological reasons and who might conceivably go to their death rather than talk, I think it is absolutely clear that anybody who does it for money is going to agree to cooperate with the Government at some point, and one of the conditions of that is going to be that the death penalty is off the table. So I think as a practical matter it would not happen.

But I would say the most important point is is that it is certainty or very high likelihood of being caught that deters here and not the theoretical possibility that you might get the death penalty.

Senator SPECTER. Well, just a final statement because I know the Chairman wants to move on. I agree with you about the swiftness and the certainty as a deterrent, but I respectfully do not agree

with you about people not thinking about the death penalty. I think especially now as we see espionage motivated by ideological reasons to monetary ones, my own experience is that people do think about the consequences, and especially people who want to make crime pay and want to make espionage pay. And where you don't have a specific murder involved, I do not think that that line of cases is applicable here at all. There you are talking about no murder for rape, or no murder for a remote accessory in a felony murder. But where you subject many people to the risk of death and have a very prime societal interest as you do in espionage, I do believe that the constitutionality would be upheld. But I agree that we are not going to settle this today.

Thank you very much, Mr. Halperin. Thank you, Mr. Chairman.

Chairman BOREN. Thank you very much. Thank you, Senator Specter, for continuing on and thank you, Mr. Halperin, for some very, very helpful testimony.

Mr. HALPERIN. Thank you, Mr. Chairman, I very much appreciate it.

Chairman BOREN. Thank you.

Our next witness is Kenneth E. deGraffenreid who served as Director for Intelligence Programs at the National Security Council under the Reagan Administration. In this capacity he was responsible for developing and coordinating the counterintelligence and security policies for the Administration. As I mentioned earlier, since he left the White House, he has been affiliated with the National Strategy Information Center and has written extensively concerning improvements in counterintelligence capabilities.

And I know, Mr. deGraffenreid, that you need to be out of here in about 15 minutes, and so what I would like for you to do if you can is summarize, hit the highlights of your testimony. We'll put your entire testimony in the record. And then we will try to constrain our questions as much as possible to get you out in time to catch your plane. I apologize we have gone on so long, but it has been because of the interest in this subject and the caliber of the testimony we have received. We very much appreciate your inconveniencing yourself to come and take the time to be with us today.

[The prepared statement of Mr. deGraffenreid follows:]

PREPARED STATEMENT OF KENNETH E. DEGRAFFENREID

Mr. Chairman, it is an honor and pleasure to have this opportunity to speak with you today on the recommendations on security and counterintelligence made to you by the Eli Jacobs Panel and on S. 2726, the "Counterintelligence Improvements Act of 1990."

As one who began working on security and counterintelligence policy issues as a staff member on this Committee in the late 1970's (as Senator Chafee's designee) and who had responsibility for pushing security and counterintelligence reforms as director of intelligence programs on the NSC staff at the White House for most of the 1980's, I know firsthand how this Committee has carried the torch in this vital area of protecting the national security from the foreign intelligence threat. Over these years, the Committee has consistently kept energy and attention focused on reforming and improving the Nation's security, countermeasures, and counterintelligence capabilities. The Committee's interest has remained steadfast even when, on occasion, interest and attention has flagged within some quarters of the Executive branch.

While substantial progress has been made in improving these capabilities, this area of Government has proven particularly resistant to reform and to change, even in the face of a decade of strategically damaging espionage disasters. There is a seri-

ous question whether the progress we have made will be sufficient for the challenges of the coming decade.

Once again, the Committee is out in front in its willingness to consider the series of timely and, heretofore somewhat, contentious issues, which have been examined by the Jacobs Panel. The Committee has now given legislative form to these recommendations in S. 2726. It is particularly gratifying to see within S. 2726 many ideas which date back to at least the late 1970's and which, for many years, have badly needed to be addressed seriously.

I believe from a public policy viewpoint that the provisions of S. 2726 are eminently sensible, sound, and balanced, in keeping with our country's values, and will make a significant contribution to countering one very dangerous aspect of the foreign intelligence threat. Indeed, they are long overdue.

From the testimony of the Jacobs Panel before the Committee, it is clear that the proposals are designed to provide the Government with more effective tools to deter and detect spies and to aid in the prosecution of human espionage. By enhancing prosecutorial capabilities, the legislation would serve both as a security tool (in adding to the deterrence of espionage) and as an important counterintelligence tool because of the critical role successful prosecution plays in obtaining vitally needed damage assessments. Passage of this legislation would also send a powerful signal to the intelligence and national security communities of the continuing broad public support for this vital, but often unsung, work. I have specific comments on some of the provisions of S. 2726 to which I would like to return in a moment.

Key counterintelligence concerns beyond the focus of the Jacobs Panel

But first I have a few, more general, comments which I hope will be useful to the Committee as it considers this legislation. S. 2726 is focused clearly on several important improvements to detecting and deterring one damaging ingredient of the foreign intelligence threat to our national security—the Government or contractor employee with access to highly classified information who volunteers or is easily seduced into committing espionage.

However even while pursuing this needed legislation, it is essential to recognize that deterring and detecting this type of spy is but one part of the comprehensive systematic strategic security approach to the foreign intelligence threat which we will require in the decade of change and complexity which lies ahead.

Thus, as helpful as I believe the recommendations of the Jacobs Panel to be, it would be a disservice to leave the Committee with the impression that these legislative remedies are sufficient to counter the most serious of the foreign intelligence challenges we are likely to face. There are several reasons why this legislation, while necessary, is unlikely to be sufficient.

First, the Panel limited its inquiry primarily to those steps which would assist the Government in deterring, detecting, and prosecuting Americans who volunteer to committing espionage, particularly those motivated by greed. While these volunteer spies—Walker, Whitworth, Pelton, and others—have done grievous strategic damage to the United States, it is not clear that this is the only type of spy with which we have had to contend, or will have to contend, in the future.

The full set of human espionage cases over the past fifteen years indicates that while a majority were volunteers, others were "classical" recruitments. Some represent a complicated mixture of both. Nor were these volunteers only motivated by money: other motivations, such as disgruntlement with their job, disenchantment with their place in life, revenge, political sympathy, and emotional or psychological instability, seem to have been at work. It is difficult, for example, to conclude that greed alone was the motivation of William Kampiles who received only $3,000.00 when he sold a TOP SECRET satellite operating manual in the mid-70's. As yet, pending expanded research and analysis, we don't fully understand why people commit espionage.

Furthermore, we obviously don't know the motivation of those spies we have yet to uncover. I mention this obvious fact because a surprising number of the volunteer/venal spies analyzed by the Jacobs Panel were uncovered by means other than direct counterintelligence techniques (e.g., Walker was turned in by his former wife). It is at least possible that spies recruited on the basis of other motivations—ideology, blackmail, false flag operations, and the like—practice better "tradecraft" and could still be spying.

Secondly, the Jacobs Panel limited its examination almost exclusively to only one of the three variables in the espionage equation: the American who betrays his country. In fact, however, the foreign intelligence threat may be thought of as a system of sorts. It consists, to be sure, of the people in Government and industry charged in various ways with protecting strategic information from foreign collec-

tion, who are themselves vulnerable and subject to exploitation (the focus of the Jacobs Panel). But two other elements are involved as well: the foreign collection activities, including SIGINT and other forms of technical collection as well as human espionage, whose threat varies with level of effort and the degree of proximity to U.S. secrets; and the sensitivity and vulnerability of strategic information, programs, activities, and technologies on which the foreign collection efforts are focused.

If it can be said that the Jacobs Panel focuses on the vulnerability of people, the third variable concerns the nature and vulnerability of the information itself. How well the Government offers security to the information which it identifies as strategically vital to its interests (for example, TOP SECRET cryptographic or SCI information) is equally vital to its protection. This protection must proceed from a comprehensive understanding of both its degree of sensitivity and its vulnerability. Because this understanding is the sine qua non for an effective response to the strategic foreign intelligence threat, I believe that our shortcomings in this area are more damaging even than our difficulties in detecting the volunteer spy.

Finally, the threats we will face in the 1990's are likely to be far broader than we have seen even in the decade of the spy. As you know, Mr. Chairman, and as you and Directors Webster and Sessions have stated publicly, the foreign intelligence threat in the 1990's is increasing despite the lessening of tensions with the Soviet bloc. Add to this the threat to our strategic information, programs, and technology posed by others—friends as well as adversaries and former adversaries—who seek not just traditional national security secrets, but financial, industrial, and proprietary secrets of the private American economy.

While I believe that the Jacobs Panel proposals will be very helpful in detecting and countering the narrow, albeit damaging, aspect of the threat they have studied, the fundamental problems with American counterintelligence and security are not addressed by the Jacobs Panel recommendations. It is clear that much more needs to be done to address the changing threat and vulnerability environment of the 1990's. Unfortunately, these threats will encompass more than just the American who voluntarily sells out his country. To protect against these broader threats (to which I will return in a moment) will require a number of policy, resource, organizational, and "cultural" reforms which do not lend themselves necessarily to legislative remedies.

Of these broader reforms, I would like to raise one specific recommendation which I believe the Committee could support and foster. This recommendation picks up on a point made by Admiral Inman during presentation of the Jacobs Panel recommendations on May 23, 1990. Admiral Inman noted that prior to the Jacobs Panel review, the intelligence and security agencies had not gone through the past espionage cases in a systematic way with the objective of trying to understand lessons to be learned in detecting patterns of activity, especially where legislation or other reforms might make a difference.

