S. HRG. 103–933

JOINT SECURITY COMMISSION

HEARING

BEFORE THE

SELECT COMMITTEE ON INTELLIGENCE

OF THE

UNITED STATES SENATE

ONE HUNDRED THIRD CONGRESS

SECOND SESSION

ON

Joint Security Commission

THURSDAY, MARCH 3, 1994

Printed for the use of the Select Committee on Intelligence

U.S. GOVERNMENT PRINTING OFFICE

85–567 WASHINGTON : 1995

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0-16-046656-3

SENATE SELECT COMMITTEE ON INTELLIGENCE

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

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

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

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

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

CONTENTS

JOINT SECURITY COMMISSION

THURSDAY, MARCH 3, 1994

UNITED STATES SENATE,
SELECT COMMITTEE ON INTELLIGENCE,
Washington, DC.

The Select Committee met, pursuant to notice, at 2:35 p.m., in room SH–216, Hart Senate Office Building, Hon. Dennis DeConcini (chairman of the committee) presiding.

Present: Senators DeConcini, Glenn, Kerrey of Nebraska, Byran, and Warner.

Also present. Norman Bradley, staff director; Judy Ansley, minority staff director; Britt Snider, chief counsel; and Kathleen McGhee, chief clerk.

Chairman DECONCINI. The Committee will come to order.

Welcome, Mr. Smith, We thank you for being with us today.

Last May, the Secretary of Defense and the Director of Central Intelligence appointed a Joint Security Commission to develop a new approach to security. Specifically, the Commissioners were asked to assess the security practices and procedures of the cold war era and decide how they could be simplified, made more uniform and less costly.

In response to this, the Commission has produced an unclassified report of 158 pages, which was presented earlier this week to the Secretary of Defense and the Director of Central Intelligence.

We meet today in public session to have the Chairman of the Joint Security Commission, Jeffrey H. Smith, present the Commission's findings and recommendations.

I confess to my colleagues that I have not personally read the report. But our staff has read it, and has highlighted the key points in the summary we have in front of us.

It is clear that this is a very significant report—perhaps the most comprehensive analysis of security practices and procedures that has ever been done.

It is also clear that your recommendations, Mr. Smith, and those of the Commission, are not the standard bureaucratic responses that we've become somewhat accustomed to. They call for sweeping and fundamental change.

We have a system that in my judgment is broke and you are telling us in relatively concrete terms of some specific ways in which to fix it.

Mr. Smith, I think you and your fellow Commissioners are to be truly congratulated for the excellent piece of work you've put together.

That's not to say I don't have questions concerning some of your recommendations, because I do. But overall, I think the Commission has made a very significant contribution.

I am also interested in your reaction, straightforward and candid, to the bill that I introduced yesterday to provide a statutory basis for the security classification system. As you know, my counterpart, Chairman Glickman in the House, has done likewise. A little different bill, but along the same lines. So I'll be asking a few questions on that.

In the meantime, I want to welcome Mr. Jeffrey Smith. He has a long history of credibility in the Senate, having served as legal counsel for the Armed Services Committee and before that as legal counsel for the State Department, I believe. Mr. Smith, thank you for taking the time to be with us today, and for your long service up here. You have been helpful to this Senator on a number of occasions when you worked with the Armed Services Committee, and I will remember that for a long time.

Senator Warner.

Vice Chairman WARNER. Mr. Chairman, I certainly join you in that. We might also add that the our guest today was in the transition office of the President handling basically those departments and agencies dealing with national security and foreign affairs. And so you've had a long and distinguished career of public service. And as the chairman said, we extend our appreciation for what you and your fellow Commissioners have done.

Like the Chairman, I will have some disagreements with you, but at least you have put down a benchmark from whence we can work. And also we jointly apologize to you for the absence of a number of Senators who otherwise would be here. Some 33 Republicans just departed to go off on a seminar on health, which as you know is a current subject of great interest. And the Senate is not on record votes today. So you know that from a good deal of a lifetime here with us.

Thank you very much.

Chairman DECONCINI: Thank you, Senator Warner.

That many Republicans have bad health?

Vice Chairman WARNER: They are working up a little home brew for you and your colleagues.

Chairman DECONCINI: Touché.

Mr. Smith, please proceed.

STATEMENT OF JEFFREY H. SMITH, CHAIRMAN, JOINT SECURITY COMMISSION

Mr. SMITH. Thank you Mr. Chairman.

It is a special privilege to be here today to appear before this, my old committee. And you may recall that I was not only the general counsel of the Armed Services Committee, I was also Senator Nunn's designee to this committee. So I feel very much at home and I am honored to be back here on this side of the table.

As you mentioned, we presented our report, Redefining Security, to the Secretary of Defense and the Director of Central Intelligence on Tuesday of this week. Previously, I briefed the Vice President on our principal findings and recommendations.

As you mentioned, our Commission was established in May of 1993 by Les Aspin, then the Secretary of Defense, and Jim Woolsey, the Director of Central Intelligence. The Commissioners are individuals who may be familiar to many of you. They are listed in the book, but they include Duane Andrews, former Assistance Secretary of Defense for C3I; Bob Burnett, former Executive Vice President of TRW; Ann Caracristi, former Deputy Director of NSA; Toni Chayes, former Under Secretary of the Air Force in the Carter administration; Tony Lapham, one of the early general counsels of the Central Intelligence Agency and a law partner of Jim Woolsey's; Nina Stewart, Deputy Assistant Secretary of Defense in the last administration; Dick Stolz, former Deputy Director of Operations at the CIA; Harry Volz, director of corporate security for Grumman; and Larry Welch, former Chief of Staff of the Air Force and now president of the Institute for Defense Analysis.

Vice Chairman WARNER. How many formal commission meetings did you have?

Mr. SMITH. Senator, I am not sure. We averaged about one meeting a month. But I broke the Commission into subcommissions or subcommittees, which met much more frequently. We held a number of sessions with industry—one in California, one in Massachusetts and one here—in which we invited representatives of industry to meet with us and give us their views on what worked and what did not work. And those were very helpful. We also met with representatives of the public, public interest groups, and with Members of Congress that were interested in this subject.

Vice Chairman WARNER. You had quite a well experienced staff, also.

Mr. SMITH. We did. We had an extraordinarily talented staff led by Dan Ryan, who is here today, and representatives of all of the interested agencies.

I should also say even though our focus was limited to the defense and intelligence community, we had observers from the Department of State, Department of Energy, FBI, Treasury, NSC, and so on. So we invited participation from the other agencies.

Unlike most other commissions, we will remain in place until June 1 to work with the Secretary of Defense and the DCI and Congress to implement those of our recommendation that are adopted. And we look forward to working with you on the bill that was introduced up here as well as any other matters that are of interest to this committee.

The Commission was created because there was broad agreement that the existing security system is inefficient, costly and cumbersome. In Desert Storm, we learned that some information was so highly classified, it could not reach the persons who needed it. In industry, vast amounts of money are spent on duplicative inspections and unnecessary security requirements. It was also clear that our security was not as good as it should be—as was borne out last week by the arrest of the Ames'.

The Commission was asked to review the security policies and procedures of the defense and intelligence communities. I set three simple goals for the Commission:

Find what works and keep it;

Find out what's broken and fix it;

Identify what the future demands and implement it.

Over a 9-month period, as I said a moment ago, we met with a number of individuals.

Our principal findings are:

First, the current security system, which is rooted in the cold war, must be changed. We are spending far too much protecting against threats for which we have almost no evidence—that is to say, Russian agents climbing over the fence at 2 o'clock in the morning—and not nearly enough on matters for which we have plenty of evidence—an employee who stuffs classified documents in his or her briefcase, walks out the front door and sells them to the Russians.

Second, there is no effective method for evaluating the threat and developing appropriate countermeasures.

And third, the development of security policy is fragmented throughout the Government. There is no central mechanism to develop security policy or oversee its implementation.

The principal recommendations of the Commission are:

First, much more must be done in the personnel security field. More attention must be paid to spotting employees who are, or may become, spies.

Second, increased effort must be paid to protecting our Information Management Systems. Our Government is only now beginning to understand the ramifications of this issue. Much more must be done.

Third, a Security Executive Committee should be established, as a subcommittee of the National Security Council, to develop government wide security standards.

Fourth, a new classification of information system is needed. In our view there should only be two levels of classification: Secret and Secret Compartmented Access. This is a radical simplification of the current system which has upwards of 12 different classifications categories.

And fifth, a methodology must be developed to account for security costs. At the moment, no one knows how much we pay for security. It's very difficult to manage something that can't be measured.

I will discuss these conclusions in a bit more detail but first let me set the stage.

Vice Chairman WARNER. Mr. Smith, if I could ask you one question. Our predecessors, Senator Boren and Cohen, were quite active and the result was the Jacobs Panel proposed legislative items. I did not hear you recite in your litany that you reviewed that as a part of your work.

Mr. SMITH. We did not look at it closely, Senator, because that was good they plowed and plowed very skillfully. We do however, endorse what they recommended.

Vice Chairman WARNER. Across the board?

Mr. SMITH. Not entirely. There are some things that I know were controversial when Congress last looked at it. I think clearly certain aspects—namely the—probably the most important is the consent——

Vice Chairman WARNER. Well, at an appropriate place today, you'll make reference to that.

Mr. SMITH. I was planning to discuss it only in the most general terms, Senator. I would be happy to go more into more detail.

Vice Chairman WARNER. Whatever way you wish to do it. But Senator DeConcini and I and others will be looking at that in the context of our own legislation which we hope to introduce in the not distant future.

Mr. SMITH. Well, I think it is very important, Senator, and as I said, I would be happy to work with you and your staff in more detail to take a look at that and see what we think makes some sense.

