98TH CONGRESS
2d Session

SENATE

REPORT
98-665

REPORT

OF THE

SELECT COMMITTEE ON INTELLIGENCE
UNITED STATES SENATE

JANUARY 1, 1983, TO DECEMBER 31, 1984

OCTOBER 10 (legislative day, SEPTEMBER 24), 1984.—Ordered to be printed

---

U.S. GOVERNMENT PRINTING OFFICE

51-010 O

WASHINGTON : 1985

SENATE SELECT COMMITTEE ON INTELLIGENCE

BARRY GOLDWATER, Arizona, *Chairman*
DANIEL P. MOYNIHAN, New York, *Vice Chairman*

JAKE GARN, Utah
JOHN H. CHAFEE, Rhode Island
RICHARD G. LUGAR, Indiana
MALCOLM WALLOP, Wyoming
DAVID DURENBERGER, Minnesota
WILLIAM V. ROTH, JR., Delaware
WILLIAM S. COHEN, Maine

WALTER D. HUDDLESTON, Kentucky
JOSEPH R. BIDEN, JR., Delaware
DANIEL K. INOUYE, Hawaii
PATRICK J. LEAHY, Vermont
LLOYD BENTSEN, Texas
SAM NUNN, Georgia

HOWARD H. BAKER, JR., Tennessee, *Ex Officio*
ROBERT C. BYRD, West Virginia, *Ex Officio*

ROBERT R. SIMMONS, *Staff Director*
PETER M. SULLIVAN, *Minority Staff Director*
DORTHEA ROBERSON, *Clerk*
GARY M. CHASE, *Chief Counsel*

PREFACE

The Senate Select Committee on Intelligence hereby submits to the Senate a report of its activities from January 1, 1983 to December 31, 1984. Under the provisions of Senate Resolution 400, the Committee has been charged with the responsibility to carry out oversight of the programs and activities of the Intelligence Community of the United States. Most of the work the Committee is, of necessity, conducted in secret. Nevertheless, the Committee believes that intelligence activities should be as publicly accountable as possible. It is in this spirit that we submit this public report to the Senate.

This will be the last report issued by the Committee with the two of us serving together as Chairman and Vice Chairman, respectively. As part of the reorganization of the Senate in the 99th Congress, a new Chairman and Vice Chairman will be selected to serve for the coming two years. Accordingly, we take this opportunity to thank all Senators who have served with us on the Committee and helped us as we pursued its important oversight activities over the past four years. In particular, we would like to thank Senator Inouye, who will be leaving the Committee after eight years of distinguished service, and who served as the first Chairman in 1976 and 1977. We also thank Senator Huddleston, a Charter Member of the Committee, who will be leaving the Senate at the end of this Congress.

Finally, we would like to thank those members of the staff who worked for us and assisted us in the performance of the Committee's business over the past four years. In particular, we note the contributions of Rob Simmons, who served as Staff Director; Peter Sullivan, who served as Minority Staff Director or as Minority Counsel; and Dorthea Roberson, who served as Chief Clerk during most of this time.

Congressional oversight of the American Intelligence Family is a vitally important function of our Government. To our colleagues who will lead and serve the Committee in the next Congress, we wish all the best.

BARRY GOLDWATER,
Chairman.

DANIEL PATRICK MOYNIHAN,
Vice Chairman.