This glaring oversight is indicative of perhaps the most serious deficiency in our capability to detect and counter the foreign intelligence threat: the Government doesn't do strategic risk assessment. By that I mean we lack comprehensive analytic capabilities to identify the vulnerabilities of our most sensitive data, combine the departments' and agencies' knowledge of the multidisciplinary threat, and, based on systematic analysis, thereby assess the risks involved to that information. Absent such a capability—a "brain" (or "brains") for the system—we have no way, purposefully and efficiently, to allocate scarce security and counterintelligence resources or coordinate their efforts to protect our most vital secrets.

I believe that correcting this deficiency is the single most important undertaking facing those charged, in the Congress and the Executive branch, with protecting the Nation's vital secrets.

A national counterintelligence and security assessment capability

In July of last year, the National Strategy Information Center co sponsored a conference of counterintelligence and security practitioners at the National Defense University to explore the requirements of a national counterintelligence and security countermeasures policy. Not surprisingly, the conference concluded that U.S. counterintelligence and security countermeasures today remain fragmented and incomplete in their defensive coverage against the threat. I chaired that conference and developed a number of recommendations based on its conclusions.

One key recommendation of the conference is the creation of dedicated analytic risk assessment and coordination capabilities within the national security community so the counterintelligence and security agencies can know which secrets and technologies to protect and can coordinate their efforts efficiently. These analytic func-

tions include many activities which are not currently performed or even, in some cases, assigned as a mission, or when performed, are not conducted from a coordinated national perspective. If this recommendation were implemented, the most sensitive U.S. secrets could be identified and prioritized. Their vulnerabilities assessed, the full range of threats analyzed, and the Nation's limited security resources deployed in a balanced, coherent, and coordinated fashion to reduce overall risk. With a "big picture" understanding of the lessons of past security failures, as well as the intelligence "signatures" of U.S. secrets, offensive counterintelligence operations at home and abroad could be tailored to interdict and neutralize hostile operations to compensate for the gaps in security and countermeasures effectiveness. The specific functions required for comprehensive risk assessment include:

—identifying and prioritizing the Nation's strategic secrets in each of the national security departments and agencies. The current implicit method for setting priorities—the classification system is woefully inadequate from a strategic perspective.

—identifing and analyzing the security vulnerabilities of vital secret programs, activities, technology, and information. Certain secrets are vital to our national security, we must understand the nature and location of their inherent vulnerabilities and security weak points.

—evaluating all dimensions of the hostile intelligence threat, including possible deception. Despite some progress in this area, there is still no place in the Government where all knowledge about the varied threats of the KGB and other foreign services is collected and analyzed.

—balancing vulnerability versus threat to determine the risk to each strategic secret. The management of security risk is a key ingredient of successful operations and programs. In the long run accomplishing objectives securely is the only effective and affordable way.

—coordinating strategic operational security, countermeasures, and counterintelligence analysis and operations at home and abroad. Despite some progress, the Government's efforts remain fragmented, incomplete in defensive coverage against the threat, and do not proceed from a common strategic plan.

—developing performance standards for and evaluating the effectiveness of these security, countermeasures, and counterintelligence efforts. Leaders in the Congress and Executive branch must be able to measure performance if they are to provide the necessary resources and political support to the counterintelligence and security community, which lacks a "constituency."

I have prepared a "model" of what such an assessment center might look like at the national level. While this is not the only organizational arrangement possible, it is a useful model with which to explore the concepts involved. I respectfully offer a copy of that analysis for the Committee's consideration.

Mr. Chairman, I hope the Committee will find occasion to fully and formally consider this proposal. I respectfully recommend that the Committee examine the organizational, budgetary, oversight, and policy guidance necessary to ensuring the performance of essential strategic risk assessment, both from a centralized national perspective, as well as at the departmental and agency level.

Mr. Chairman, let me offer two additional recommendations.

Moving to action on hundreds of reform recommendations

The "decade of the spy" revealed scores of cases of successful human and technical espionage against the most sensitive and closely guarded of the Nation's strategic information, programs, and technology. The total cost in dollars has yet to be calculated, but it certainly runs to tens of billions in stolen military technology, war plans, intelligence "sources and methods," cryptographic systems, and industrial economic losses. To this must be added "opportunity costs" and the expenses of building additional generations of weapons and intelligence systems to replace those compromised. And the financial loss may be the least of the damage—in some cases, it appears that U.S. western defenses could well have been negated had a war or crisis developed. The potential damage to U.S. diplomatic and negotiating positions may never be known. The weaknesses of American counterintelligence and security in preventing this damage have been well documented.

Over the last fifteen years a multitude of studies have been conducted and literally hundreds of recommendations amassed on how to counter various aspects of this threat through reform of our security, countermeasures, and counterintelligence capabilities.[1] The causes of past failures have been analyzed, and requirements for the future have been put forth by observers inside and outside the Government. The issues have been studied by this Committee and the House Permanent Select Committee on Intelligence in their series of reports as well.

However, despite the alarming and sustained nature of the losses and overwhelming consensus about the necessary reforms, this entire area of Government has proven distressingly resistant to change.

I would urge the Committee to take as its mission the development of a systematic implementation plan for the large number of these recommendations which are repeatedly made over the years and about which there is consensus (although little impetus within the bureaucracy). Some of these may involve legislation, as with the Jacobs Panel recommendations, but the vast majority involve mission definition, budget enhancement, and organizational improvement. Only a few are beyond the reach of the Committee.

As you have stated Mr. Chairman, "there is a formidable agenda for action. Many of the initiatives proposed in the mid-1980's by the Stilwell Commission, the Inman Panel, the Senate Intelligence Committee, and other experts have not yet been fully implemented." I believe the cumulative effect of even modest improvements in many of these areas would be to substantially improve security, easing the burden on counterintelligence agencies and inspiring the professionals who toil at these difficult tasks with regard to these many worthwhile recommendations, the task now is not further study but to move to action.

The new intelligence threats of the 1990's

Although we need to move to action on these long-standing recommendations, there is also need for detailed study of the coming threats of the 90's. I think it would be useful to single out, in particular, five of these broader threats, where I believe this Committee has a critical and, indeed, unique role to play.

Because the Committee's vision in creating the Jacobs Panel has already resulted in an obvious success, I strongly recommend that the Committee consider the creation of similar panels in each of these five areas. While this is no small workload, I believe that issues raised in considering how to respond to these threats are so important that they justify this level of effort and commitment. I also believe the Committee would have no trouble in finding a sufficient number of distinguished citizens to assist in this work.

The strategic security threat posed by on-site inspection of arms control agreements

Whatever their other benefits, the security dimension of these arms agreements for the U.S. and the Soviet Union will be asymmetrical. While the U.S. counterintelligence and security organizations and the national security communities have been able to cope with on-site inspection under the INF treaty, these efforts began belatedly and have not been cheap either in manpower or dollars. However, it is by no means clear that they have the resources and capabilities to provide the same degree of protection under the proliferation of treaty inspection sites which will encompass a wide variety of technologies and locations under various arms control treaties now under negotiation: START; a CW agreement; TTBT; PNT; CFE; "Open Skies."

There will be an expanding multidisciplinary threat from the hundreds of Soviet inspectors who will be introduced into some of the most sensitive U.S. facilities, representing an unprecedented challenge to relatively limited U.S. counterintelligence and security capabilities. Their primary mission will be collection on non-treaty related items: advanced U.S. technology and the elicitation of personal vulnerability data on key U.S. personnel. Geography, culture, the current easing of tensions with concomitant perception of reduced threat, and the scarcity of counterintelligence and security resources will assist the Soviets' work.

The Government has yet to decide on a comprehensive approach to identifying the strategically sensitive information, programs, activities, and technologies, which would be placed at higher risk because of on-site inspection. Such analysis, if supplied in a timely manner, could inform U.S. negotiating positions and be used to maximize U.S. advantages under on-site regimes while minimizing U.S. security risks. An essential requirement is for performing risk analysis which identifies and ranks the vulnerabilities of U.S. sites, as well as specific Soviet threats. A systematic process for counterintelligence and security at these installations will be required once treaties are ratified.

Without this knowledge, the U.S. might agree to inspection procedures which result in a sense of "false security" or which are overly protective of U.S. programs whose security is not further threatened by on-site inspection regimes. As a result, U.S. negotiators may fail to press the Soviets on necessary inspection procedures and limits, erroneously believing they are protecting U.S. systems.

Even if security priorities are understood, individual departments and agencies and the Government as a whole, lack systems for efficiently marshalling protection assets in a coordinated, efficient, and cost effective fashion. I mention efficiency be-

cause I think without a coordinated approach the Government could well wind up paying for a lot of "stupid" security. In some cases, security officers protect against the "wrong" threat—wasting limited resources and further jeopardizing the technologies and secrets to be protected. In other cases, lacking a comprehensive systematic "OPSEC" approach, telltale "signatures" remain exposed to Soviet collectors after all conventional security procedures have been taken.

The strategic security dimension of economic competitiveness

A second expanding threat is the foreign intelligence threat to American economic competitiveness. As you have pointed out, Mr. Chairman, "an increasing share of the espionage directed against the United States comes from spying by foreign governments against private American companies aimed at stealing commercial secrets to gain a national economic advantage."

In recent years, we have all come to recognize what has long been true: that the strength of the U.S. economy—the result of liberty and free enterprise—is a key element of our total national security. We also understand that national security allies are becoming economic competitors. Some have a "mercantilist" approach to international relations—their foreign policies are driven increasingly by the search for advantage for their commercial sectors and domestic economy. As DDCI Dick Kerr pointed out last April, many, if not most, industrialized nations spy against the U.S.—both the Government and commercial secrets—and share the strategic information they collect with companies in their own industrial sectors. Thus, many foreign corporations enjoy an advantage, and U.S. companies face a very unlevel playing field.