The first responsibility of Government is to provide security for its citizens. There are, of course, many aspects of that responsibility, including military strength, economic vitality and moral soundness. Our Commission was asked to review one aspect of that security, namely the policies and practices that protect Government information, facilities and people. In a democracy, the people's security also depends on the health of the democracy itself. This in turn depends on careful maintenance of the balance between the right of the public to know and the Government's need to keep some things secret. We hope our recommendations strike the right balance.

The world has changed a lot, as this committee knows better than any, and that must also be taken into account. In some respects the military threat has waned, but the world remains a very dangerous place. The United States remains the most important intelligence target in the world. There are a lot of folks out there who want our secrets and they want more than just political and military information. They want economical, technical, and commercial information. We must protect that information but we must do it better, smarter, and with fewer dollars.

Now let me turn to a more detailed discussion of our report.

In the past, most security decisions have been based on assumptions about threat. Under this approach, we tried to totally avoid all security risks by maximizing our defenses and minimizing our vulnerabilities. Today's threats are more diffuse, and dynamic. There are some situations in which the consequences of security failures are so profound that exceptional protective measures are justified. In others, the consequences are less severe. We urge the adoption of a new philosophy, one that we characterize as risk management, to choose the level of protection necessary. This approach balances the risk of loss against the cost of countermeasures. It should enable the selection of security measures that provide adequate protection without excessive cost.

We were guided by four principles, and I will tick those off very quickly:

First, our security policies and practices must match the threat we face. It must be sufficiently flexible.

Second, our security policies and practices must be consistent and coherent.

Third, our system must ensure fair and equitable treatment of the individuals and companies upon whom we rely to protect our nation's security.

And fourth, the system must provide the needed security at a price we can afford.

Let me discuss some of our specific recommendations. I am just going to highlight those. There are an awful lot more than this, but I want to call out some that I think are the most important.

First, the Commission recommends that increased attention and resources be devoted to personnel security. Personnel security is the very heart of the Government's security system. Safes, locks, fences and guards are useless if we cannot ensure the trustworthiness of those to whom we entrust our secrets.

I will not comment on the Ames espionage case, as such, since it would be appropriate for me to do so during the ongoing investigation and prosecution.

Vice Chairman WARNER. You mean inappropriate.

Mr. SMITH. That's correct Senator. I think you'll certainly understand that. But I can certainly talk about——

Vice Chairman WARNER. No, no, I agree with you. The chairman and I have likewise talked with our colleagues on this committee as well as the Director and we all fully understand the inappropriateness.

Mr. SMITH. Yes. But there are certainly some issues that lay the ground work that I think I do look forward to discussing with you.

The Commission does note in its report, however, that over the past 20 years the most damage to national security has been caused by individuals who are already cleared but who choose to sell classified information to foreign governments or to give it.

The Commission believes that a number of improvements are possible that will increase both the effectiveness and the efficiency of our personnel security system. For example, additional information should be obtained prior to granting an initial clearance. A joint investigative service should be established to conduct background investigations and periodic updates of personnel in the defense and intelligence community and in industry. Such a service will not only be more efficient, it will also ensure that individuals are cleared to a common standard, thus assuring reciprocity.

As the committee knows, one of the great frustrations in the current system is that one organization frequently will not honor a clearance granted by another. For example, recently a contractor needed to reassign 170 employees to work on a DIA contract. Despite the fact that these employees all had current clearances and were on record in the intelligence community's clearance data base, DIA required new personnel history statements from each person and readjudicated each case. After 6 months, only 32 of those people had been processed. That is terrible inefficiency and terrible waste of money. There ought to be one clearance and it ought to be immediately transferable and recognizable.

It is also very important that Government investigators have access to financial information about applicants and employees. In that regard, I urge the committee to support the recommendations of the Jacobs Commission, particularly those dealing with access to financial information. I was pleased to see that Senators Metzenbaum, DeConcini, Simon, and Reid have introduced parts of the Jacobs Commission recommendations, and I understand that Senator Cohen has reintroduced the entire package of recommendations. I hope the Senate will consider and pass legislation along these lines this year.

While reinvestigations provide an important way to monitor the integrity of the work force, Employee Assistance Programs, or safety nets, are also needed to help ensure that personnel do not become counterintelligence risks after they obtain a clearance. Most American spies turn to espionage as a way to resolve a personal problem or a crisis. A few convicted spies have stated at the time they begin spying, they were emotionally distraught and in need of counseling. Better education and training is needed so that supervisors and fellow employees can spot potential trouble. Although only a very small percentage of employees with personal problems become involved in espionage, the damage that can be caused by even one person with sensitive access illustrates the value of programs that help employees resolve personal problems. It's smart to do that on human terms but it is also smart on national security grounds.

The personnel security process has too many forms, too many delays and too many inconsistencies. Personnel security is needlessly complex, costly, and cumbersome. For example, there are over 45 different prescreening forms used in Government and industry that request essentially the same information. The system is not automated. The process used to clear individuals in the defense and intelligence communities vary widely from agency to agency. In addition to establishment of the joint investigative service, we have a number of specific proposals designed to simplify and speed up the clearance process.

We also recommend that personnel security investigations be centralized and automated. To insure the reciprocity needed to facilitate personnel assignments, clearances must be based on a common set of adjudication standards. Using modern information technology, clearance status can be centrally verified, and economies of scale can be achieved by utilizing a common badge throughout the defense and intelligence communities.

This would eliminate one of the greatest frustrations with the current system—clearance verification. The Commission received countless complaints from government and industry about the enormous waste of time and money caused by the need for security officers to verify the clearances of visitors from outside their immediate organization who must attend a meeting or receive a document. I think our favorite story was one that Brent Scowcroft tells in which he, shortly after he became Assistant to the President for National Security Affairs, went to a meeting and couldn't get in because his clearances hadn't been verified. And have I always thought General Scowcroft was a reliable fellow.

The Commission was pleased to learn that homosexuality, per se, is not now and should not be a bar to a security clearance. The nondiscrimination guidelines recently issued by the Attorney General should, in my view, be the basis for the Govermentwide standards that we urge be adopted.

The Commission struggled hard with the issue of polygraphs. Opinions ranged, at times, over the entire spectrum of possibilities from doing away with the polygraph to leaving it alone. In the end, the Commission recommends the continued use of the polygraph by those defense and intelligence community organizations that cur-

rently use it, with some significant revisions in the way it is used to enhance oversight and minimize abuses.

It is not a perfect instrument. Spies have passed it and innocent people have failed it. Too much reliance has been placed on it in the past. But the Commission reviewed much evidence that the polygraph also elicited information from applicants and employees that was not produced by other means. A typical example is an initial applicant who on his or her personal history form states that they used marijuana only briefly in college, but then admits in the polygraph exam that they are an active cocaine user.

Despite our reservations about the polygraph, the Commission concluded, on balance, that it should be retained but with the modifications I have highlighted.

The second major area requiring increased attention and funding is information systems security. The Commission considers the security of information systems and networks to be the major security challenge of the next century. We are concerned that there is not sufficient awareness of the serious dangers that we face in this area. In addition to information systems that must be protected for military and diplomatic purposes, there are lots of information contained in the Nation's infrastructure systems that need protection, including the air traffic control system, power distribution and utilities, telephone system, stock exchanges, the Federal Reserve monetary transfer system, credit and medical records, and a host of other services and activities. Never has this Nation's information been more accessible or more vulnerable. This vulnerability applies not only to Government information, but also to the information, technology, and intellectual capital held by private citizens and institutions.

Increased connectivity is vital for our continued economic growth. We live in and must master the Information Age. But this connectivity also creates great vulnerability. Technology associated with information systems is evolving at a faster rate than information systems security technology. Overcoming this gap will require careful threat assessment, comprehensive investment strategies, and sufficient funding to protect the security of both classified and unclassified information systems. The question of the role of Government in protecting information, particularly in private hands, is one that is extraordinarily difficult. We have no answers. We only suggest that it must be looked at and addressed.

Third, we recommend a radically new classification system that would greatly simplify the current system that has three primary levels—CONFIDENTIAL, SECRET, and TOP SECRET—but with a potential of many different control systems. The chart that we've just flipped over shows how these special access programs are structured and the different types of special access programs that currently exist. So-called bigot lists are lists in which individuals are named by name that are permitted to see information. SCI stands for special compartmented information. That's the Director of Central Intelligence's scheme to control special access programs. DOD SAP, special access programs is DOD's scheme to protect special access programs. These have a way of proliferating and the problem is that they often have authority to make their own security rules and set their own security requirements.

Under our proposed system, classified information would be given only two degrees of protection. Generally protected information would be labeled SECRET and would be subject to ordinary need to know controls. Material label SECRET Compartmented Access would be information and materials requiring a higher level of protection and to which stricter need-to-know rules would apply. A single control channel for SECRET Compartmented Access information using codewords to identify the access list for each compartment would replace all existing special access program and all sensitive compartment information and bigot list control channels. So you will go from this very complicated system on the bottom chart to a very simple system depicted on the top chart. This is very controversial, Mr. Chairman, within the defense and intelligence community. It in a sense would collapse the special access world and the SCI world into a single world with common standards so that there would not be the confusion that exists between the two systems making it very difficult to move information back and forth within the Government and between Government and industry. You'll have one set of standards and criteria that would govern the whole of the special access world.

The potential benefits of our new proposed system, in our judgment, are enormous. The classification system is the operating language of the security system. Many aspects of the system are keyed to the level of protection. For example, adjudicative criteria for granting clearances, physical security standards for facilities, and procedures for handling of documents vary according to the level of classification that is at stake. The complexity of the current system contributes directly to confusion and overlapping requirements and this means barriers to efficient movement of information and wasted money.

But if one boils the current system down to its essence, there are, despite all the complexity, really two levels: ordinary classified information and compartmented information. We are simply proposing that this reality be codified and further simplified. In our view, there should be only two sets of procedures: one that would govern the general information; that is, ordinary secret, top secret, and confidential; and one system that would govern the compartmented world, rather than the myriad of rules that now exist.