CONTENTS

	Page
Preface	III
I. Introduction	1
II. Central America	3
Collection and Analysis	3
Covert Action	4
History of Nicaraguan Program	4
Other Oversight Activities Concerning the Nicaraguan Program	12
Covert Action Reporting Procedures	13
Political Violence in El Salvador	15
Background	15
Conduct of Investigation	16
Committee Report	17
III. Legislation: Freedom of Information Act	18
Counterintelligence and Official Representation	22
Polygraphs	24
National Historical Intelligence Museum	27
Legislation Regarding DCI and DDCI Positions	28
IV. Intelligence and Security Activities	29
Analysis and Production	29
Counterintelligence	29
General Collection	30
Human Intelligence Collection	31
Communications Security Program	33
V. General Oversight	35
Foreign Intelligence Surveillance Act	35
Unauthorized Disclosure and Espionage Cases	37
Terrorism	39
Chemical and Biological Weapons	41
Korean Airline Incident	41
Grenada	42
Arms Control	42
Arms Control Violations	43
ASAT Arms Control	43
Soviet Space Program	44
VI. Budget Authorization	44
The Budget Authorization Process	45
Classified Budget Authorization Report	46
Statutory Authorization	46
Other Activities	47
Jurisdiction Relating to Intelligence Authorization	47
Legislation Enacted in Authorization Acts	47
VII. Administrative Issues	51
Committee Membership and the Eight Year Rule	51
Committee Facilities and Staff	51
Committee Reporter	51
New Committee Staff Office and Hearing Room	51
Map Library	52
VIII. Appendix	52
I. National Security Council Decision Directive 145	52
II. Summary of Committee Activities and Publications	60

98TH CONGRESS
2d Session

SENATE

REPORT
98-665

REPORT TO SENATE ON SELECT COMMITTEE ON INTELLIGENCE

OCTOBER 10 (legislative day, SEPTEMBER 24), 1984.—Ordered to be printed

Mr. GOLDWATER, from the Committee on Intelligence, submitted the following

REPORT

I. INTRODUCTION

On May 19, 1976, the United States Senate voted 72 to 22 in support of Senate Resolution 400, which established a Senate Select Committee on Intelligence (SSCI). Among other things, Section 1 of that Resolution stated that it would be the purpose of this Committee to "report to the Senate concerning . . . intelligence activities and programs" of the United States Government. In accordance with this provision, it has been the custom of the Committee to prepare a report at the conclusion of each Congress which summarizes in an unclassified fashion the oversight activities of the Committee during that Congress. The 98th Congress, having adjourned sine die, this report on our activities from January 1, 1983 to December 31, 1984, is submitted herewith.

The 98th Congress has been an unusually busy one for the Select Committee in Intelligence. During this period, the Committee held 127 meetings, hearings and briefings on the record, which compares favorably with 133 in the 97th Congress and 99 in the 96th. As well, it reported 12 bills or resolutions, and the Committee issued 10 reports.

Not only has the Committee maintained a high level of the oversight activities with which it has been charged, but also it has weathered the stresses and strains which have come in the course of fulfilling its oversight responsibilities, particularly with regard to the conduct of covert action activities. The Committee has been charged under the provisions of Senate Resolution 400 "to provide vigilant legislative oversight of the intelligence activities of the United States to assure that such activities are in conformity with the constitution and the laws of the United States." The word "vigilant" is stressed. Many intelligence activities of the United

51-010 O

States Government are, of necessity, conducted in secret. This adds a special and complicating dimension to the duties of this Committee. It makes the job far more difficult than is the case for other oversight Committees of the Congress.

Over the past two years, there may have been moments when some might have thought the Committee could have been more vigilant in ferreting out the facts regarding some of our government's intelligence activities. However, it is in the nature of our Nation's highly secretive intelligence work that an Oversight Committee must rely heavily on the Intelligence Community to be forthcoming in telling the Committee the things it must know to carry out its responsibilities. There have been situations when elements of the of the Intelligence Community did not live up to their legal obligation to keep our Committee "fully and currently informed" about intelligence programs and activities. This experience has led to a reappraisal of and improvement in the oversight compliance practices of the Executive Branch and of the Committee's own oversight procedures.

When the Select Committee on Intelligence was established in the Spring of 1976, our first Chairman, Senator Daniel K. Inouye, articulated what he felt to be the role of this Committee. Among other things, he said the following:

> We have learned that there must be active, continuous legislative oversight of intelligence activities, if we are to protect individual freedoms. Wise and honorable men tried, in the past, to regulate the Intelligence Community. But, for too long, they received little support and, as the Intelligence Community grew, excesses and the abuse of trust occurred. The Agencies, having no counterweight, bowed to Executive pressures and the excesses were magnified. So, we have learned that there must be a viable structure for legislative oversight, a focal point of responsibility and authority, if there is to be a legislative guardian of liberty. And, that is this Committee.