Because U.S. economic strength is directly attributable to our free market and the minimization of Government involvement in the private sector and because it would be contrary to our other values, I do not believe the answer to U.S. competitiveness lies in trying to mimic this mercantilist approach. Rather, the issue is how to level the playing field and encourage Government decisions which maximize both competitiveness and national security.

Some have proposed U.S. Government intelligence sharing with the U.S. private sector. Perhaps some kinds of information can be shared with the private sector. For example, a general technology database, accessed via subscription to the Commerce Department might be helpful as a clearinghouse function. But the answer is likely to be no to the sharing of secret intelligence (clandestine intelligence/SIGINT, etc.) with private U.S. companies for many reasons, including: security, fairness, legality and morality; to name but a few.

I believe that the playing field can best be leveled by a national effort to protect U.S. Government and commercial strategic secrets. While at first glance this seems the least compatible with the "American way," in fact, it would do the least violence to American values. However, many problems and issues must be addressed.

Balancing the importance of the "free exchange of ideas" with the need to protect some information from being proliferated in an uncontrolled way (recognized domestically in patents, copyrights, and proprietary information).

—the need for a process and capabilities in both the U.S. Government and the private sector to identify strategically vital information and understand its vulnerabilities and "signature."

—the appropriate role of the U.S. Government in providing security, countermeasures, and counterintelligence support to, or on behalf of, the private sector.

—the need for a national process to balance various intelligence and security equities as the U.S. Government attempts to remove obstacles to U.S. economic competitiveness.

The continuing threat to telecommunications and computers

A third area of threat for the 1990's, which I would single out both because of its potential for strategic damage and because of the particular difficulty we have had in addressing it, is the security and protection of our information system: telecommunications and computers.

The Government must ensure the absolute 100 percent security of the communications and computer systems which process classified information because these systems are the nerves that link together the rest of the national security system. Indeed, the Jacobs Panel correctly has focused a number of its legislative recommendations in the area of protecting our cryptographic integrity.

But, in studying the issue in the Reagan Administration, we also found that the less than 100 percent effective area of of our telecommunications and computers which process and transmit ostensibly unclassified information was also necessary and worthwhile (as opposed to the securing of classified information). Technical protection to the systems which communicate and process this information must be

based on an informed risk assessment which balances known and potential threats with actual vulnerabilities. The need for this protection owes to the telling fact that, in today's world, because of the power of machines to aggregate information and to sort, the most highly classified information can be gleaned from data that is, in fact, unclassified when taken in isolation. Here I am thinking of such vulnerabilities as Government telephone calls within the Washington, D.C. area or the accessing of large Government or commercial computer databases. This problem is exacerbated by the fact that the technology to exploit information systems has become ever cheaper and easier to access. The ability to glean this information is now readily and cheaply available, not just to the KGB, but to anyone who knows what to buy at Erol's or Radio Shack.

Much progress was made in the Carter Administration and early Reagan years in developing policies and capabilities for improving both security and protection of telecommunications and computer systems. Experience has shown that this protection function, which is aimed solely at preventing illegal acquisition of this information while it is being transmitted or processed, responds well to incremental improvements. Unfortunately, because of particular political and perceptual problems (which I believe were extraneous to the foreign intelligence threat issue), progress has been halted in this area. Indeed, there has, in my view, been some retrenchment.

Because of its special understanding of both intelligence and counterintelligence needs, this Committee is uniquely equipped to sort out these difficult policy and practical issues and to reenergize this vital security effort.

Threats from non-State run intelligence activities

The fourth threat I would single out for the Committee's attention is that posed by what political scientists might call non-State intelligence actors. Here I am thinking, in particular, about intelligence operations run against U.S. interests by terrorists, illegal narcotic traffickers, and other criminals. Increasingly, sophisticated intelligence operations being run by foreign and domestic drug traffickers threaten U.S. counternarcotics operations. At present, it appears that the Government lacks a comprehensive security doctrine, as well as many of the counterintelligence and security capabilities, needed to protect our counternarcotics operations. Here again the Committee is uniquely qualified to address this problem, because it understands the need for comprehensive security efforts and has experience with the difficult issues of the interface between intelligence information and information gathered for criminal prosecution, given its past work in FISA, and the Classified Information Procedures Act.

The continuing Soviet threat in a period of declining awareness and increased access

A fifth threat of the 1990's, which I believe requires special attention from the Committee, is, in fact, an old one. Mr. Chairman, you have been in the forefront of those cautioning that the tremendous changes we are seeing in the Soviet Union and particularly in Eastern Europe will place greater, not lesser, demands on U.S. intelligence. But I am concerned that in this era of warming relations, the Administration, the American people, and others in the Congress may come to believe that the Soviet intelligence threat, and indeed strategic intelligence threat, has disappeared. When coupled with the additional degree of threat in real terms which will result from the greatly expanded Soviet access to American society (particularly that threat directed against our high technology), and the continuing pressure on resources, we may find a counterintelligence and security community simply overwhelmed by the challenges they will face, despite the carefully developed reforms and enhancements of the past decade.

I am concerned that, as the overall national security budget is sharply reduced, cuts not be visited upon the security, countermeasures, and counterintelligence activities where, as we know, the threat, in reality, is increasing. An immediate example comes to mind. The number of investigators handling background checks for the Defense Investigative Service (D.I.S.) has been slowly built up in recent years directly as a result of the work of this Committee, concerned about the very real problem of reinvestigation (an issue addressed by the Jacobs Panel). Yet, I have heard that D.I.S. has been told to prepare for a 25 percent cut in its approximately 4,000 employees. After all of this painstaking work, and with the requirements increasing, I believe it would be the height of folly to allow a meat-ax approach to cutting the defense budget to damage this security capability, and put us once again behind the eightball on personnel security.

I am aware that the complexity of our budget process and the size and peculiarities of the bureaucracy often make it difficult to selectively protect such areas, but I believe that the Committee's understanding of how our capabilities are funded

give it grounds and opportunity to intercede on behalf of reason and protect, and where necessary enhance, the budgets of the security, countermeasures, and counterintelligence elements of the Government.

Further, Mr. Chairman, I also worry about a more insidious problem. That is the possibility that those in U.S. security and counterintelligence professions will see the lessening of restrictions on the flow of technology to the Soviet Union—e.g., COCOM control reductions—as a signal that American policy in this area is no longer seriously concerned with protecting our vital technology. If these policy changes are misconstrued as official indifference, those extremely sensitive and vital technologies which we have determined must be protected at all costs will be put at risk. There are a finite number of vital secrets in this democracy which are, relatively speaking, more precious strategically than may be the case with governments which have far more of them. Our deterrence, defense, and security depend on our keeping those secrets secure, even in times of lessened tension. It is important that those charged with their protection continue their effort even in a period of change.

I would urge this Committee to continue to make the case that despite the events in Eastern Europe, the foreign intelligence threat is not receding, but is increasing in quality, quantity, and breadth. To argue for sufficient resources, and to help the American people understand that good security and counterintelligence will allow us to keep our "peace dividend" of freedom, security, and prosperity and compete economically in the world on a more level playing field.

SPECIFIC COMMENTS ON THE PROVISIONS OF S. 2728

From a security and counterintelligence policy perspective, I support each of the recommendations made by the Jacobs Panel and the provisions of S. 2726 which would implement them. If fully and enthusiastically implemented by the Executive branch, they will improve counterintelligence and security capabilities. These recommendations are reasonable, carefully crafted, and, in my view, are respectful of the rights of all Americans, including especially those who incur added obligation as a result of their access to classified information.

I am particularly impressed that S. 2726 focuses largely on the most sensitive categories of classified information and places the additional security burdens on those with access to TOP SECRET or to other sensitive categories such as cryptographic information. I believe these provisions, tailored to protecting the most sensitive information, demonstrate both the careful approach the Committee has taken and its recognition that our security and counterintelligence efforts must proceed from an understanding of the importance of our secret information and programs, their security, vulnerability and threat they face.

I would underscore once again that virtually all of these provisions, especially those directed at improvements in personnel security, require sophisticated analysis to make practical use of the information developed. As I have indicated at the present time, all-source analytic centers with full access to security vulnerability and threat data to conduct such analysis do not exist.

Uniform requirement for access to TOP SECRET

The failure of the Executive branch to solve the easily remedied problem of uniform minimum standards for access to TOP SECRET exemplifies virtually all of the factors which work against an effective counterintelligence and security policy: fragmentation; lack of leadership; extreme bureaucratization; the repeated placing of turf consideration above the good of the country; and a general unwillingness to consider reform.

If the Executive branch has been unable to solve this problem after all these years, it is time for congressional action.

I would also point out that the Jacobs Panel looked at past cases, which is sensible; but, to the extent that we make progress in dealing with the volunteer/venal type of spy, we should expect foreign intelligence services to adapt by shifting their strategies (perhaps back to ideological recruitment. This again points out the need for an ongoing analytical capability to monitor the situation and make sure that the next time around, it doesn't take us twenty years to realize that the adversary has changed tactics.

This section of S. 2726 also requires agreement to report foreign contacts where an apparent effort is being made to acquire classified information. There are such policies within the Executive branch now; the problem is that they are not effective because the Executive branch has not developed a well publicized, workable system for carrying out this obligation. I believe the Committee should direct that the Administration bring forth such a plan as part of the requirement for implementation (in section 805).