Fourth, the Commission recommends that security countermeasures be based upon accurate, timely, threat assessments. The Commission also recommends that, except for very limited applications based on specific threat information, technical security programs, such as the TEMPEST Program, for which we have spent a huge amount of money, be reduced or completely eliminated for domestic applications. And the operations security programs, or OPSEC as it is known, should be integrated into risk management analysis of security issues. In our judgment OPSEC should not be an additional, duplicative program. The OPSEC community has grown a great deal in the last few years, and quite frankly, a number of us had some trouble understanding exactly what they contribute.

Nowhere will the payoff for improving our security policies, practices, and procedures be higher than in the industrial base supporting the Defense and Intelligence communities. The present system

is complex, rigid, inconsistent, and often contradictory. Security requirements imposed on industry often exceed the requirements we impose on the Government in protecting the very same information. There are far too many inspections of the same facility by different Government security agencies applying different standards. In our report we cite some examples of some companies where the number of their Government contracts has gone down but the number of inspections they are receiving has gone up.

In another example, we require companies to account for each and every SECRET document they hold. Vast amounts of time and money are spent in frequent inspections tracing those documents. Yet no such requirement is levied on Government facilities. We are spending all of this time counting the number of secret documents that exist in industry. We ought to be devoting some of those resources to, among other things, personnel security, as I mentioned earlier.

In our view there ought to be one agency, the Joint Investigative Service, which we have suggested be created, that will do the vast bulk of these inspections in industry. They should inspect less often and they should apply common standards.

One of the consequences of this chart that is on the floor now is that the SCI world and the SAP world often have different standards for industry. Large companies that have contracts with both the CIA—with CIA, NSA, NRO, and DOD, will often find different industrial security standards being imposed on them by different parts of the Government—an enormously costly and wasted effort. One agency will require something, say a wall be 12 inches thick. Somebody else requires that it be 14 inches thick and they have to pour 2 more inches of concrete. There are lots of examples like that we think don't add a great deal to security. That money ought to be spent worrying about the disgruntled employee who's going to copy something and walk out the front door with it.

As I mentioned, these different requirements add unnecessary cost and confusion to the security process and we found little reason to treat industry different from Government for security purposes. A partnership is needed between Government and industry to achieve common security goals.

Fifth, the Commission also felt it essential to establish mechanisms that will allow us to trace security costs. Risk management means managers must know how much a given security measure costs. This is virtually impossible because today's accounting system are not designed to collect the costs. The Commission believes that establishing a standardized system to capture security costs is urgently needed. We recommend the creation of a uniform cost-accounting methodology and tracking system for security resources expended by the Defense Department, the Intelligence community, and supporting industry. And I will be happy to talk about costs during the question-and-answer period because I think it is an important issue.

Sixth, and to my mind among our most important recommendations, is the formation of the Security Executive Committee.

As I mentioned at the outset, current security policy formulation and execution is fragmented throughout the Government. This fragmentation is probably the greatest single cause of the confu-

sion, waste, and inefficiency in the system. The chart I am putting up now is what we call the spaghetti chart. This chart depicts the current Government agencies and committees that are engaged in the development and execution of security policy. Many of those are interagency committees that have been established in order to try to coordinate security policy. They have grown up sort of in a very ad hoc fashion over the years, because there is a recognition that security policy is not being coordinated. This is an effort to depict those committees and agencies that are engaged in it.

We strongly urge the creation of the Security Executive Committee as a subcommittee of the National Security Council, to develop and coordinate security policy governmentwide. Existing security policymaking committees should either be abolished or reconstituted as working groups of the Security Executive Committee. The next chart shows the simplicity of the structure we propose.

The committee should be chaired by the Deputy Secretary of Defense and the Director of Central Intelligence because they are responsible for roughly 85 percent of the classified information in the Government. As you know, NSC subcommittees are usually chaired by the agency head most concerned with a given problem.

In our view, the committee should have responsibility to develop common security standards and oversee their implementation. The committee should be advised by a security advisory board of prominent private citizens appointed by the President who will ensure that the system is fair and balanced. This security advisory board could also serve as an appellate board for complaints from the public, including on such issues as whether information is properly classified.

Mr. Chairman, the Commission has recommended many major changes in security processes and procedures. But we hope these specific recommendations will lead to a sea change in the way security is viewed. The Commission endorses a new security policy, one in which security is more customer-oriented and service-driven. Security should be a positive undertaking that values problem prevention over problem resolution and individual responsibility over external oversight and rigid rules. Security should recognize the interdependence of all the security disciplines. Each discipline is critical to overall success but none must be sufficient by itself. We must shift our priorities from those security measures that do not produce results to those that do.

Mr. Chairman, the results of our review show clearly that, some fine and proactive work has already been started in the Defense and Intelligence communities, but much more remains to be done. Many of our Commission's recommendations will be controversial, but we hope they will reduce cost inefficiencies and enhance our security. Most important, we recommend changes in the structure that develops, evaluates, and oversees security policies and a change in the way security is viewed.

This concludes my opening statement and I will be pleased to answer questions and engage in a discussion on particular issues.

Chairman DECONCINI. Thank you, Mr. Smith. I do have some questions, and we will limit them to 10 minutes each so everybody will have an opportunity to get some questions in.

The Commission has produced a 170 page report. On the one hand you say that many security practices which exist today are useless and wasteful and should be eliminated; on the other hand, you say there are things that we should be doing that we are not. You give a few examples of these and I wonder, could you tell us, taking the Commission report as a whole, do you think it makes a case for loosening the security system, or do you view your recommendation as tightening it?

Mr. SMITH. I view our recommendations as calling for a shift in priorities. Moving away from those areas that, in our judgement, are very costly and provide very little security. And by that I mean very expensive and elaborate alarm systems, guards, gates, and fences, and a duplicity of requirements, and spending and shifting those resource areas where there is a high return—like personnel security. One of the things that we found, for example, was one industrial site that we visited had a building that was itself inside a very secure area and in that building there were several different programs. Each of those programs required an individual SCIF. Now a SCIF, for those who might not know, is a special compartmented information facility which is a secure room where highly classified information can be protected. The various competing programs would not let this company use a single SCIF. They had to build six SCIF's inside a single building. Now that is an enormous—in my judgement an enormously wasteful expenditure of our money. And that's the kind of shift we're talking about, Mr. Chairman, where you shift away from some of what we think are unnecessary requirements and use that money more wisely.

Chairman DECONCINI. In your judgement that could be done without mixing up compartmentalized areas of, as in your example, top secret or secret information.

Mr. SMITH. We believe very strongly that compartments are necessary and important.

Chairman DECONCINI. But you could accomplish that, again within your example, without mixing them?

Mr. SMITH. That's correct, Senator. A lot of this can be done with information management systems. You can program computers so that certain information only goes to certain individuals. You can manage it without a lot of the important physical requirements, the very expensive physical requirements that are now levied.

Chairman DECONCINI. Is it your Commission's objective or its recommendation to create more openness or create more secrecy?

Mr. SMITH. It is certainly aimed at creating more openness in those areas where secrecy is not required. That is a very difficult objective to achieve. In my judgment it depends on a change of culture and a change in management. No amount of rules or regulations, whether imposed by the President or the Congress will really change things very much unless people take a different attitude toward and have a different understanding of what needs to be protected. Hopefully the kinds of things that we are recommending and that your bill get at will lead to less classified information.

Chairman DECONCINI. Is it your Commission's recommendation, that it should only be limited to DOD and CIA? Why doesn't it go to other areas? Do you know?

Mr. SMITH. I believe I do, Mr. Chairman. In the early days of the administration, there was talk about having this Commission address the whole of the Government security system. But that proved a bit much to bite off at first; and the feeling was that it would be easier to solve the problems in the Defense and Intelligence community, which had the bulk of the problems, that if you began to deal with the Department of Justice, the FBI, and the State Department and Energy with their statutory responsibilities and their Q clearance, it was just a bit harder.

Chairman DECONCINI. I can understand. I can see the magnitude, because in this Senator's opinion, the whole thing is just out of control. The charts I have back there demonstrate the magnitude of the amount of classified documents we have, and recurring between 6½ and 7 million a year is just unbelievable, and declassifying far less than that. I notice your report does address declassification?

Mr. SMITH. Yes.

Chairman DECONCINI. And would you reclassify everything under these new procedures, if they were adopted, by executive mandate or by legislation?

Mr. SMITH. I would not reclassify it, Mr. Chairman.

Chairman DECONCINI. Redesignate?

Mr. SMITH. That's right. I think there needs to be a procedure to address the huge volume of classified information that currently exists.

Chairman DECONCINI. So you would want it to review it? You think it should be reviewed.

Mr. SMITH. That's correct. I think there needs to be some sort of automatic declassification after a period of time. And as you know, our report recommends automatic declassification after 25 years with six limited categories that would permit some information to be classified beyond that time. But you are quite correct, the existing system drastically needs overhaul.

Chairman DECONCINI. Have you had a chance to look at the legislation that Congressman Glickman and I have introduced?

Mr. SMITH. I have looked at it very briefly, Mr. Chairman.

Chairman DECONCINI. Do you have any views, any initial views on it?

Mr. SMITH. I think, quite frankly, the central question is whether Congress should legislate in this area. And as you know——

Chairman DECONCINI. And what is your opinion? Should it be left to the executive branch or should there be some guidelines in the legislative area?

Mr. SMITH. My initial reaction is that it should be left to the President.

Chairman DECONCINI. To the executive?

Mr. SMITH. That's correct. Yes.

Chairman DECONCINI. Solely.

Mr. SMITH. Although I think that is an issue that needs to be looked at very carefully. My strong inclination would be to give the President an opportunity to produce a new Executive order on classified information, and as you know, one is in the works. I suggest that the Congress ought to take a look at that, and if it is satisfied with it, leave it with him.