The Committee and Vice Chairman concur with this statement and have attempted over the past four years to achieve this worthwhile goal—namely, that this Committee be the "legislative guardian of liberty." They have attempted to do this in a bipartisan fashion. Partisan political concerns and activities are incompatible with the effective oversight of the Nation's intelligence activities.

Section 1 of Senate Resolution 400 also charges the Committee with making "every effort to assure" that the Intelligence Community provides "informed and timely intelligence for the Executive and Legislative Branches to make sound decisions affecting the security and vital interests of the Nation." Soon after its establishment in the Spring of 1976, the Committee set about the task of rebuilding our national intelligence resources had been severly depleted. Then Deputy Director of Central Intelligence, Admiral Bobby Inman, spoke of the problem on April 27, 1982, when he stated that:

> The intelligence establishment was cut back sharply in the 1960's and 1970's after a major buildup in the 1950's,

losing 40 percent of its personnel from 1964 to the mid-1970's.

It was evident that this trend had to be reversed. Intelligence budgets began to rise in the late 1970's and this trend line increased sharply in the 98th Congress. Indeed, the Intelligence Authorization Act for Fiscal Year 1985, enacted in November of this year, authorized the largest budget in the history of the Committee and of the Intelligence Community. The Committee believes that this increased funding has helped to rebuild and revitalize our Nation's intelligence capabilities, and is the product of strong bipartisan support for intelligence in both the Executive and Legislative Branches.

In summary, the period of the 98th Congress has been an eventful one for the Select Committee on Intelligence and for Congressional oversight of the American Intelligence Community. It is hoped that the following report of the Committee's activities will also show that this period was a productive one for this important Congressional activity.

II. Central America

During the 98th Congress, the Committee continued its oversight of intelligence activities in Central America. Matters affecting this region claimed a major share of the Committee's time. The intensity of interest was also reflected in the number of Members who visited the region (Senators Leahy, Cohen, Moynihan, Huddleston, Chafee, and Roth) and the service of Senators Inouye and Bentsen, as well as the late Senator Jackson, as Senior Counsellors to the National Bipartisan Commission on Central America.

COLLECTION AND ANALYSIS

Over the past years, the stability of the region has been increasingly threatened by the Cuban-Soviet supported military build-up in Nicaragua and the Sandinista regime's assistance to insurgencies seeking the overthrow of the governments of El Salvador and other neighboring countries. The problem has been compounded by anti-democratic elements in El Salvador and other countries which engage in political violence to achieve their objectives.

These developments have underscored the need for effective intelligence collection and analysis to support the efforts of our government to formulate and implement economic and security assistance programs and a variety of other foreign and defense policies.

In May 1983, the Committee conducted hearings as part of a comprehensive review of U.S. Intelligence efforts in Central America. The review enhanced the Committee's appreciation of the relative strengths and weaknesses of collection and analytical programs and was helpful in identifying areas requiring attention in the budget process.

The Committee has continued to follow closely intelligence reporting and performance on Central American political and military situations. In addition to reviewing current intelligence reports and analyses, the Committee and its staff have received numerous briefings on various topics, including arms supplies to Nica-

ragua and the impact of its increased military capabilities on the regional military balance; the insurgencies in Nicaragua and El Salvador; and, as discussed more fully elsewhere in the report, political violence in El Salvador.

The information obtained in the course of the Committee's oversight is part of the basis of judgments which Members make on legislative issues such as the nature and extent of assistance the U.S. should give to El Salvador and Honduras and to anti-Sandinista activities in Nicaragua.