Another issue related to this section of the proposed legislation is the standardization of the background check procedures. It should not be that agencies refuse to recognize the background check of another agency, or refuse to recognize clearances from another agency, or that one individual requires several background checks by different agencies. The Committee should insist that the procedures of each agency meet a commonly recognized performance standard.

Requirements for access to cryptographic information

Given the Executive branch's continuing inability or unwillingness to set and enforce such standards, I believe that this very sensible legislation is absolutely required.

Amendment to right the financial privacy act

This amendment is necessary, but again, alone it will not produce the required security improvement without a practical plan for implementation. My impression is that Panel and Committee envisage that Government would request reports on a selective basis, but since it would rely on these reports as an early indicator of trouble, selective access would not be enough. To make effective use of access to financial records as a screening indicator, it would seem that the Government would want to receive, on a periodic basis, reports on everyone with a TOP SECRET clearance. Such a requirement seems reasonable—we do much the same for conflict of interest financial reporting, which presumably is a lesser threat to national security. Some automated way of screening the reports for indicators of trouble would be needed and appropriate protection against misuse developed.

Extending FISA to physical searches

Perhaps the most difficult provision for me, from at least one perspective, is the proposed extension of the Foreign Intelligence Surveillance Act (FISA) to physical searches. I am not a lawyer and cannot speak to the legal theories involved. However, I do believe the Committee should question the Administration carefully because it is my impression they believe strongly that the President has constitutional authority to conduct these searches for intelligence purposes. I do feel qualified to address this issue from a national security policy perspective, however, since I spent six years staffing the President and his national security advisors on FISA requests and was thus intimately involved in the FISA process.

In general, Mr. Chairman, I am concerned that the impetus for this provision stems from a perception of unease among intelligence officers that they do not feel comfortable acting on a claim of inherent presidential authority. If that is the case, I think the President and his advisors and other officials should be under some obligation to bolster the Intelligence Community's confidence and take measures to ensure that this necessary tool is available. Further, I know of no suggestion that the Intelligence Community is abusing this intelligence technique. Thus, the presumed danger to intelligence officers in conducting these intelligence operations seems to me vastly overblown.

Moreover, I personally believe we have learned much in the last twenty years about intelligence activities and the prevention of abuse of civil liberties. Today, we have this Committee and the House Permanent Select Committee on Intelligence. A systematic misuse of an intelligence tool that could have occurred twenty or thirty years ago simply cannot, as a practical matter, occur today. And if an individual breaks the rules, procedures are in place (in many cases, far more effectively than in other areas of Government) to deal with such a transgression.

Thus, I believe that concerted leadership should be able to overcome any uneasiness of officials over the use of physical search for intelligence and security purposes. However, if such an effort is not possible and the Committee is satisfied that there is absolutely no other way to ensure the necessary use of this counterintelligence activity, I believe that this provision is acceptable.

Thank you Mr. Chairman for the opportunity to share these views with the Committee.

ENDNOTE

[1] These studies include:

—numerous Senate Select Committee on Intelligence and House Permanent Select Committee on Intelligence Reports: Senate Report 101-78, "FY 1990-1991 Appropriations Authorization for Intelligence Activities," July 1989; HPSCI Report 100-1094, "U.S. Counterintelligence and Security Concerns: A Status Report—Personnel and Information Security," October 1988; HPSCI Report 100-5, "U.S. Counterintelligence and Security Concerns—1986," February 1987;

Senate Report 99-522, "Meeting the Espionage Challenge: A Review of United States Counterintelligence and Security Programs," October 1986.

—annual multidisciplinary counterintelligence assessments beginning in 1978 through the present.

—numerous counterintelligence and security capabilities studies conducted during the Reagan Administration.

—the Stilwell Report—"Keeping the Nation's Secrets: A Report to the Secretary of Defense by the Commission To Review DOD Security Policies and Practices," November 1985.

—the State Department "Inman Panel" report on embassy security.

—the President's Foreign Intelligence Advisory Board reports to the President dealing with counterintelligence and security.

—annual telecommunications and automated information systems security assessments beginning in 1985.

—recommendations from numerous damage and vulnerability assessments, inspector general reports, and other postmortems resulting from the espionage cases of the last fifteen years, and reviews of technical security problems such as those at both U.S. embassies in Moscow.

—select outside recommendations including the consortium for the study of intelligence volumes—Intelligence Requirements for the 1980's: Counterintelligence (1982) and Intelligence Requirements for the 1990s (1989); National Strategy Information Center papers, authored by Kenneth E. deGraffenreid: "The National Counterintelligence and Security Assessment Center" (1990); "Countering Hostile Intelligence Activities as a Strategic Threat" (1989); "Overcoming Counterintelligence Shortcomings: Three Levels of Reform" (1989); and "Defeating the Hostile Intelligence Threat to American Security: Counterintelligence; countermeasures and security reform" (1989).

TESTIMONY OF KENNETH E. deGRAFFENREID, FORMER NATIONAL SECURITY COUNCIL STAFF MEMBER

Mr. DEGRAFFENREID. It is not an inconvenience at all, Mr. Chairman. It is an honor and pleasure to be here, particularly since in the late 70's I was a staff member here for four years and it's always a great pleasure to be here even when you have some other commitments. Unfortunately, today is the one day of the summer where everything is happening at once.

Chairman BOREN. I understand that.

Mr. DEGRAFFENREID. I do know though from that experience and certainly since then, how this Committee has carried the torch on this subject over the years and has consistently kept energy and attention focused on reforming and improving our counterintelligence and security capabilities. I think the Committee's involvement has remained steadfast in this area, even when on occasion, I am sorry to say, interest and attention has flagged in some quarters of the Executive branch ever the years. Now, once again, the Committee is out in front with its willingness to consider the issues which have been examined by the Jacob's Panel, and it is particularly gratifying to see within S. 2726 many recommendations some of which date back to the late 1970's and which for many years, in my view, have badly needed implementation.

However, I am little concerned that we should not have to wait for the creation of a distinguished panel like the Jacob's Panel in order to learn the lessons from the painful experiences of the last decade. And in my view, I believe the Administration and the Intelligence Community should have been conducting on-going studies of these matters all along.

From a security and counterintelligence policy point of view, I support each of the recommendations made by the Jacob's Panel. I believe the provisions of S. 2726 which would implement them are

imminently sensible, sound, balanced, carefully crafted, in keeping with our country's values, and in my view are very respectful of the rights of all Americans including especially those who incur added obligation as a result of their access to the information which protects our national security. And I believe if fully and enthusiastically implemented by the Executive branch, they will improve our counterintelligence and security capabilities and will make a very significant contribution to countering one, but only one, dangerous aspect of the foreign intelligence threat. In fact, they are long overdue.

Of course, these proposals would enhance prosecutorial capabilities and to that extent would serve both as a security tool, adding to deterrence and defense, as Senator Specter indicated, and also as an important counterintelligence tool, for a number of reasons, but particularly because of the critical role that successful prosecution plays in getting an accurate damage assessment. Damage assessments, as you know, Mr. Chairman, are critical to learning the lessons of the past and being able to improve so that in each case in the future we are not facing the same problems. And one of the problems of the decade of the spy is the repetitive nature of the problems we faced.

But I also think the passage of this legislation would send a powerful signal to the intelligence and national security communities of the continuing broad public support and expectations for this vital but sadly often unsung work. And I think it would also remind the American people, as you have done in some of your speeches, Mr. Chairman, that the challenges to foreign intelligence threats to our strategic programs, technology and information, continues despite the dramatic changes we have witnessed in Eastern Europe. Indeed this threat is expanding as friendly nations as well, target American national security and industrial secrets.

However, as helpful as I believe these recommendations to be, I think it would be a disservice to leave the Committee with the impression that these legislative remedies are sufficient to counter the most serious of the foreign intelligence challenges we are likely to face in the decade of change and complexity ahead. Nor do I think they really get at the fundamental problems facing our security and counterintelligence community. There are several reasons why this legislation, while very necessary, can really only be a small part of the comprehensive, systematic and strategic security approach to the threat that we are going to require in the 90's.

First, the Jacobs Panel limited its inquiries primarily to spies who volunteer, motivated by greed, as has been discussed. And while these kinds of spies—Walker, Whitworth, Pelton, and the many others—have done grevious strategic damage to this country, it is not clear that this is the only type of spy with which we have been confronted, nor with which we will be confronted in the future. Indeed, we can expect that to the extent that we make progress in dealing with the volunteer, venal type of spy, we can expect foreign intelligence services to adapt by shifting their strategies, perhaps back to ideological recruitment or some other motivation. And this again points out a need for the kind of risk assessment and performance monitoring that I want to mention in just 1 minute—to make sure that the next time around it doesn't take us

20 years to recognize that the nature of the threat and that the adversary has changed his tactics.

And indeed, while many of the spies of the last 15 years are in fact volunteers, many were also classical recruitments or a complicated mixture of both. And many were motivated not just by money, but by disgruntlement with their job, disenchantment with their place in life, revenge, political sympathies, and emotional or psychological instability. All these motivations seem to be at work. Frankly, I don't think we fully understand why people commit espionage, and I know the Committee has been in the forefront of directing that that work go ahead to better understand this phenomenon.