My concern, Mr. Chairman, is that the classification system is really central to the way in which the President manages a lot of the aspects of foreign policy and intelligence and military policy. And if Congress begins to legislate in the field, my fear is that—in an era when we are suggesting more flexibility and more simplicity in the classification system and in the security system, if Congress enacts a law, it may become rigid and inflexible. And it is much easier to change an Executive order than a statute.

My concern also is that statutes have a way of growing over time and if the initial statute were to get larger and larger and more complicated, that would make the system more rigid than——

Chairman DECONCINI. Not to be argumentive, and I don't mean to get into a debate in support of a legislative approach, but you're making some very strong, I think, perhaps because they agree with the legislation, suggestions of ten year classification and then renew on a 5 year basis. And it seems to me, not to try to point the finger at any administration or President, or what have you, but this is a problem that the executive branch has created. And even if a new Executive order came out and adopted 50 percent or all of your recommendations, it seems so easy for another Executive order to come out and modify it and not have any parameters of where you should be going.

And my feelings were that you could do something legislatively, but leaving enough leeway, particularly with the President having absolute authority to extend it forever or in perpetuity if in his judgment it was necessary. I'm just bewildered, as I got into this, to see what a mess it is, and how the fact that it is not an issue that is of paramount importance at the White House, I don't believe, or in these agencies, is just so easy to let it go along. But Executive orders, I think, have a way of growing, too. Now, I only throw that out for perhaps your comment, or just my own self-gratification.

Mr. SMITH. I'm sort of 52 to 48 on this one, Senator. 52 percent says leave it with the President, but I've participated in the drafting of several Executive orders on classification of information when I was in the State Department and then again when I was up here, and I know exactly the problem that you are addressing, and frankly the administration has not done as well as it ought to have and one would hope that your legislation, whether it passes or not, would serve as a clarion call to the administration to get it right this time.

Chairman DECONCINI. I'm really pleased, because I have heard so many complaints from defense contractors, and we will have testimony as we conduct hearings on the legislation, where they have purchased a building and had to spend twice the capital investment to maintain the security requirements for the black programs that they operate than they did buying the building in the first place, or building it, when they didn't know they were going to do classified programs in them. So I am pleased that you not only investigated this, but came up with some of the exact examples that you have.

Mr. SMITH. Thank you Mr. Chairman, I think that is one area that we can rapidly save a lot of money and outlay money.

Chairman DECONCINI. Because the contractors charge that back, right?

Mr. SMITH. Absolutely.

Chairman DECONCINI. It isn't anything that they are absorbing out of their profits that they would be reporting at the end of the year. I yield to the Senator from Virginia.

Vice Chairman WARNER. Thank you Mr. Chairman. I'd like to pick up on Chairman DeConcini's thought here. If you change a system to update DOD and CIA how do they then interface with other agencies that they must work with on a daily basis. It is sort of like coupling up railroad cars which have different couplers and they are operating on different tracks. How do you work that system out?

Mr. SMITH. Well, clearly, the classification system will have to be governmentwide.

Vice Chairman WARNER. Well, that is a key point there. You are using this as a model study of two agencies with the thought in mind that the actions taken by the executive and legislative branches would be Government wide.

Mr. SMITH. That's correct.

Vice Chairman WARNER. That's clear.

If it were left only to the executive branch through an Executive order, how would you invoke the appropriate penalties? Penalties are needed to be a deterrent to make the system work.

Mr. SMITH. I noticed that the version of the chairman's bill that I saw had sanctions in it.

Vice Chairman WARNER. That's in the legislation side.

Mr. SMITH. That's correct.

Vice Chairman WARNER. I thought you said you were 50 to 48, leave it to the executive branch.

Mr. SMITH. Well, certainly of the 48 percent that is on the side——

Vice Chairman WARNER. You mean the division of the work, the labor?

Mr. SMITH. I'm sorry, I didn't mean to be flip, Senator. In my mind it is a close call as to whether Congress should legislate in this field or not.

Vice Chairman WARNER. But if Congress does not, then how do you get the appropriate penalties to act as a deterrent?

Mr. SMITH. That's a very good point, Senator, and it may be at a minimum that Congress ought to enact penalties. That's a good point.

Vice Chairman WARNER. On page 13, I will read it to you—don't have to take time to refer to it—you say, "Fourth, the Commission recommends that security countermeasures be based on accurate, timely threat assessments." Now, Mr. Smith we worked together here in this institution about 10 years. I don't know how many threat briefs we sat through in the various committees—primarily Armed Services and this committee—and you know that no matter how hard people labor, there isn't any such thing as an accurate—or very rarely, an accurate assessment. It is the best judgment rendered by professionals. But I have rarely seen the word accurate applied to them.

Mr. SMITH. It is a real problem, Senator. But the difficulty is that the current system is based—particularly in industrial security on a rigid application of the industrial security manual. For example, it would require the same kind of security protection for a building located right next to the Russian consulate in San Francisco as would be required of a building in the middle of Nebraska. And what we are suggesting is the threat this much greater if you are across the street from the consulate than if you are in Nebraska. There ought to be some ability to take that into account.

Vice Chairman WARNER. And I think you are absolutely correct on that. But I was thinking as to whether we should classify anything secret, or under your system secret whatever it is, as opposed to not classifying it. And it is awfully hard to predicate it on an act, a threat assessment.

In other words, I think a lot of our classification errs on the side of caution. And I do not, as I carefully followed your presentation, detect that you want to loose that erring on the side of caution.

Mr. SMITH. You could tell by the commissioners, Senator, were all are very conscious of the need to protect information. That particular reference to threat assessments and measuring the risk deals, I think principally, with physical security to try to get—you know, where there is no need to overdo it.

General Welch, one of our commissioners, was found of telling the story about the thickness of the doors that had to be built on the missiles sites in North Dakota. And it was just in his view——

Vice Chairman WARNER. Excessive.

Mr. SMITH. Yes.

Vice Chairman WARNER. Let's turn to the limited way in which we can today make reference to the *Ames* case. Any of these recommendations in your report that would have helped preventing this type of security problems, to the extent that we understand it?

Mr. SMITH. Yes, we think very much so, Senator. As I said even before the *Ames* case broke in the press, we were aware that there was an additional need to focus on personnel security issues—plain, old fashioned, non-dramatic counterintelligence work. We need to do more periodic updates on those individuals who have access to the most sensitive information. We need to have a way of catching those individuals who have a personal problem or a crisis, for whatever reason, and spot them early. We need to be more attentive to financial considerations. We need to be more aware of individuals who, for one reason or another, have had a change and need to be watched.

We had made those recommendations, and I think the *Ames* case, if it has a silver lining, should serve to point out the need to further emphasize those very techniques.

Vice Chairman WARNER. In the very limited framework of the comments I've made on the *Ames* case, I've tried to express an interest I personally have, that there are really two ways to get at a problem of the *Ames* problem. In other words, you've got to have persons in the very sensitive areas of our Government, in my judgment, subject to further scrutiny. Now, each time you scrutinize, you sort of take away a measure of personal privacy, personal dignity, other attributes, so there has to be balance.

Based on your extensive experience in Government, out of Government, in your own work in the legal area, cannot much of this be accomplished if the employee wishes to voluntarily sign a waiver as opposed to passing a framework of laws and having them promulgated by head of the agency?

Mr. SMITH. Yes. One of the feature of the Jacobs' recommendations is that individuals sign consent forms.

Vice Chairman WARNER. That's correct.

Mr. SMITH. And I think that is an excellent idea.

Vice Chairman WARNER. In other words, if an individual desires to serve our Nation in certain areas of tremendous sensitivity, he or she would have to balance their own lifestyle, and to the extent it could be invaded in certain ways, versus the necessity to give every appearance as working in this system of security.

Mr. SMITH. That's right. I think it is important, Senator, that we not over react. We have countless numbers of honorable men and woman who work terribly hard for the security of this nation, and we should not impugn them or overreact and infringe upon their dignity and their individual rights in response to the *Ames* case.

My view is there is some fine tuning that needs to be done and some shifting of emphasis that clearly needs to be done. But we should not overreact.

Vice Chairman WARNER. On the other hand, I can assure you that down in the crossroads of my State, they cannot comprehend how this *Ames* case could have arisen, given their lifestyle and the flamboyance in which they did things.

Mr. SMITH. Senator, we are from the same State, and those are very hard questions to answer.

Vice Chairman WARNER. They are.

Automatic declassification. For the vast majority of classified information, you recommend automatic declassification after a decade. The only exceptions that are allowed must be specifically approved by a newly created agency, the Security Executive Committee. This seems like a rather cumbersome process which could well result in the declassification of information that should remain protected. How does this new declassification requirement contribute to the security of our country?

Mr. SMITH. That's not what we quite intended, Senator.

Vice Chairman WARNER. Well, then I may well have misinterpreted.

Mr. SMITH. The thought was that there would be, as we said, a presumption that all material would be declassified at 10 years, except material falling in categories pursuant to guidelines issued by the head of the Department. So that the Secretary of Defense, the DCI, the Secretary of State, could issue guidelines that would say what kinds of information could be extended to 25 years. Now, we think those guidelines should be reviewed by the Security Executive Committee, because we think some oversight is necessary. But clearly, my concept of this is that there be increasingly narrow funnels, so that at bottom, there would be very little that would remain classified.

At 25 years, I suggested that we specify in the Executive order or in the law, if that is the course that the Nation follows—that there be very narrow exceptions for information that would be clas-

sified beyond 25 years. And you can imagine what those are. Information on sources and methods that are particularly sensitive; military operations that would be still sensitive after 25 years; certain kind of technology that remains sensitive after 25 years and so on. But very narrow categories of information.