COVERT ACTION

The most important part of the Committee's oversight concerned covert action affecting Nicaragua. At least a quarter of the Committee's time was devoted to this subject. The program in Nicaragua gave rise to serious and difficult issues for the Committee. As discussed further below, the mining of Nicaragua's harbors in 1984 and the failure of the Director of Central Intelligence (DCI) to adequately notify the Committee of it in advance,[1] precipitated a crisis in the Committee's relations with the Intelligence Community. With the approval of the President, the DCI entered into an agreement with the Committee on June 6, 1984, which provides procedures designed to ensure that the Committee receives prior notice and adequate information concerning covert action operations, including those in furtherance of ongoing covert action programs.[2]

In October, 1984, the Congress voted to suspend funding of the Nicaraguan program until February 28, 1985, and to resume it thereafter only upon enactment of a joint resolution. Inadequate supervision and management of this program in 1983–1984 certainly contributed to this outcome. Subsequent to adjournment, the Committee learned of CIA's production of the Psychological Warfare Manual which offered questionable advice to Nicaraguan insurgents on how to achieve their goals. These factors will surely affect Congressional consideration of any request by the President to resume the Nicaraguan program.

HISTORY OF NICARAGUAN PROGRAM

Most covert actions do not become subjects of public debate, much less the subject of public legislation, while they are being conducted. For a number of reasons, including publicity generated by the Nicaraguan insurgents often referred to as "Contras," the Nicaraguan paramilitary program is an exception. In December, 1982, some Members of the House of Representatives became concerned about public reports regarding the objectives of reported CIA support of the Contras, some of whom declared their intention to overthrow the Sandinista regime. During Floor deliberations on the Continuing Resolution providing Appropriations for Fiscal

---

[1] Senator Garn did not concur with the Committee's judgment that the DCI had failed to notify the Committee.

[2] The Intelligence Oversight Act of 1980 requires the DCI to give the Intelligence Oversight Committees prior notice of "any significant anticipated intelligence activity." This requirement and the new Covert Action Reporting Procedures are discussed in more detail in the following section of the Report.

Year 1983, these House Members sought to amend that measure to prohibit support of such objectives.

The Chairman of the House Intelligence Committee, Congressman Boland, assuaged these concerns by noting that the House and Senate Intelligence Committees had previously treated this issue in the classified report language associated with the Intelligence Authorization Act for Fiscal Year 1983 (P.L. 97-269, September 27, 1982). Drawing on the classified statement of managers supplementing the Conference Report on that Act, Congressman Boland offered the following amendment to the Continuing Appropriations Resolution which the House adopted:

> None of the funds provided in this Act may be used by the Central Intelligence Agency or the Department of Defense to furnish military equipment, military training or advice, or other support for military activities, to any group or individual, not part of a country's armed forces, for the purpose of overthrowing the Government of Nicaragua or provoking a military exchange between Nicaragua and Honduras.

Congressman Boland noted that although the Administration did not like the amendment, it would accept it.

Later a similar debate occurred in the Senate. Members of the Select Committee offered an amendment substantially the same as Congressman Boland's as a substitute for a more restrictive proposal. While the underlying amendment was tabled and the Committee's amendment set aside, the Committee nevertheless expected the Senate to accept the Boland Amendment in Conference. It did so and this amendment became law. (Section 793 of the Department of Defense portion of P.L. 97-337, December 21, 1982, making Further Continuing Appropriations for Fiscal Year 1983). In late December, 1982, the Vice Chairman of the Committee, Senator Moynihan, wrote to the DCI advising him of the Committee's support of the Boland Amendment and that it expected the CIA to conform its activities to both the letter and spirit of the law.

This was the point of departure for the Committee's oversight of the Nicaraguan program in the 98th Congress.

In January, 1983, Senator Leahy, accompanied by staff of the Committee, visited Central America to review U.S. intelligence activities related to Nicaragua. His findings, supplemented by follow-up Committee briefings and inquiries, revealed two important facts: 1) the Nicaragua program was growing beyond that which the Committee had initially understood to be its parameters; and 2) there was uncertainty in the Executive Branch about U.S. objectives in Nicaragua, particurlarly in view of the goals avowed by some of the forces receiving U.S. support. In addition to raising questions about compliance with the Boland Amendment, there seemed to be a lack of coordination between the covert program and U.S. diplomatic initiatives, with the program appearing at times to be preceeding policy, rather than following it.