And there is another point here, Mr. Chairman. Because a surprising number, in my view, of these volunteer venal spies slipped not only through our security barrier, but were uncovered by means other than our direct counterintelligence techniques—Walker was turned in by his wife ultimately—it is at least possible that spies recruited on the basis of other motivations—ideology, blackmail, false flag and the like—could be practicing better tradecraft, if you will, and could still be spying. And so I would have to disagree somewhat with Mr. Halperin on this point. I think we need to examine a full range of motivations at least as we contemplate why people commit espionage.

I also think that the Jacob's Panel limited its examination almost exclusively to only one of the variables in what I call the espionage equation: the American who betrays his country. In fact, however, the process by which intelligence services steal our strategic secrets and harm our interests has at least two other elements. One concerns the nature of the threat itself, including technical collection as well as human espionage. And this threat, as you know, sir, varies with the size and level of the foreign effort and with the degree of access and proximity to American secrets and people.

The other variable concerns the nature, sensitivity and vulnerability of the secret information itself, and there has been some discussion of whether the classification system itself is adequate to convey this kind of sensitivity. And I personally believe it is inadequate to that task and we need to develop other techniques. And I would agree with Senator Specter and Mr. Halperin on that point.

To be effective then our response to the threat—security countermeasures and Counterintelligence—must be part also of a system and must comprehensively address each of these variables in the espionage equation. Today unfortunately the totality of our efforts are not part of a well coordinated system which proceeds from a common strategy for defeating this foreign intelligence threat, broadly conceived in this way. To protect against the threats of the 90's will require a number of policy, resource, organizational and cultural reforms which go well beyond the very necessary legislation contained in S. 2726.

Of these broader reforms, I would just like to mention the one that Mr. Halperin referred to, risk assessment. It is also a point that Admiral Inman made as part of the Jacobs' Panel, that he was appalled at the fact that the Intelligence Community itself had not gone back and analyzed these espionage cases the way the

Jacobs' Panel did. And I think there is a reason for that and it is that by and large the Government does not conduct risk assessments in this field. By that I mean, we lack a comprehensive analytic capability to identify the vulnerabilities of our data, combine the full range of what all the departments and agencies know about the multi-disciplinary aspects of the threat, and based on systematic analysis, assess the risks involved to that information. Absent such a capability—a brain for the system, if you will—we have no way purposely and efficiently to allocate scarce security and counterintelligence resources in a balanced, coherent fashion. Nor can we coordinate their efforts.

And finally, without a "big picture" understanding of the lessons of past security failures, as well as the intelligence signatures of our secrets, it would be very difficult to tailor our counterintelligence operations, either at home or abroad, to interdict and neutralize foreign intelligence operations in order to compensate for the kinds of gaps we find in our security and countermeasures, some of which are endemic to a democratic society and some result, in my view, simply from poor performance.

In short, Mr. Chairman, I believe that correcting this deficiency is the single most important undertaking facing those, both in the Congress and in the Executive branch, charged with protecting the Nation's secrets. I have prepared a study on the need for this analysis which I would respectfully submit for the record.

Chairman BOREN. Without objection, it will be included in the record.

[The paper referred to follows:]

THE NATIONAL COUNTERINTELLIGENCE AND SECURITY ACCESS CENTER

A key element of a coordinated national response to the strategic threat to American national security posed by foreign intelligence activities is the National Counterintelligence and Security Assessment Center. The Center would: (l) act as the analytic "brain," providing macro-level counterintelligence and security vulnerability and threat analysis; and (2) coordinate strategic security and Counterintelligence operations and activities. The Center would receive information from and be supported by expanded or newly created departmental and agency level analytic and coordination centers.[1]

Part I of this paper describes the Center and the functions it would perform. Part II illustrates how the Center would work in providing strategic security for on-site inspections under a future START agreement.

PART I—DESCRIPTION AND FUNCTIONS OF THE CENTER

The Center would perform a variety of analytic and coordination functions to ensure a unified national approach to protect against hostile intelligence activities. Many of these functions are not currently performed or even assigned, or are not conducted from a coordinated national perspective. The Center's functions include:

a. Identifying and prioritizing the nation's strategic secrets;

b. Identifying and analyzing the security vulnerabilities of these secrets;

c. Evaluating all dimensions of the hostile intelligence threat, including possible deception;

d. Balancing vulnerability versus threat to determine the risk to each strategic secret;

e. Coordinating strategic security, countermeasures, operational security, and counterintelligence activities and operations at home and abroad; and

f. Developing performance standards for and evaluating the effectiveness of U.S. security, countermeasures, and counterintelligence efforts.

Functions

a. Prioritizing Strategic Secrets. The Center would collate and analyze a range of strategic secrets based on submissions by the various departments and agencies of

the national security community. These involve the secret intentions, information categories, programs, activities, and technology that are critical to the Nation's defense, diplomacy, intelligence, and economic well being.[2] Individual departments and agencies, which best understand the details and the strategic importance of their programs and activities, would develop a priority ranking of their secrets for the Center. (For most of these organizations this would be a new mission and activity.)

The Center then would prepare a suggested ranking of security values for the entire national security community. This would take the form of a draft National Security Directive (NSD) for consideration by the National Security Council and for Presidential approval. This ranking would serve as national policy guidance for priority allocation of security and counterintelligence resources, as well as for conducting security and counterintelligence operations and activities.[3]

To accomplish this function, senior intelligence, operational, and policy analysts—with wide-ranging backgrounds in U.S. national security policies, programs, and procedures—would be required to analyze relative values, suggest tradeoffs between these values, prepare draft NSDs, and provide staff support to the decisionmaking process. Much of the work involved in identifying and prioritizing would be accomplished by analytic centers in individual departments which would supply this information to the National Center and act as the focal and coordination point for departmental analysis and activities.

b. Identifying the Vulnerabilities of Strategic Secrets.[4] Vulnerabilities include those inherent characteristics of a secret program, activity, or technology which make that secret liable to compromise. Security vulnerabilities naturally are to be found within all classified intentions, information, programs, activities, and sensitive technologies. Vulnerabilities result from a variety of factors: human weaknesses; exposed locations and other physical characteristics; inherent technical flaws or weaknesses; operational procedures and requirements; etc. While all secrets involve people and thus are generally vulnerable to classical forms of espionage, there are also vulnerabilities specific to various types of technical collection.

The degree of vulnerability often does not remain constant—the changing-technologies and capabilities of hostile intelligence agencies can increase or decrease the potential for damage. As a result, the assessment process must be dynamic, and vulnerability assessments must be informed by knowledge of the skills, capabilities, techniques, and successes of both foreign and U.S. intelligence collection activities.

The Center would establish baseline vulnerabilities for U.S. strategic secrets and evaluate them on a continuing basis. The results of vulnerability assessments on particular secrets would be provided to departmental level assessment and coordination centers as well as to the security and Counterintelligence elements charged with their protection. The information also would be used by the Center to determine, when balanced against specific threats, the overall risk to each secret.

Identifying vulnerabilities and determining which, potentially, are most harmful will depend on:

(1) Comprehensive vulnerability assessments of each strategic information category, technology, program, or activity during its life-cycle or the duration of its sensitivity.[5]

Certain elements within the national security community have developed highly effective assessment programs which include sophisticated evaluation techniques and models. Several special access programs to protect highly classified and fragile technologies ("black programs" such as "Stealth") include very thorough vulnerability assessments. Also, those organizations with extensive operational security (OPSEC) programs generally have strong vulnerability assessment capabilities. This capability should be developed in all organizations possessing strategic secrets.

The assessment process begins with an examination of the totality of an activity to determine which exploitable indicators could be acquired by a hostile intelligence service. Although the operational assessment activities would be carried out by the relevant individual organizations, tasking authority for these assessments would be given to the Center in order to ensure thoroughness, avoid duplication, and concentrate scarce resources on the most important strategic assets. Often, more than one organization will be involved in conducting a comprehensive assessment of programs or activities (e.g., the National Security Agency will assist in COMSEC vulnerability assessment, the Defense Investigative Service in industrial security).

(2) Damage assessments of espionage cases and other hostile intelligence successes (e.g., electronic bugging of the U.S. Embassy buildings in Moscow).

These must be mandated by, and the results provided to, the Center. Comprehensive and thorough damage assessments provide invaluable lessons which reflect a very practical test of security effectiveness. Because such unvarnished damage as-

sessments are rare, procedures to increase rigorous objectivity (including bureaucratic protection for investigators), and sufficient resources will be required government-wide in order to obtain the necessary information and to provide it to the Center on a timely basis.

(3) Information obtained about the targets of foreign intelligence services and their operational successes which illuminate U.S. vulnerabilities.

For example, if the KGB is observed by U.S. intelligence to be spending substantial resources recording certain specific enciphered U.S. communications links, there are grounds for questioning whether that cipher is secure. Such a discovery would lead to a thorough vulnerability assessment on a priority basis.

(4) The vulnerabilities in the programs, technologies, and operations of foreign governments discovered through U.S. intelligence successes.

Often, vulnerabilities can only be discovered through the practical test of attempting to penetrate foreign security efforts. For example, if U.S. intelligence develops an advanced surveillance device which can compromise the security of a particular Soviet technology, appropriate U.S. security and countermeasures elements should be alerted that potential generic vulnerabilities exist and can be exploited. The Center would act as a "buffer" in this process by developing procedures to sanitize this information in order to protect the success and other sensitivities of U.S. intelligence operations.

(5) Anomalies or otherwise inexplicable successes of foreign governments (in their policies, capabilities, activities, or operations).