Vice Chairman WARNER. I have another area in which I think some clarification is needed, and that's risk management. In your report there are numerous references to, "risk management." This implies to me that the Commission is willing to accept some degree of risk to security of the United States as a consequence of its recommendations. How did you assess the acceptable level of risk?

Mr. SMITH. What we are saying, Senator, is that in the past we have overdone it. We have tried to protect everything against everyone, and in so doing we have not protected those things that really need protection. We do think that there is, admittedly, some risk if you lower the current standards particularly in physical security and technical security where the bulk of the money is spent. Tempest, for example, is a good case. For facilities that aren't anywhere close to a hostile intelligence service operating area, such as most areas in the United States, there is really very little need to require the extraordinary costly facilities that Tempest calls for. Shielding and everything has to be in tubes and so on. There is virtually no evidence of efforts by foreign intelligence services to collect in this country, that require Tempest. So in our judgment there isn't the need to spend that kind of money. So we are suggesting that, looking at a given facility, measure against what threat we know of, permit program managers, permit base commanders to make some judgments to how they want to spend their money, and not require them to comply with a rigid manual that doesn't permit that kind of flexibility. That's really what we are talking about.

Vice Chairman WARNER. I thank the witness very much. Forgive my absence, I must join others to work on the health plan. Thank you very much and may I commend you and your Commissioners and your staff for a very good piece of work. I am confident that out of it will come a measure of increased work on this in the Government. It is cost savings, both in the government and in the private sector.

Mr. SMITH. Thank you, very much.

Chairman DECONCINI. The Senator from Nebraska, Senator Kerrey.

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

Mr. Smith you really have produced and the Commission has produced a very fine report, and I look forward not only to reading the details of it, but working with our and other members of the Commission to see that these recommendations are given full consideration and we have a chance to discuss them further.

Mr. SMITH. Thank you.

Senator KERREY of Nebraska. You are, in your executive summary, calling for the creation of the new security structure. I mean, you are really not just talking about tinkering with the system. You're saying that the world is changed, that the nature of the threat has changed, the nature of the technology has changed, and as a consequence for reasons of efficiency—that is to say, continu-

ing to protect the interests of the United States of America and for reasons of cost—that we have excess costs both in the taxpayer side as well as the private sector side, and for reasons of adjusting to the new technologies that are now available to us, that we need this kind of structural change. Indeed, that there is an urgency to do so. I'm asking you if that is a fair summary of what you have said?

Mr. SMITH. Yes.

Senator KERREY of Nebraska. Let me address a couple of areas in those categories. One, in the threat area, it seems to me that we need some additional deliberation on this matter so we can understand what it is we are talking about. For example, we talk a great deal, and I think correctly so, about the potential nuclear threat from nations such as North Korea that make a decision not to abide by the Non-Proliferation Treaty, and that, for obvious reasons, is of great concern to the country. And we monitor that at great expense to the country and try to not only monitor but take action to prevent that from becoming a reality.

It also seems to me, Mr. Smith, that the world has allowed relatively small arms to terrorize us as well. I mean, we saw that in Sarajevo—a 120mm mortar hit the market place in Sarajevo and the entire world saw it and it affected our policy. In this case, it seems to me that the response of the President, the response of NATO, response of Russia, has been positive. But it was the seeing of that incident that provoked the response. At least that is how I view it.

Similarly, in Mogadishu, it was the seeing of an American being drug through the streets, the seeing of that provoked a dramatic change in the allied policy. It was the seeing of the scene in the Cave of the Patriachs in Hebron that produced a change in policy as well. And unfortunately, it appears to be going in the wrong direction, although one can't be certain.

All I'm suggesting is that this is basically a small arms issue. This is not an issue where our policy is changed as a consequence of fearing obliteration from nuclear weapons. And I think it is important for us to focus on that, and I am not asking for your response to it, but I think it is important for us to focus on it because taxpayers are constantly asking us, as members of the Oversight Committee, why do we continue to spend all this money? What's the threat, what's the issue here? Isn't the Soviet Union gone? Are the security people basically looking for a new mission that really is not there? Or is there indeed a list of new threats that pose a special problem to us that not only require a continued investment, but present the urgency that I at least feel in this report? I mean, you've come with a considerable amount of urgency for the need to restructure again, in category one, so that we can do the job.

Mr. SMITH. The point, Senator, is that the threat has clearly changed. And we—I think I mentioned before you came in, the United States remains the most important intelligence target in the world. Everybody wants to take our secrets, whether they be—you mentioned nonproliferation—whether they be technologies that would assist in the production of nuclear weapons or other weapons of mass destruction, or chemical weapons, we remain an important target.

What we are suggesting is not more spending. We are suggesting shifting priorities. Our task was to try to take what we have and spend it smarter. We are clearly wasting a lot of money on security measures that don't really provide security. We have not really addressed the broader question of how should the United States respond to all of the change in the world. Our focus was a bit more narrow. But in my judgement it would be—we simply need to shift our priorities.

Senator KERREY of Nebraska. Well, I hear you saying though in your report that the current structure of our security system is inadequate to meet the challenges that face us today, the threats that face us today.

Mr. SMITH. That's correct. And the reason is we think it is too rigid, that it is based on cold war mentality, and we focused very much on issues like industrial security. And by that I mean, what is industry required to do to protect itself from somebody trying to steal its secrets.

Senator KERREY of Nebraska. Let me be a little bit more precise. If I say that the cold war is over, everybody understands what that means. That the Soviet Union has broken up, that they now have turned their missiles away, and that we got new cooperation with the newly independent states, and that the administration has worked out an agreement with Ukraine, and we begin to understand that that security issue has changed dramatically, that the potential for an annihilation of the United States of America and the complete loss of our independence and freedom, that the potential has been substantially reduced—perhaps not completely eliminated—but substantially reduced. So that is a change. We understand that. We see that change.

Have there not been other changes that perhaps we haven't put enough attention into that have been real changes? For example, I would argue and I would appreciate your response to it, that there were two big changes that occurred in the 1980's that now pose particular security problems for us. One is the introduction of crack cocaine. I mean, that's a new problem. It is been felt as an invasion in Omaha, NE, to law enforcement officers. And there are in every single large community in America, there will be killings over the weekend as a consequence of the introduction of crack cocaine. Perhaps we now view it as squelch and background noise, but I think that is a big change.

I also think that the development and the mass production and the distribution of the personal computer is a substantial technological change. It is not small. It is big, with large implications not only for what we have to protect against, but for what we have to do to organize our intelligence work.

Do you agree? Do you see these two things as changes?

Mr. SMITH. Absolutely, they are clearly changes.

Senator KERREY of Nebraska. Let me ask a couple of questions. You say in your report, you stress the security challenge posed by the ever expanding information highway, and you say, "we have neither come to grips with the enormity of the problem, nor devoted the resources necessary to understand fully, much less rise to the challenge." That is in the report.

Yet the administration has devoted a considerable amount of time and energy to developing hardware, specifically the clipper chip, to supposedly provide security for information transmitted by computer. And I would just like to ask you, do you have an opinion on the clipper chip issue? And it appears that you are saying that clipper chip is an insufficient response.

Mr. SMITH. We did not dwell at length on the clipper chip issue because others were looking at it and we saw no reason to replicate what they were doing. The clipper chip is limited, as I understand it, Senator, to encryption issues. We are talking about broader issues. That is to say, the vulnerability of information systems in the United States to either collection by other governments or worse, manipulation or attacks. Air traffic control, the banking system, all of those systems and how they are linked together. And it's my understanding that the clipper chip only goes part way toward resolving the issues that are presented by those kinds of systems.

Senator KERREY of Nebraska. Second question, Mr. Smith. Again in this sort of this new technological age here and although I have a great deal of interest in it, I don't pretend to be a technological expert. I am intrigued, though, by the increasing use of open source information to make intelligence decisions.

Mr. SMITH. Yes.

Senator KERREY of Nebraska. I am intrigued as well by the possibility of using what I know is Secretary Perry's belief that increasingly we are going to have to develop a dual use technological strategy. In other words, the technology that has an application for our military and national security uses should also have an application for private sector. That is a philosophy I think that Dr. Perry as well as President Clinton and Vice President Gore have talked about, seems to me be a guiding principle of the administration, and I think a correct one.

I'm intrigued by the possibility that the principle could be used in the intelligence area to inform decisionmakers such as myself and the President and others who are having to make national security decisions, and battlefield commanders who similarly having to make national security decisions, as well as law enforcement people who are making decisions as how to protect this country.

I am intrigued that it is possible for us not only to provide information and inform those decisionmakers, but that it might be possible for us to use that some technology to inform 250 million decisionmakers called citizens of this country, who are also having to make decisions on a variety of issues.

For example, we came, I think relatively close, dangerously close, to a confrontation with North Korea. It appears that that crisis has passed. But my own thinking was last week that if there wasn't a blink, that it wasn't outside that the range of possibility we could be involved in a land war on the Korean Peninsula. And I think the American people are not prepared for that. Not prepared for that at all. And not prepared as a consequence of this continuation of a presumption that I have got to use these sensing devices and so forth that we have to inform me and then I am expected to turn around and interpret what I have just been shown to the citizens, and I either am incapable sometimes of interpreting, which is apt to be the case, or I am nervous about what I can or cannot say,

and so I say nothing. And as a consequence, the American people are not informed.

So I am intrigued by the possibility that I could use the technologies that we absolutely need to continue to perfect and improve upon for national security reasons and intelligence reasons, that I can use that technology as a means to inform the citizens, thus sort of completing the loop of this open source effort. I appreciate your comments on that.

Mr. SMITH. I think that is very important, Senator. In a democracy there is nothing more important than the people understanding what is at issue. I think your comment about North Korea is especially timely, because I think there was insufficient understanding of the risks and the dangers, and we came pretty close in my view.