In May, 1983, the Committee advised the Executive Branch that its program was not sufficently specific with respect to what was being undertaken, the grounds for doing so, and the objectives sought. The Committee then took the rather unusual step of re-

quiring that, before it approved any more funding, the Administration articulate in a clear and coherent fashion its policy objectives in a new Presidential Finding, the process by which covert action operations are required by law (the Hughes-Ryan Amendment, Section 662 of the Foreign Assistance Act of 1961) to be authorized. In this connection, it should be noted that, while the Committee may recommend whether or not to fund a particular covert action program and the Congress, pursuant to its power over appropriations, may prohibit such expenditures, the initiation of a program is within the powers of the President. The Committee is entitled by law to be informed of the President's Finding authorizing such an action in advance of its implementation and to offer its counsel, but does not have the right to approve or disapprove implementation of the Finding.

On August 3, 1983, the DCI appeared before the Committee with the outlines of a proposed new Finding. The DCI seemed receptive to concerns which were raised that the proposal was too broad and ambitious. The draft was revised and then signed as a Presidential Finding. On September 20, the new Finding was presented to the Committee by the DCI and Secretary of State Shultz. In large measure, the new Finding and its elaboration in the briefing was responsive to the concerns the Committee had previously raised.

The following day a news story in the New York Times quoted an Administration official with respect to the new Finding and the previous day's briefing:

> We were always being questioned . . . on whether we were going beyond our program of interdicting arms. Now we say: Yes, we are supporting the rebels until the Nicaraguans stop their subversion in neighboring countries.

That article went on to say:

> The Administration official stressed that this approach should end the argument over whether the Administration was violating its pledge by doing more than just stopping the arms flow. The official also said that there was no thought of the Administration backing the insurgents in trying to overthrow the Sandinista government.

Subsequently, the Committee, by a nearly unanimous vote, approved funds for the redefined program in the Intelligence Authorization Act for Fiscal Year 1984. On November 3, 1983, the Senate passed this bill on a voice vote. A conference with the House of Representatives, which had voted to terminate the Nicaragua program, recommended a compromise which imposed a $24 million ceiling on funds available for this activity. The conferees also agreed to include in their report a statement of Congressional findings drawn from the House bill, but which also reflected the view of the Senate. This provision stated, among other things, that:

> by providing military support (including arms, training, and logistical, command and control, and communications facilities) to groups seeking to overthrow the Government of El Salvador and other Cental American governments, the Government of National Reconstruction of Nicaragua has violated article 18 of the Charter of the Organization

> of American States which declares that no state has the right to intervene, directly or indirectly, for any reasons whatsoever, in the internal or external affairs of any other state.

The conference report was accepted by the House and Senate and the Authorization Act was signed into law on December 9, 1983, (P.L. 98–215). The same $24 million ceiling was included in the Department of Defense Appropriations Act for Fiscal Year 1984 (P.L. 98–212).

As the first session of the 98th Congress came to a close, the Committee believed that the close consultative relationship between it and the Executive Branch—a relationship contemplated by the intelligency oversight legislation enacted in 1980—contributed significantly to the forging of a strong majority on the Committee supporting the new Finding on Nicaragua. However, without notifying the Committee, as required by the Oversight Act, major changes were made in the conduct of this program, including the mining of Nicaragua's harbors. The Committee was not informed of these actions until after they were substantially accomplished. Only upon subsequent inquiries by the Committee was the nature of U.S. involvement ascertained.

The intelligence oversight process was further undermined in March 1984 when the Administration attempted to obtain the approval of the Senate Appropriations Committee for $21 million in supplemental funding for the covert assistance program in Nicaragua before the Select Committee had an opportunity to consider this request. Secretary of State Shultz apologized to the Committee for this irregular procedure. The first effort to secure Appropriations committee approval failed, allowing the Select Committee time to consider the $21 million request. The Select Committee recommended approval of supplemental funding of $21 million, of which $14 million would be placed in the CIA's contingency reserve, with its release conditioned to compliance with the notification provisions of the Intelligence Oversight Act. Such a provision was included in the urgent supplemental appropriations bill recommended by the Senate Approporiations Committee and later passed by the Senate on April 5, 1984. However, the Senate receded from this position on July 26, following a deadlocked conference with the House.