These can suggest the compromise of U.S. secrets. For example, detection of otherwise unexplained changes in Soviet submarine tactics which seem to optimize Soviet strengths at the expense of U.S. vulnerabilities indicates the possible compromise of U.S. programs and procedures, possibly by compromise of U.S. tactics and penetration of enciphered U.S. communications, as in the Walker espionage case. A process for alerting the Center to such anomalies would be developed. The Center would draw on relevant expertise throughout the government for these alerts and this information.

c. Evaluation of All-Source Multidisciplinary Intelligence Threat Data. The Center would evaluate the capabilities (including strengths and weaknesses), operational methods, targets, and degrees of success of hostile intelligence services. The Center would receive information obtained from counterintelligence operations as well as "positive" collection which yields information about foreign HUnMINT, SIGINT, PHOTINT, and other intelligence activities. Centralized analysis of hostile intelligence activities would bring together all relevant information available to the U.S. Government. Today such detailed information on the nature and methods of foreign intelligence services is not routinely shared among all U.S. intelligence organizations. As a result, counterintelligence analysis is often incomplete, making the understanding of hostile intentions and modus operandi difficult. Collation of this information would also facilitate the coordination of Counterintelligence analysis, activities, and operations by various elements of the U.S. Intelligence Community.

The Center would analyze hostile intelligence activities without the artificial "foreign/domestic," geographic, or other functional distinctions which currently impede effective analysis and coordination. Patterns in activities and the modus operandi of foreign services can reveal the services' thinking about a variety of strategic issues in addition to identifying U.S. secrets that they have targeted. From this effort, the Center would provide various types of counterintelligence analytic products to assist security and counterintelligence elements throughout the government. The evaluation of possible foreign deception activities likewise depends on a full understanding of all counterintelligence information. Also, opportunities for sophisticated U.S. counterintelligence responses (for example, in support of U.S. OPSEC or deception operations) would be enhanced.

d. Assessment of Vulnerability Versus Threat. A key function of the Center (not being performed today) is the evaluation of vulnerability versus threat for each identified U.S. strategic secret program, activity, technology, or category of information. The result of this effort would be an assessment of the relative security risk to each secret. Evaluation of risk, of course, depends on the successful integration of the above mentioned activities (a through c).

The judgments produced by the Center are central to the fundamental responsibilities of national policymakers, department and agency heads, as well as program managers and others charged with managing security risks and neutralizing foreign activities. Based on the Center's assessment, decisionmakers would be in a better position to apportion security and countermeasures efforts and resources, initiate comprehensive OPSEC or deception programs, and direct counterintelligence activities to focus on gaps in security coverage.

As part of the assessment process, the Center would produce a variety of analytic products and data, including:

(1) "National Intelligence Estimates" (NIEs) on foreign intelligence threats, as well as vulnerability net assessments for national policy leaders so that security concerns may receive appropriate consideration in overall U.S. national security policy.

For example, an NIE on the threat posed by the ability of the People's Republic of China or certain East European intelligence services to acquire U.S. high technology would be critical to policy decisions on the exact level of technology that could safely be shared with these countries. Without such knowledge, policymakers could not easily set a realistic level for legal technology transfers. Likewise, because Soviet intelligence services, in particular, represent a strategic threat to U.S. security, an NIE on Soviet intelligence activities would be analogous to the annual NIE on Soviet strategic offensive forces.

(2) Draft inputs for Presidential NSDs establishing national security and counterintelligence priorities.

The Center also would draft sections on security for other NSDs and national policy guidance. For example, there should be a protective security dimension to national and departmental policy directives on strategic offensive nuclear modernization programs, strategic defense activities, the verification monitoring aspects of arms reduction agreements, high technology trade, and national telecommunications in addition to other national security issues.

(3) Technical information, analysis, and support to senior managers of U.S. strategic programs, diplomatic and intelligence activities, and other activities requiring protection of strategic assets.

This would include providing risk ("threat versus vulnerability") assessments and data to security and counterintelligence elements, as well as to operational managers, commanders, and other authorities conducting OPSEC programs. This is a critical function of the Center and would consist of regular finished products, specialized analysis, as well as real-time support to security and counterintelligence operations and activities. Operational commanders and managers must know which secrets and technologies are most vulnerable and in what priority they should be protected. A dynamic process which monitors the totality of the threat and which includes a feedback mechanism to report on the security status of programs and activities is required.

The Center would provide tailored assessments so that a systematic operational security approach can be "built-in" to the development and life-cycle of each secret information category, activity, technology, or program using systems security engineering techniques. For example, inputs could be prepared to assist DOD in bringing OPSEC consideration to the Defense acquisition process. This form of OPSEC is "forehanded"—designed to protect programs by preventing hostile penetration or by ameliorating the degree of harm. By maximizing security and countermeasures efforts, this approach can make more manageable the task facing limited Counterintelligence capabilities.

(4) Threat and vulnerability data for security managers to use in their risk management, training, and educational responsibilities.

Good security leadership is an exercise in managing risks to accomplish a mission as securely as possible. In many cases, today's security managers have little understanding of the specific multidisciplinary aspects of the threat facing them. They also lack important details about the vulnerabilities of their own programs. To improve performance, department and agency security and counterintelligence specialists (as well as program managers and operational commanders) require extensive training which includes in particular, current and historical examples of U.S. and foreign intelligence and security successes and failures. The Center's products would assist these officials in underscoring to their employees the idea that security is a key element of operational and combat effectiveness, not a hindrance.

(5) Information for resource managers to use in budgetary decisions.

It is very difficult today to express quantitatively the strategic impact of foreign espionage and to determine the resources which should be spent on security for particular programs or technologies. The Center would estimate the dollar cost of losses to foreign intelligence activities so that policymakers in the Executive Branch and the Congress can factor this information into decisions on the appropriate level of the security and Counterintelligence effort required for specific programs.

e. Provide Coordination for Strategic Security and Counterintelligence Activities and Operations. In this capacity, the Center would be similar to other national intelligence centers (such as the National Military Intelligence Center or the National SIGINT Operations Center) and would provide a continuous interagency coordina-

tion capability. While day-to-day security, countermeasures, and Counterintelligence operations would remain with the individual departments and agencies, coordination of assets for strategic operations would be assigned to the Center.

f. Develop Performance Standards and Measures of Effectiveness for U.S. Security and Counterintelligence as well as Coordinate Performance Evaluations. For security and Counterintelligence to be improved, policymakers must understand specific shortcomings and be able to measure the effect of various reforms and enhancements. Unlike many other areas of government where performance evaluation is routine, at present there is no rigorous mechanism for measuring how well the U.S. is doing in protecting its strategic secrets from hostile intelligence services. Nor is there an easy system for establishing national security performance standards. The Center would conduct evaluations of techniques, operations, etc., and develop, test, and apply these standards.

Tasking Authority

The Center would have government-wide authority to task departmental and agency security, countermeasures, Counterintelligence, and other elements to collect all-source threat information, damage assessments, and vulnerability data. This information would be provided to the Center for evaluation and coordination.

Staffing

To accomplish its many missions, the Center initially would require a staff of twenty-five to thirty analysts. More analysts might be required when fully operational—a process which could take several years. The national security community currently possesses, at least in small numbers, people with many of the skills required to staff the Center. In many cases, the Center's activities would offset activities undertaken elsewhere, and thus would require no net increase in personnel. However, in some cases, the Center's functions are not currently performed and additional personnel would be required. Yet, given the size of the national security community and the importance of the Center's work, equivalent personnel spaces should be located without great difficulty. In some cases, required skills do not currently exist or are not performed from a national perspective. An intensive training program and an incremental staff build-up would be required to develop these skills and this perspective.

Resources

Creation of the Center will require only modest resources. These will go mainly for additional personnel who cannot be transferred from current assignments within the government; data processing and other specialized technology required for a "watch" and coordination center; as well as specialized security procedures which will be required to protect the security of the Center itself. However, the savings realized by the products of the Center would more than offset its cost. First, the Center would greatly improve the efficiency of security, countermeasures, and counterintelligence activities. Second, and most importantly, preventing the theft of valuable secrets could save the U.S. billions of dollars.

Security

Earlier proposals to gather all-source sensitive data within one agency or office have raised concerns about "bringing all the family jewels together in one place." Such a characterization implies increased vulnerability and risk. Yet, on closer examination, the suggestion that the national assessment center would present an increased security risk is seriously misleading. In fact, existing program-level OPSEC and security assessment centers have very successfully managed the potentially increased security risk of aggregated information.

Virtually all other national security areas (except counter-intelligence) not only routinely centralize the most sensitive secrets, but have devised methods for protecting this aggregated information. For example, the production facilities for cryptographic material at NSA have security methods which combine personnel, physical, and electronic control and accountability procedures. Individuals are permitted to work with the most sensitive material while retaining appropriate internal controls which prevent any single person or small group of persons from compromising the whole body of information.

One of the premier strengths of U.S. intelligence is the integration of collection systems and disciplines using various national intelligence fusion centers which rely on the aggregation of sensitive information.

In any case, the potential security risks associated with a national assessment center (designed to improve substantially overall security) must be weighed against the proven espionage risks to currently distributed strategic secrets.

Organizational location

It is difficult to ascertain where the Center should be housed. Each suggested location within a major security or counterintelligence organization has advantages and disadvantages. While the Director of Central Intelligence has broad Intelligence Community responsibility, the CIA is enjoined from many domestic security functions, and the FBI is primarily a domestic counterintelligence organization lacking security, countermeasures and OPSEC responsibilities. Although the Secretary of Defense has responsibility for the security of many strategic programs and technologies, his purview is limited to military matters. While charged with coordinating many U.S. activities abroad, the Secretary of State's purview likewise is limited.