But you are right that we need to do more with open sources, both in terms of collecting and understanding from open sources and in making intelligence information available and part of the public debate. One of the things that we recommended is that there be more use of what are known as tear lines. That is to say, when a document is produced by the intelligence community, there be a line drawn across the page and above the line is the sensitive information—that is to say, where it came from, the source or the method that was used to obtain it—but below the line is the information that was collected or the analysis that was performed. And if you could do more of that and have those individuals who need to know the entire the body of the document—that is to say, in order to evaluate it, need to know where it came from—then they can see the whole thing. But the rest of the document, below the tear line, could be made available in a much wider form, including much of it that can be unclassified and used as part of the debate.

I know that Jim Woolsey is very interested in having intelligence information more widely available and part of the public debate and he is trying to do what he can to push old information out the back—that is to say, information that is currently classified, get it out for historical review—some of which had relevance to today—but I think also interested in making it more available to the public.

Senator KERREY of Nebraska. My time has expired. Mr. Smith. If the chairman would indulge just to close, my interest for over a year has been in the imaging area, and thanks to the chairman and the ranking member of the committee's holding hearings on this thing. I think we've begun to move the ball a little bit. But I am genuinely enthusiastic about going further. I really think that this idea that citizens of the United States of America have a very high obligation to become informed and that I have a sacred right to inform them, that is not privatizable. I cannot privatize that obligation. I have an obligation to inform the citizen. And connected to that is the opportunity to use images to get that job done.

Chairman DECONCINI. Thank you, Senator.

Mr. Smith, going to a couple of other areas, in your report, Which as I said, I have not read, nor did I ask my staff this question, did you find that any of these agencies contracted out for security investigations?

Mr. SMITH. Yes, some agencies do. And they have done it because they don't have confidence in the existing background investigation conducted by various agencies.

Chairman DECONCINI. That is very confusing to me. Did the CIA do any contracting out?

Mr. SMITH. To my knowledge, the CIA does not. I believe the NRO does.

Chairman DECONCINI. The NRO does. And is that because—who would they normally use?

Mr. SMITH. Normally they would use the Defense Investigative Service.

Chairman DECONCINI. I see.

Mr. SMITH. But they decided to contract out.

Chairman DECONCINI. So there obviously is a need for one central, or maybe not one central, but need for some universal standards on what various agencies would do when they do a background check. Is that within your recommendation?

Mr. SMITH. Very much so, Mr. Chairman. The problem is there has been an effort over the years to do that, but it has not worked.

Chairman DECONCINI. Yes. What efforts have there been to do that?

Mr. SMITH. Well, there was an Executive order signed by President Bush which called for a single scope background investigation [SSBI], with the idea that everybody would have the common—everybody would apply common standards. But that hasn't worked, because every agency has decided that their information is more important than the fellow down the street, and therefore, they have layered additional requirements on it, or they don't believe that the adequacy of the investigation conducted by that fellow's investigation agency is appropriate, so they have to reinvestigate. And that's one of the problems.

Chairman DECONCINI. So nobody was designated to write those standards, nor was it an order that all agencies adopt unwritten standards, but the standards should have been put together. Is that where it broke down?

Mr. SMITH. I don't know exactly what caused it to break down, Mr. Chairman, but it broke down and it hasn't worked, and it needs to be fixed quickly.

Chairman DECONCINI. Going back to an Executive order, do you think an Executive order could accomplish that without some legislation?

Mr. SMITH. It should, Senator. We think that, again, the establishment of this committee that we have urged, the Security Executive Committee, would have as one of its responsibilities to ensure that sort of thing happened.

Chairman DECONCINI. Would that be the oversight or the overseer or the enforcer, in essence——

Mr. SMITH. That's correct.

Chairman DECONCINI. They did adopt it.

You talk about the special access program.

Mr. SMITH. Yes.

Chairman DECONCINI. Explain to me how that would work in highly technical black areas that you might have a contractor who would have three. You gave an example of limiting what would be

accessible on the computer. Would you still have to have separate storage rooms?

Mr. SMITH. I think separate storage rooms, yes, and I think separate areas in a building that would govern a particular program, of course. But what troubled us was, as I said, this one instance in which the contractor or the program managers for different programs insisted on having six SCIF's in a single building. That just seemed to us really overkill. And we are strong believers in compartments. One of the things that we recommend is that there be increased effort—and we suggest that the Defense Information Agency—Defense Information Systems Agency [DISA], be the one that is responsible for developing increased ability to audit the way in which information moves within an information system. So that if, for example, to stay in the industry example, if you had a company that had six black contracts, that if you had an individual who was cleared for one of those programs, if he or she suddenly began requesting lots of information from the other programs, that that could be spotted early on. We currently do not have the availability to do that without a huge effort. We ought to devote money to try to figure out how to do that.

Chairman DECONCINI. Do you have a feeling or know of any instances where you think that is occurring?

Mr. SMITH. Yes.

Chairman DECONCINI. You do? Did you do something about those, just out of curiosity? Can you—I don't mean here, but——

Mr. SMITH. We would be happy to talk to you in private about that, Mr. Chairman.

Chairman DECONCINI. I would like to see that that is turned over to somebody, because it leads me to my next question or my real question is in the course of this. You probably found a number of areas that were at least questionable as to present security standards, did you not?

Mr. SMITH. I'm not sure we did quite in so many words, Mr. Chairman. We didn't find any areas that gave us grave concern about areas where there was not adequate security other than, as I keep emphasizing, that we haven't done enough about individual personnel security. We've overdone it on the physical and technical side and we need to shift resources and effort back to plain old good personnel practice, you know, watching out for your people. A good commander is always suppose to know what's going on in his unit. A good manager in Government ought to be doing the same, so that he or she ought to know if they've got a problem.

Chairman DECONCINI. Let me try to understand what your report did. Maybe it did two things. It dealt with this problem, I'll say problem A over here, of a massive amount of classified information and how to review it, how to get it reclassified if necessary, when it should end, what procedures should be utilized and who should enforce them through Executive orders. Is that fair to compartmentalize part of your report?

Mr. SMITH. Yes, that's correct.

Chairman DECONCINI. Now then, your report also dealt with the personnel security and how you should monitor, and how you should investigate and approve or disapprove someone who is being considered for the classification system?

Mr. SMITH. That's correct. We dealt with that issue as well, yes.

Chairman DECONCINI. So the legislation that Chairman Glickman and I have introduced only deals with part A.

Mr. SMITH. That's correct.

Chairman DECONCINI. And legislation I would like to introduce and work on, along the Jacobs Report, deals with your part—I will just call it part B.

Mr. SMITH. Yes.

Chairman DECONCINI. So you have two distinct areas here that you have dealt with—and maybe more that I have missed—but there are two distinct areas. Do you consider them distinct, too? Is that different than the other, or must they be folded together if you are going to try and do a comprehensive effort?

Mr. SMITH. They clearly relate to one another. For example, the classification system, as I said, is the language of the security system. An individual is granted a clearance to a certain level. The standards to investigate and adjudicate under the current system are pegged to the different levels. In order to get a secret clearance, you have to have a certain amount of background investigation. To get a top secret, you need additional investigation. To get a top secret codeword you need something beyond that. So A and B are related. And there is much overlap between the two.

Chairman DECONCINI. Your Commission report does not give recommendations that were dealt with specifically in the Jacob's Report, that is, financial disclosure, is that correct?

Mr. SMITH. We only touched on it, Mr. Chairman.

Chairman DECONCINI. There was a reason for that?

Mr. SMITH. Well, the reason was, as I said, the Jacobs Commission had done this. I met with Mr. Jacobs and we talked about this, and I talked to the Director, Jim Woolsey, about it, and it just seemed that given the shortness of time that we had to devote to it, it wasn't a good use of our time to spend a lot of time on those questions.

Chairman DECONCINI. Mr. Smith, do you know off-hand other areas that you didn't get into because they were covered in the Jacobs Report, or would you care to supply that to us?

Mr. SMITH. I would be happy to give you a bit more on that, Senator, but we didn't look at all of the issues he raised which were—for example, we didn't look at whether the espionage statutes should be amended to make it a crime to sell classified information to a foreign power. As you know, that is currently not a crime. You have to have intent to harm the national security—we didn't look at that, because he had already done it. There were some other areas that we really didn't get into.

Chairman DECONCINI. Well, I really appreciate the effort of this Commission. I think it is most timely, and I just hope that, if nothing more, at least by Executive order, we see some change in this thing. It is most disturbing to me and it has gone on for so long. Obviously, other administrations have thought about and even put paper and ink together, but nobody has ever done much to see that there be some simplification or modification or something, and maybe this will be changed.

Mr. SMITH. Let me commend you, Mr. Chairman. In the past there has been some talk in Congress about legislating in this area.

But your bill is more serious than the others, than the previous efforts, it's gotten much more attention. It will be taken much more seriously on the other end of Pennsylvania Avenue because of your leadership and your position.

Chairman DECONCINI. I thank you, Mr. Smith. I think some of it has to do with the present circumstances of the *Ames* case and what have you, and timing is everything. Due to the Jacobs legislation, which I had forgotten about until all of this came up, tell you the truth—I was on the committee. I realize that it was just timing, that well intended legislation by Senator Boren and Senator Cohen just kind of dropped aside because of the Berlin Wall coming down and the euphoria that, hey, we don't have to worry anymore. But indeed we do.

I have no further questions.

Before I have to leave, I would like to submit for the record the statement of Senator Bryan, and have it included in full.