On April 10, 1984, in a closed session, with most of the Members of the Senate in attendance, the DCI made his first formal presentation to the Committee of the details of the mining operations and the decision-making process which led to it. Following this briefing, the Senate, by a vote of 84–12, passed a sense of the Congress resolution that:

> No funds heretofore or hereafter appropriated in any Act of Congress shall be obligated or expended for the purpose of planning, directing, or supporting the mining of the ports or territorial waters of Nicaragua.

On the same day, the Chairman of the Committee, Senator Goldwater, issued a statement which stated, among other things:

> . . . [The] Intelligence Community did not fully inform . . . [the] Committee concerning mining of harbors in Nicaragua despite the fact that they had a legal obligation to do so.
>
> [The] Intelligence Authorization Act [for Fiscal Year 1981] amended the Foreign Assistance Act of 1961 to require that each operation conducted by or on behalf of the Central Intelligence Agency in a foreign country, other than activities intended solely for obtaining necessary intelligence, shall be considered a significant anticipated intelligence activity for the purpose of Section 501 of the National Security Act of 1947 [popularly referred to as the Intelligence Oversight Act of 1980].
>
> Because the legal requirement of the law was not followed in this case by not briefing our Committee, I, therefore, wrote a strong letter to Director Casey expressing my extreme displeasure. In the letter, I explained to Director Casey that we in Congress had been debating for almost two weeks whether we would increase funds for the Nicaraguan program. Since neither the Committee nor my staff were briefed on the substance of the program, I had to engage in repeated debate on the Senate Floor. Having discovered the truth of the matter, I was then placed in the position of having to apologize to Members of the Committee and the Senate.
>
> I told Mr. Casey that this is no way to run a railroad and that it is indefensible on the part of the Administration to ask us to back its foreign policy when we don't even know what is going on because we were not briefed pursuant to the legal requirements. The Committee and Congress were left holding the bag in this instance. And, if we are to support the foreign policies of this Administration then, the President and his spokesman should let Congress and the American people know what is going on.
>
> In effect, what I told Director Casey was that if plain old fashion common sense had been used, the type of problem we face today would have never happened.

The Chairman's statement concluded by saying that:

> The issues being raised now by me will have to be resolved to the satisfaction of my Committee and the Congress. Until that is done, I would hope and suggest that the debate on this issue be put on hold.

Public debate, however, continued. On April 12, 1984, DCI Casey issued an "Employee Bulletin" in which he asserted that the CIA had "fully met all statutory requirements for notifying our Intelligence Oversight Committees of the covert action program in Nicaragua . . . [and] complied with the letter of the law in our briefings . . . [and] with the spirit as well." On the same day, according to a press report, the President's National Security Advisor, Robert McFarlane, told the Naval Academy Foreign Affairs Conference, that:

> Every important detail [of the mining] was shared in full by the proper Congressional Oversight Committees.

The report said Mr. McFarlane went on to say that "disclosure of secret plans to specified Congressional Committees 'as . . . provided by law,' was 'faithfully' accomplished."

On April 15, 1984, Senator Moynihan announced his intent to resign as Vice Chairman of the Committee, stating:

> This appears to me the most emphatic way I can express my view that the Senate Committee was not properly briefed on the mining of Nicaraguan harbors with American mines from an American ship under American command.
>
> An employee bulletin of the Central Intelligence Agency issued April 12 states that the House Committee was first briefed on 31 January, but the Senate Committee not until March 8. Even then, as Senator Goldwater has stated, nothing occurred which could be called a briefing. The reference is to a single sentence in a two-hour Committee meeting, and a singularly obscure sentence at that.
>
> This sentence was substantially repeated in a meeting on March 13. In no event was the briefing "full," "current," or "prior" as required by the Intelligence Oversight Act of 1980—a measure I helped write. If this action was important enough for the President to have approved it . . . it was important enough for the Committee to have been informed . . . [before implementation].
>
> In the public hearing on the confirmation of John J. McMahon as Deputy Director of Central Intelligence, I remarked that with respect to intelligence matters the "oversight function necessarily involves a trust relationship between the Committee and the Community because we cannot know what we are not told and therefore must trust the leaders of the Community to inform us."
>
> I had thought this relationship of trust was securely in place. Certainly the career service gave every such indication. Even so, something went wrong, and the seriousness of this must be expressed.