Most importantly, the Center must have a national level perspective transcending the views of any one department or agency, as well as the leverage to overcome bureaucratic resistance to national taskings and the ability to ensure subordination of "agency views" to national requirements. Thus, a White House-affiliated location has been recommended by many observers. At a minimum, a White House imprimatur is required.

PART II—HOW THE CENTER WOULD WORK: SECURITY FOR ON-SITE VERIFICATION

The following example illustrates how the Center would work.

The U.S. will require comprehensive, systematic security to protect strategic secrets in the face of intensive on-site arms control verification inspections under a START treaty. The National Counterintelligence and Security Assessment Center would be integral to this effort.

The START agreement, which will rely on complicated on-site inspection regimes, will bring hundreds of Soviet intelligence officers into or adjacent to several hundred of the most sensitive installations conducting classified activities in the U.S. for extended periods of time. These include production facilities, research and development activities, and operational military installations. Most of these sites also conduct non-treaty related sensitive activities and have classified information not relevant to treaty verification located within them. The unprecedented scope of Soviet access to this array of installations will be a major challenge to U.S. security and counterintelligence capabilities. American geography and culture, the generally close proximity of treaty-related installations to other sensitive sites, and the current scarcity of security and counterintelligence resources add to this challenge.

To prevent the Soviets from obtaining a windfall of intelligence on U.S. secrets, a number of protective steps must be taken. To be successful, these tasks must be accomplished from a comprehensive national perspective. Moreover, in a period of tight budget constraints these security measures must be the most cost effective possible. Today, despite some improvements resulting from experience with the INF Treaty, the U.S. has no comprehensive systematic approach for responding to this strategic threat.[6] The National Counterintelligence and Security Assessment Center (and similar departmental-level centers within the national security departments and agencies) would be key to such an effort. How might the Center work in this context?

a. Prioritizing the Nation's Strategic Secrets.

If they are to maximize U.S. national interests, policymakers must weigh the tradeoff between the treaty compliance advantages of on-site inspection and the security shortfall resulting from intrusive Soviet inspections of U.S. facilities. This analysis is required both during the treaty negotiation phase, so that the most advantageous terms and inspection arrangements can be obtained, and during the inspections themselves.

At present, however, the U.S. has no method for understanding or ranking the relative security values of various U.S. installations for use during negotiations over on-site inspection locations and procedures or at these installations once a treaty is ratified. The Center could provide an understanding of the relative strategic "worth" of individual U.S. sites necessary to both treaty negotiations and implementation. Armed with this ranking, both negotiators and those charged with protection could seek to maximize the security of the most important secrets. This information would be extremely critical to negotiations on the extent, timeliness, and degree of intrusiveness of these inspections. During treaty implementation, such as during the dynamic process of suspect site inspection, a prioritization of secrets is essential.

b. Identifying the Vulnerabilities of Strategic Secrets.

The Center would analyze the particular vulnerabilities to KGB/GRU human and technical collection of U.S. secrets to be found at the various sites (perimeter portal monitoring sites, facilities subject to suspect site inspections, etc.). To provide this

analysis, a number of tasks must be accomplished, including detailed vulnerability assessments and security evaluations, which must look to SIGINT, imagery, and other technical threats, as well as human collection. This is a complicated effort requiring specialized expertise, systems integration capabilities, and sophisticated analytic techniques. The Center would draw on resources from across the national security community in directing and analyzing these assessments. The Center would provide rankings of relative vulnerability for each site to national decisionmakers, as well as to program and security managers.

c. Evaluating All Dimensions of the Threat.

Since the Soviets have less need to ensure U.S. treaty compliance via inspection, it can be assumed that the Soviet inspectors have as a primary assignment intelligence collection. Moreover, because Soviet collectors are technically sophisticated and highly experienced and because they will have narrowly focused collection targets, even casual observation of many U.S. facilities can potentially be extremely harmful. The Center would collect and coordinate all multidisciplinary threat data (HUMINT, SIGINT, imagery) related to the possible inspection sites, acting as a clearinghouse for this information.

d. Balancing Vulnerability Versus Threat to Determine the Strategic Risk for Each Site.

The Center would offer its judgment of the relative security risk at each site, by balancing vulnerability and threat. The Center would assist in integrating this information into interagency deliberations on U.S. negotiating positions, particularly regarding sensitive site selection, as well as protocols establishing timing of inspections and degrees of access to installations. Alternate sites could be offered in those cases where the security risk is unacceptable. Where alternate sites are not possible, the Center could identify vulnerabilities of threatened U.S. programs for which managers could fashion compensatory strategic security "safeguards." These could be offered, for example, at the time of Senate ratification as appropriate security measures.

The Center would alert managers of threatened programs in sufficient time to permit adjusting security and adding countermeasures, if necessary and possible. Likewise, counterintelligence elements would have sufficient time to request resources and prepare counterintelligence operations, which have not always been possible in the past. Because the security system must be thorough and protect all U.S. secrets within the geographic range of Soviet inspectors at each site (government installations as well as contractor and subcontractor facilities), the Center would have government-wide tasking authority in order to obtain necessary threat and vulnerability data.

e. Coordination of Security and Counterintelligence Activities and Operations.

After treaty approval, the Center would coordinate a systematic approach to security at treaty-related sites. For example, the Center would direct NSA COMSEC assessment capabilities to assist the Defense Investigative Service in assessing the threat to particular defense contractor activities. The Center would also monitor the performance of strategic security and countermeasures plans to ensure that they are sufficient to detect and neutralize collection activities in minimum time. This information would be provided to counterintelligence agencies which could then concentrate resources on gaps in protective coverage or on offensive counterintelligence operations. Lessons learned also would be catalogued to provide a basis for future activities.

KENNETH E. DEGRAFFENREID.
March 1990.

This paper represents the views of the author. The National Strategy Information Center as an institution does not take positions on issues of public policy.

ENDNOTES

1. A national policy directing security assessment activities at the departmental level is contained in NSDD–298 of January 22, 1988, "National Operations Security Program." This directive outlines the assessment process described in this paper and directs that each executive department and agency establish a formal OPSEC program.

2. Categories of strategic secrets include: sensitive diplomatic negotiating positions, strategies, and intentions; the locations of our hidden retaliatory forces; the codes and ciphers which protect military and diplomatic communications; war plans; intelligence sources and methods which provide warning about and understanding of threats and opportunities; as well as the sensitive technologies which give military and commercial advantage.

The current method for setting priorities is limited to classifying general categories of secret information according to, the potential harm to national security resulting from the loss of this information to a foreign power. However, this information classification system (TOP SECRET, Secret, and Confidential) is woefully inadequate from a strategic perspective. As a process, the system is totally decentralized. Decisions are based on almost intuitive judgments by low-level officials about the value of the information from the national U.S. perspective, often with little understanding of vulnerability or threat. The system itself is overburdened by a massive volume of documents and by instances of bureaucratic misuse.

Most troubling, the three categories do not provide sufficient discrimination between varying sensitivities. While statutory elaborations on the classification system identify somewhat narrower categories of secret information (including atomic energy data, intelligence agents' identities, communication intelligence information, as well as intelligence sources and methods), the present classification system does not provide sufficient predicate for a tailored strategic security, countermeasures, and counterintelligence program.

3. For purposes of this discussion, security includes all the activities which fall under the heading of countermeasures and security.

4. This is the area perhaps most in need of improvement. At present there is no national process for gathering vulnerability data, very little analytic capability devoted to vulnerability assessments, and few organizations with experience in conducting these assessments. As a result, only a few of the most sensitive U.S. programs and technologies have vigorous, dedicated vulnerability assessment programs. Nor has there been an attempt to systematically protect strategic information which is increasingly vulnerable through automated data processing as well as via the compromise of personnel and paper.

5. Such assessments are difficult, complicated, and demand a high degree of rigor. Moreover, unless these assessments comprehensively examine every aspect of the hostile threat, openings for hostile intelligence targeting and operations will be overlooked.

6. Following years of negotiations, the INF Treaty was signed December 8, 1987, to go into force on July 1, 1988. Soviet inspectors began arriving in the U.S. shortly thereafter as part of an on-site inspection regime for INF weapons-related production and storage sites. Soviet inspectors were stationed permanently outside the Hercules Corporation's former PERSHING solid fuel rocket motor plant near Salt Lake City and at a variety of other sites on a temporary basis to monitor destruction of INF weapons.

Unfortunately, U.S. and Soviet negotiators had agreed on these sites before the United States had reviewed the security vulnerabilities at these locations. Subsequent security surveys found "target-rich" collection environments for Soviet inspectors, many of whom are known to be KGB/GRU officers. As a result, U.S. security and counterintelligence agencies had to scramble to catch up to protect nontreaty related secret programs and technologies from compromise. For example, at the time the Treaty was signed no one inside the U.S. Government was aware of which secrets, programs, and technologies were located within the travel boundaries and SIGINT range of Soviet inspectors. Since INF, programs have begun at DOD and other agencies to identify the location of all special access program activities.

Mr. DEGRAFFENREID. Basically it is a five or six step process. Identify the secrets; identify their vulnerabilities in information, technology, programs and activities; evaluate the threat holistically—because that is how we attack intelligence problems in a multidisciplinary way; and then balance this threat versus vulnerability to come up with a risk assessment. Some things we don't need to protect as much as other things and some are absolutely vital to our survival. Then use that information to deploy, efficiently and cost effectively, what are, after all, very limited resources; and finally—and this is something I think the Committee could be very helpful on—develop performance standards for evaluating the ef-

fectiveness of these efforts, so that we will know next time around, how well we are doing. The Committee and the President can be told if the problem is "bigger than a breadbox", and how well we are doing.