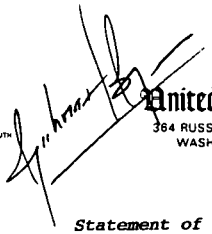
[The prepared statement of Senator Bryan follows:]

RICHARD BRYAN
NEVADA

OFFICES
300 BOOTH STREET
SUITE 2014
RENO, NV 89509
(702) 784-5007

300 LAS VEGAS BOULEVARD SOUTH
SUITE 1110
LAS VEGAS, NV 89101
(702) 388-6605

600 EAST WILLIAM STREET
SUITE 304
CARSON CITY, NV 89701
(702) 885-9111



United States Senate
364 RUSSELL SENATE OFFICE BUILDING
WASHINGTON, DC 20510-2804
(202) 224-6244

COMMITTEES
BANKING, HOUSING, AND URBAN AFFAIRS
COMMERCE, SCIENCE, AND TRANSPORTATION
ETHICS—CHAIRMAN
INTELLIGENCE
ARMED SERVICES

Statement of Senator Richard H. Bryan
before the Senate Select Committee on Intelligence
on the Joint Security Commission Report
3 March 1994

Mr. Chairman: I appreciate the opportunity to review the work of the Joint Security Commission and their analysis of security practices and procedures. I have a number of concerns on this issue, and I am very pleased that the Director of Central Intelligence and the Secretary of Defense initiated this review. I also commend Mr. Jeffrey Smith and the members of the Joint Security Commission for their work.

The national security of the United States requires that certain information is not openly available. American lives and the lives of our Allies could be put in needless danger if certain information became publicly available. However, as the Commission Report points out, there are a number of significant problems with the current security structure.

This debate is particularly significant given the recent events surrounding Rick Ames, and the disastrous results of his actions. This case has led to serious questions in my mind regarding the ability of the CIA and other agencies to find out personal financial information from those who are entrusted with national security secrets. I know this issue has already been addressed in legislation introduced by some of my colleagues, and I feel we in the Intelligence Committee must take a comprehensive look at some changes that will prevent a situation like the Ames case from ever occurring again.

However, I want to focus my remarks today on the issue of excessive classification. It is indisputable that some information must be kept secret to protect our national interests. However, the recent initiative by Secretary of Energy Hazel O'Leary has provided clear evidence that information about unconscionable experiments were kept from Americans, all in the name of security. Yet, it is difficult to avoid the conclusion that this had less to do with security and more to do with evading responsibility. It is also clear that we have an inadequate procedure for declassifying information that no longer requires classification.

The public has a right to know where it's money is being spent. We are elected by the public, and supported by the taxpayer. Unless there is a continuing national security interest, information of interest to the public should be

declassified after a reasonable amount of time. For too long, we have kept information from the public that they have every right to know.

On December 7, 1993, the Department of Energy released information on 204 unannounced nuclear tests that were conducted at the Nevada Test Site. Thirty seven of these previously unannounced tests involved the accidental release of radiation. These nuclear tests occurred as far back as 1963, yet their occurrence would still be classified if it were not for the DOE openness initiative. Thirty years later, Nevadans who live in proximity to the Nevada Test Site have a right to know what happened there.

I cannot help but wonder what other information that has no relation to our national security interests is still classified -- information that would be extremely valuable to the public.

The classification system is out of control, and the cost to the taxpayers of the current security system is too high. With hundreds of different ways to protect our secrets, we have many overlapping and unnecessary regulations. The procedures for protecting secrets differs from agency to agency, and sometimes even from program to program. Yet, the Joint Security Commission found that we do not even have a system for isolating and determining the costs of security.

This situation makes the assessment and management of the security system nearly impossible. We need a common framework, both to cut down on the costs, and tighten the procedures to ensure important secrets are not disclosed.

I want to commend Senator Deconcini for introducing legislation that addresses a number of the problems that I have mentioned, and I am pleased to be a cosponsor of this legislation. The public has been unnecessarily kept in the dark for too long. It's time to create a new, simpler system that maintains security, but gives the public the information they deserve.

Thank you.

Chairman DECONCINI. Does the Senator have any other questions?

Senator KERREY of Nebraska. I do, Mr. Chairman

Chairman DECONCINI. If so, I am going to let him close the hearing.

Senator KERREY of Nebraska. You are?

Chairman DECONCINI. Yes, get used to being chairman next year.

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

Mr. Smith, you made in fact a comment that I was going to make, and I will just reinforce it, that a good manager, a good commander needs to know what's going on with the troops, and needs to become sufficiently intimate that they know if there is a change in behavior and what that behavioral change might mean. I mean, they watch for stresses in family, watch for recent divorces, watch for changes in patterns of behavior and record it, because they know that the lives of the other troops depend upon everybody pulling their full weight, and there are consequences for commanders who don't watch in that fashion. They suffer the consequences.

And I would just ask you, are there any career consequences for a boss or manager whose employee we later discover to be disloyal?

Mr. SMITH. Not to my knowledge, Senator. I think it's a difference in culture. I think in the military the appreciation for that is at a higher level. I mean, I started out as an infantry officer and it was hammered into us from the beginning. In the Intelligence community, the culture is a bit different. And I think there is a recognition that they are all part of the family and there is a kind of—one trusts one's colleagues and there is a certain tolerance and that maybe we need to think again, not to suggest that you should distrust your colleagues, but you should view—maybe the attitude ought to be closer to that that the military commanders have which is that your really need to watch out for your troops and make sure that you take care of them, because the mission depends so importantly on their performance.

Senator KERREY of Nebraska. I would go so far as to say, Mr. Smith, this really is not a question of distrust, it is a question of trying to assess what's at risk, and being intolerant of sloppy behavior, lazy behavior, which from my discussions with people is present in this case. And you say well, that is a special culture of the agency. And perhaps it is, and perhaps part of it is born of the necessity of their operations and the need to operate in secret. But it does seem to me in this case it just went too far, and as a consequence of letting their guard down, got in trouble.

Mr. SMITH. You said it better than I, Senator.

Senator KERREY of Nebraska. Let me ask you a few questions about this Security Executive Committee you have identified as the most important recommendation, is that correct?

Mr. SMITH. It's one of the two or three that I put at the top, yes.

Senator KERREY of Nebraska. Let me start off with a suggestion that you made—I'm not sure if it was in the testimony because you appeared to reference it without looking at the notes, but maybe you had it both written and looked at it earlier—that this committee may have appellate functions.

Mr. SMITH. Yes.

Senator KERREY of Nebraska. Have you thought that through? It seems to me that is a completely different function. It does seem to me a function that needs to be done by someone, but I question whether an executive committee would have the capacity to make appellate decisions as well.

Mr. SMITH. What we have in mind, Senator, is that the committee, perhaps with some participation from the citizens on the Security Advisory Board, could handle appeals from members of the public with respect to whether or not information is properly classified. In Mr. DeConcini's bill, there is a mechanism for a member of the public to write to an agency and say I want classified information—I want information on such and such a subject, and that would then be reviewed by the agency and there would be some way, if it was denied, a way of appealing up through the agency.

We are suggesting that that be taken a step further, and there be an appellate body at the national level that would handle appeals, perhaps from the agencies, on classified information. There may be other areas where they could also serve an appellate function. And we thought about that a little bit, but as we said, we remain in existence until June 1, and so we wanted to see what the reaction in the Defense and Intelligence Community was to this suggestion. But at least in the area of classified information, we thought that this was a useful function.

Senator KERREY of Nebraska. My own thinking and quick response to it is that not only are they two different jobs, but there could actually be a conflict there. And I don't know if there is. The idea occurs that a conflict could be there.

Do you have in mind that this executive committee only do classification matters?

Mr. SMITH. Oh, no, not at all, Senator. In fact, classification would be a small part of what we think it should do. It should have the responsibility of, first of all, ensuring that there is some systematic way that the threat is collected and analyzed and made available to those who need to know, including industry, by the way. We think that industry doesn't know enough about the threat that it faces. Second, the committee should be responsible for developing standards and procedures that are governmentwide. Everything from who gets a clearance to the physical security standards, to the standards for handling and processing of information. We also think it should have a oversight function to make sure that the standards and procedures that it develops are carried out. And finally we think it should have in some limited capacity this oversight or appellate function.

Senator KERREY of Nebraska. Did the President's decision and the Vice President's announcement on data encryption standard and clipper chip, did that cause this commission not to consider some recommendations in that area?

Mr. SMITH. No. As I said, we—because we knew that process was moving on a separate track and was pretty far along, we simply kept an eye on it. We didn't change any of our recommendations as a result of that decision.

Senator KERREY of Nebraska. Do you see this executive committee taking up that kind of an issue?

Mr. SMITH. Yes. I think it would be an appropriate place. I'm not sure it would be the final decisionmaker by any means, because there are certainly other equities, including the Department of Commerce and ultimately the President, I think, has to decide those issues. But this could be a forum where the equities of the defense and intelligence community could be formulated and certainly discussed. But those are very complicated issues, because the balances that have to be drawn involve a lot of different parts of the Government. So this would not be able to do anything quite that broad, in my view.

Senator KERREY of Nebraska. Well, I have supported publicly the administration's position. However, I do not think that this is the final chapter by any stretch. I think that the burden of proof must be on those who are asking for a policy to be changed, to persuade us to change. But I am persuaded to listen, because it does seem to me that there is potential there in both cases for the policy to become counterproductive. That is to say, to make it more difficult, particularly with open sources where we are trying to develop, could become more difficult for us to develop that open source if the policy restricts the development of the open sourcing networks.

What kind of considerations, when you looked at that advisory board, did you give? I must declare, I guess, my own prejudice against advisory boards. Did you think about different sectors—consumer interests, the corporate interests—what kind of consideration did you give to—what kind of advice does this executive committee need?

Mr. SMITH. The purpose of the advisory board, Senator, was that there is a lot of suspicion in various parts of this country that the classification system and that the security system is behind the curtain, behind closed doors, there is no public way, there is no representative of public interests in the security system. And it occurred to us that there needs to be some way that the public can have a voice in security decisions. Everything from classified information through standards for granting security clearances and so on.

I mean, just to give you an example, one of the concerns that I certainly had was in some cases in industry, for example, an employee could be working in a factory and be considered for a job that requires a very high degree of security clearance. At the moment they can be considered and investigated without their knowledge. If they don't get the security clearance because something shows up in their record, and they don't then move into this job, which may be a promotion, which may be career enhancing, they have been harmed and they don't know why. Nobody really worries about those kinds of things from the point of view of the employee. So the notion was that this advisory board could think about those kind of issues and could be a representative, in a sense, of that fellow on the factory floor that didn't get the clearance, that didn't even know he didn't get it. And if that gives you some sense of what we were trying to get at.

Senator KERREY of Nebraska. Do you, in the longer report, identify by categories the different areas of advice that an executive committee like this might need?

Mr. SMITH. We did talk—we have some in that, Senator. We did not go into enormous detail. I will tell you in all candor, in an earlier draft we did, but we took it out because we thought it was too much detail and we ought to leave it up to the Secretary of Defense and the DCI and the President and the Secretary of State and others, to see how they wanted to structure it, because we wanted to give them some flexibility.

Senator KERREY of Nebraska. I think it would be useful, though I appreciate leaving the detail out for a number of reasons, not the least of which is I have got enough to read as it is, but I think it would be useful for the purpose getting this Oversight Committee to understand what issues are at stake and why an advisory board like this might be necessary. I think that advisory board could play a very, very important role in promoting the public debate that very often is missing. And particularly when you are dealing with the Nation's security, I will tell you, if I have doubt, I give the benefit of the doubt to the Nation's security. And there are going to be many, many areas where there is doubt. And it is I think worthwhile as a consequence to give some sort of public airing out there, and I can in my own mind see several categories. And it would be helpful to me at least, and I think others members as well, to get some additional detail of what your thinking was.

Mr. SMITH. Senator, why don't we do a little memo to you that lays out some of our thinking and we will expand on this a little bit. Because we have given this some thought, and I think it is important. It is innovative, and I will be happy to do that.

Senator KERREY of Nebraska. I mean, there is no question that this has to change. I mean, that looks like Senator Dole's representation of the President's health care package, which I'm sure it is not. But it is no question that that—and I understand some of the acronyms in there, not all, and each one of them has a very serious mission. There is no question that that divided chain of command like that overwhelms the security policy questions, and when you are overwhelmed, you don't make decisions.

Mr. SMITH. That's exactly right.

Senator KERREY of Nebraska. Well, I'm now going to close the hearing. I do ask and will submit a very moving and eloquent opening statement that I wrote and did not give earlier.

[The opening statement of Senator Kerrey follows:]

J. ROBERT KERREY
NEBRASKA

United States Senate
WASHINGTON, DC 20510-2704

SENATE SELECT COMMITTEE ON INTELLIGENCE
OPEN HEARING ON CLASSIFICATION

MARCH 3, 1994

OPENING STATEMENT OF SENATOR BOB KERREY

Mr. Chairman, I appreciate the fact that you and Senator Warner have set this as an open hearing because how we keep our secrets is so important to our national security.

I don't think anyone would argue that some facts known to the government should be secret, just as businesses closely guard proprietary information about their products. During the Cold War we suffered the effects of an enemy who could and did steal some of our vital secrets, and we responded by classifying too much information, by classifying information at too high a level, by excessively guarding that information, and by leaving it permanently classified. Over the years we added layers and programs to create a baroque classification structure that requires years of training to navigate, and which adds enormous costs to the Defense and Intelligence Budgets. We won the Cold War, so I'm not complaining. But now that the threats are less fearsome we have an opportunity to do for this classification system the same thing that Secretary Aspin did for the Defense budget: a bottom-up review. Jeff Smith and the Joint Security Commission have done that review, and I am glad the Committee has provided this opportunity to hear their recommendations.

I have several concerns. First, I want a security system that works. If we lose vital information, as we reportedly have done in the Ames case, then the system is broken. All the safes and cipher locks and tempested computers in the world do not substitute for the loyalty of the individuals we trust. I want to hear the Commission's views on how we hire and retain loyal, dependable people.

Second, I am concerned about the unnecessary cost that the present security system adds to defense contracts and to the end price of goods and services that the taxpayers ultimately pay for. I realize that these costs are hard to capture, but I'll bet that when the Defense Department paid $400 for that hammer some years ago, $100 went for the security costs at the hammer factory.

Third, I am concerned about unnecessary security practices that keep the American people from the benefit that they would get from information or a process that they

-more-

paid for with their taxes, but which they are not permitted to know about. There is a trend toward openness in the Intelligence Community, and it is a trend which will in time bring some of the Community's classified technologies into the world of commerce, to the benefit of the public. We need to help this trend by simplifying the classification process and by declassifying what we safely can. Not only will we spread the benefit of forty years of classified work, but we will protect the remaining true national security secrets with greater vigilance.

-30-

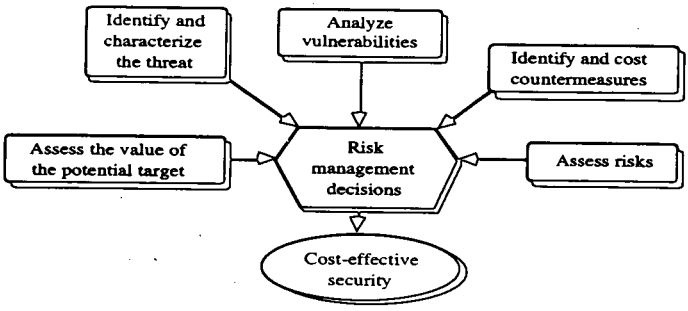
For more information please call Beth Gonzales or Greg Weiner at 202-224-6551. Thank you.

Senator KERREY of Nebraska. And again I appreciate, Mr. Smith, the work that you did and the rest of the Commission members did, the staff in supporting your effort, and most particularly, Dr. Perry and Mr. Woolsey for asking for this, and most importantly of all actually, the President for allowing it to occur. Because I do think that we now we have the hard work of following through and trying to implement and hopefully improving upon the recommendations.

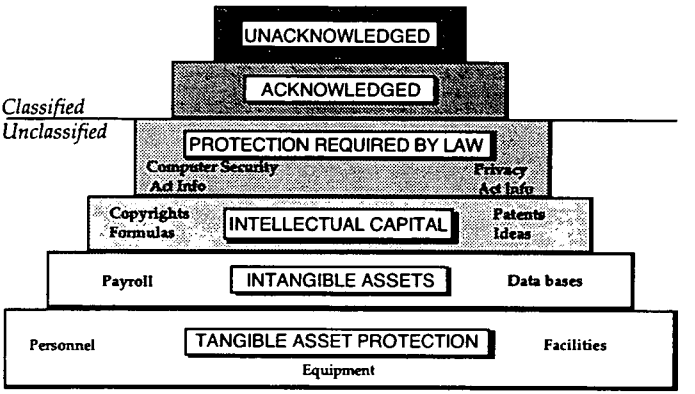
Mr. SMITH. Thank you.

Senator KERREY of Nebraska. Thank you.

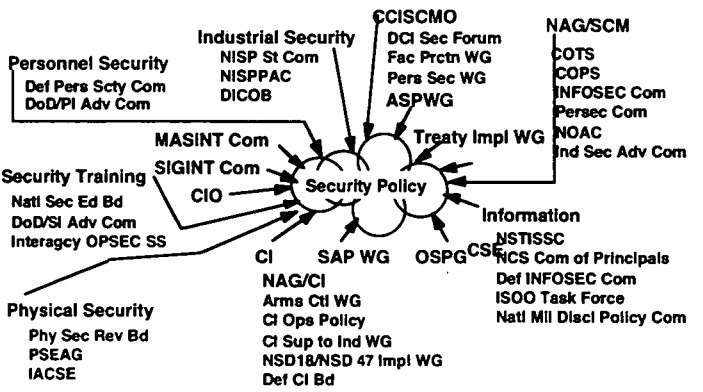
[Thereupon, at 4:13 p.m., the committee was recessed, subject to the call of the Chair.]



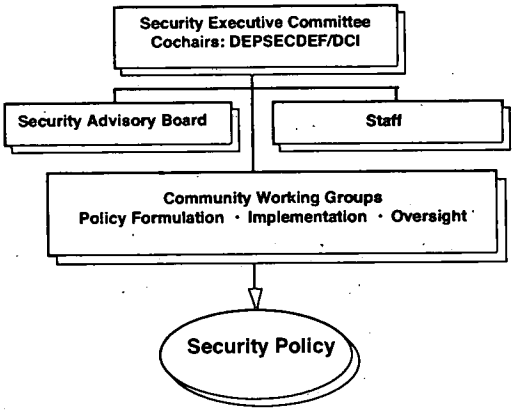
The Risk Management Process



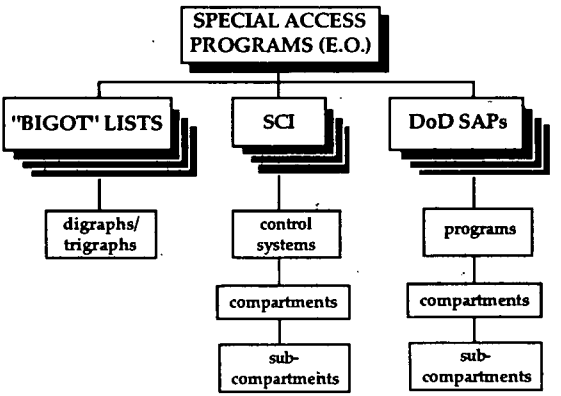
Protection by Program Type



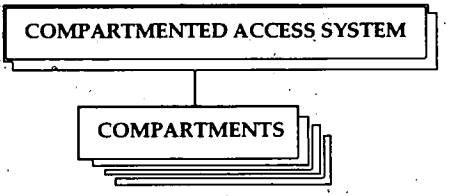
The Current Policy Structure



The Security Executive Committee



Current Special Access Program Structure



Proposed Special Access Program Structure

85-567 0 - 95 (48)

ISBN 0-16-046656-3