Two additional quick recommendations, Mr. Chairman, which are not small. First, over the years, as you have pointed out, we have developed literally hundreds of recommendations including outside commissions beginning back in the mid-60's—and I have actually compiled all of these in a little list which is part of my study—and all the work that has been done by this Committee, the House Intelligence Committee and other Committees, and by successive Administrations. These studies have produced probably 4 or 500 recommendations, which seem to move at the glacial pace we talked about earlier—7 years for some recommendations. Some haven't moved at all.

I believe that the Committee could perform an extremely useful service by designing a plan which would require implementation of these recommendations. Many of them involve budget enhancements, organizational improvements, mission definitions and other improvements. But I think even a modest improvement in many of these things would cumulatively result in a very substantial improvement in our total security at an achievable cost. So I would conclude by saying that we have studied it enough. It's time to act, we've fixed enough fence; it's time to start farming.

As to the second recommendation, on the other hand, I think there is some study to be done, and I would say that the Jacobs' Panel has already resulted in an obvious success. And I strongly recommend that the Committee consider the creation of similar panels in what I would identify as five different threat areas. And I realize this is not a small workload, but I believe the issue is raised, and considering how to respond to these threats are so important that they justify the level of effort and commitment. And I also believe that the Committee would have no trouble in finding a sufficient number of distinguished citizens to assist it in its work as it did with the distinguished members of the Jacobs' Panel.

Let me just tick these areas off. One is the strategic security threat posed by on-site inspection of arms control agreements. I, believe that remains a very difficult and potentially very troublesome area. The second is the strategic dimension of global economic competitiveness which you have spoken about, but I think the protecting of both our national security and our industrial secrets is something we need to sort through. Certainly we benefit from the free exchange of ideas, but we also recognize here at home copyrights, patents, and other things which protect certain categories of information. There are legitimate reasons to protect intellectual property.

The third is the continuing threat to telecommunications and computers which I think is increasing with the global proliferation of sophisticated collection technology, which has also become very cheap. Someone can go to Erol's and to radio Shack and buy the things to do terrible damage to our country.

Fourth is the threats from what I would call non-state run intelligence activities, especially illegal drug traffickers. I think that threat is very serious to law enforcement. The Committee's particu-

lar expertise in balancing intelligence and law enforcement functions that it demonstrated in FISA, Classified Information Procedures Act, makes it uniquely qualified, and is perhaps the only body that an seriously look at this.

And finally, the fifth area is an old one, Mr. Chairman: the continuing Soviet threat in a period of increased Soviet access, declining public awareness, and severe budget constraints. The Cold War may be over, but the intelligence wars are certainly not over.

Two specific comments on the legislation itself. One, few of these provisions will work without the kind of comprehensive analysis that I spoke about. We can collect information about who has access to TOP SECRET and their financial records, but unless we have a capability to analyze that in a coherent way, it won't do us much good, and indeed could be dangerous. A lot of "stupid" security could be done rather than the sophisticated, analytic-driven, security countermeasures and counterintelligence capabilities that we need in the 90's.

And finally regarding physical searches, the Panel, Mr. Chairman, cited as the impetus for this provision, the perception of unease among intelligence officers that they don't feel comfortable acting on a claim of inherent presidential authority for conducting physical searches. I am not a lawyer, but did have responsibilities for FISA, for a long time when I was at the White House. If there is such a perception, and I am not sure there is, I think the President and his advisors and other officials are under some obligation to bolster that confidence. But if it turns out that, there is simply no other way to do that, if that is in fact the reason for doing this, then I think legislation may be required. But I would point out that I don't know of any suggestion that the Intelligence Community is abusing this intelligence technique of physical search for intelligence purposes. And I am not sure but that this presumed danger to intelligence officers conducting these operations may be a bit overblown.

Finally, I would say I think we have learned a lot in the last 20 to 25 years about intelligence activities and about the prevention of their abuse to our liberties, which they are intended to protect. We have this Committee, the House Committee, and I think that a systematic misuse of an intelligence tool that one could suggest could have occurred in the past, simply as a practical matter could not occur today. I think individual acts, breaking the rules, may occur but we have many procedures in place in this area to deal with those probably better somewhat than in other branches and other parts of public policy.

But if that is the only way we can use this tool, which is the suggestion of the Jacobs' Panel testimony, then I am prepared to reluctantly support legislation in this area.

Thank you, Mr. Chairman, and I appreciate your accommodating my difficult schedule.

Chairman BOREN. Thank you very much.

You have made some excellent points. I think the whole point of retargeting our resources, it goes along really with what Mr. Halperin talked about risk assessment, very much on the same point. We only have so many resources. We need to restructure how those resources are targeted in order to make efficient use of them. And

I think it will have both the beneficial value of being more effective, protecting those things that most need to be protected, and probably resulting in less intrusion in the lives of others where it is unnecessary.

Now, most of these matters I would gather could be worked out without legislative enactment. In other words, with the proper initiatives from the Executive branch, the proper initiatives from this Committee, the budgeting process and the rest of it. Setting up some standard by which to judge how well resources have been reconfigured, we could really pretty much accomplish most of this without legislation, could we not? The six points you suggest?

Mr. DEGRAFFENREID. Yes, sir, I think it could. I think though that the presence of the Committee in this process and of the Congress as a whole is absolutely critical because, in my own view, the situation with regard to the TOP SECRET security clearances could have been solved already. I know as staffer at the White House who tried to solve that problem that the bureaucratics involved, the turf considerations and others simply prevented the movement to action. To get results I think may take the Committee moving to legislation. And if you will, if it takes a hammer, maybe it's time for a hammer on these issues.

Chairman BOREN. It is really mainly bureaucratic infighting between departments that has made it so difficult for the Executive branch. As I was mentioning to Miss Lawton earlier, we have now had approximately 7 years of attempts made by the past Administration and this Administration. Is that the main problem that we are dealing with here, turf protection and—

Mr. DEGRAFFENREID. I think that is the problem that has prevented these several hundred recommendations similar to the one on the TOP SECRET clearances from getting enacted, yes, sir. My own observation, when I was at the White House, was that when the Committee would issue its reports, both the unclassified and the classified, that had a tremendous effect on focusing the thinking within the Executive branch and moving to action. But so slow is this process. I mean, I have been working on some of these issues for 15 years. I think there really has to be a movement to action in this area.

But my other point is that without an analytic capability, a brain to this system, even where there is good will and the desire to make these things happen, it is serendipitous if good things happen because it's a very large process involving all kinds of agencies and departments and levels. Without some kind of coordinative function, people will simply run off, even if they are trying to do right, in all kinds of directions. And therefore I think the Committee, with its continuity and its focus and attention on this, can keep a strategy in mind to contemplate the big picture and have that out in front of them, and try to work many of these issues over time. Just take a check list and begin working off some of these recommendations. Obviously many of them are Executive branch initiatives, but the Committee's resources and other Committee functions, I think could be a catalyst for moving these recommendations forward.

Chairman BOREN. I think you are quite right that the Committee has to be involved in prodding this process and setting up an ac-

countability and a measurement standard of performance all the way through.

Let me ask this one very quick question, because we're right down to the line when you need to leave to catch your plane. In your full statement you talk about many financial records. You seem to be suggesting we could require financial reports beyond what have been required or talked about here. The Jacobs' Panel suggested more along the lines of fuller financial disclosure statements made by a very small number of presidential appointees. This is something that could be done, could it not, without legislation as an initiative by the Executive branch if they chose to do so, or could it? Or would it require—

Mr. DEGRAFFENREID. Yes, sir, I think it could.

Chairman BOREN. And filing of disclosure statements.

Mr. DEGRAFFENREID. Yes, sir. Filing those kinds of statements and I think it could be done. Again, I, would be concerned that there would be proper safeguards to prevent both abuse and what I have referred to earlier as sort of stupid security. But I think with a sophisticated approach to this, which was not burdensome, did not require hundreds of more hours of filling out forms but simply used much of the data that was available, we could learn some things. But that's a long way around the block to get at one kind of spy. And as I say, I underscore the need to look at these other threats and see where the threats of the 90's are going to be.

Chairman BOREN. Right; I understand.

Well, again, we don't want to make you miss your plane. We appreciate very much your testimony which has stimulated our thinking in a number of areas, not only those limited strictly to the legislation at hand, but the broader nature of the needs which you have outlined. We very much appreciate your taking time to come back and be with us today.

Mr. DEGRAFFENREID. Thank you, Mr. Chairman.

Chairman BOREN. Thank you very much.

This concludes our testimony in this public hearing, and again I want to express my appreciation to all of the witnesses for being with us in this unusual public session of the Committee. We are discussing matters of fundamental policy involving the civil rights and civil liberties of our citizens as well as national security concerns. And it is the belief of the members of our Committee that wherever possible, these kinds of discussions should take place in public session. We try to act as trustees not only for the whole Congress, but for the American people in intelligence policy areas. We are determined that in that trusteeship role we should act in a way that is fully consistent with the values of the American people. I know it always pleases me when we find it appropriate to be able to have these kinds of discussions in open session so that the entire population can be a part of our deliberations.

The hearings will stand in recess.

[Thereupon, at 4:45 p.m., the hearing was adjourned.]

○

37-791 (200)