On April 26, the Committee held a closed meeting with DCI Casey at which he "apologize[d] profoundly." Following the meeting, the Committee issued the following statement:

> The Senate Select Committee on Intelligence met on April 26 to review the events that led to the mining of Nicaraguan harbors and attacks on Nicaraguan ports. At the conclusion of this review, the Committee agreed that it was not adequately informed in a timely manner of certain significant intelligence activity in such a manner as to permit the Committee to carry out its oversight function. The Director of Central Intelligence concurred in that assessment.
>
> The Committee and the CIA have agreed on the need for more thorough and effective oversight procedures, especially in the area of covert action. The Committee will move

promptly to develop new procedures to ensure that the Senate will be fully and currently informed. The Central Intelligence Agency has pledged its full cooperation in this effort and recognizes the requirement to provide the Committee with prior notice of "any significant anticipated intelligence activity," as provided by the Intelligence Oversight Act.

At the request of the Committee, and in light of the Director's acknowledgement, Senator Moynihan withdrew his resignation as Vice Chairman.

The Committee, with the full cooperation of the CIA, immediately set upon the task of developing improved oversight procedures for covert action. On June 6, DCI Casey, with the approval of the President, signed a written agreement with the Committee setting forth procedures for compliance with the statutory requirements of the Intelligence Oversight Act for reporting covert action activities to the Intelligence Committees.

In May, the Committee deliberated on the Administration's request for funding the Nicaragua program in Fiscal Year 1985. The Committee held a closed session with DCI Casey and Secretary of State Shultz to re-examine the objectives and prospects of this activity in the aftermath of the mining episode. On May 24, the Committee reported the Intelligence Authorization Act for Fiscal Year 1985, which included the funds requested, but in the classified annex to its report stipulated termination conditions for the program. This reflected the view of a majority of the Members of the Committee that the predominant objective of the program had evolved from the need to see an end to Nicaragua's support of insurgencies in El Salvador and other neighboring countries, as had been previously understood, to the achievement of goals that were too much concerned with the internal structure of Nicaragua's government. This measure was reported with the understanding that the Nicaraguan program would be subject to continuing review by the Committee and that Members were free to offer amendments within the Committee or on the Floor. In this connection, the Committee met on June 13 to consider a proposed amendment to further clarify and restrict the scope of the program, but the amendment was rejected.

On June 18, during Floor consideration of the Department of Defense Authorization Act for Fiscal Year 1985, Senators Inouye and Moynihan offered a substitute to a pending amendment. Their substitute would have terminated a U.S. support of paramilitary operations in Nicaragua, while providing $6 million in funds for an orderly and humanitarian withdrawal and resettlement of the insurgents opposing the Sandinista government.

The substitute amendment failed when the underlying amendment was tabled on a vote of 58 to 38. Eight Committee Members voted for tabling the motion, while seven voted against. The division among Committee Members indicated that the consensus built in the Fall of 1983 had been fractured. This virtually assured that the policy would not survive a conference in with the House, where opposition was strong and growing.

Because of the expected impasse with the House on the Nicaragua issue, the Intelligence Authorization Act for Fiscal Year 1985 was not taken up by the Senate until the closing days of the session after the issue had been resolved in the Continuing Resolution for Fiscal Year 1985 Appropriations.

On October 3, Senator Inouye offered an amendment to the Continuing Resolution similar to the one he proposed on June 18. This amendment was also rejected by a vote of 42 yeas to 57 nays. The division among Committee Members was 6 yeas to 9 nays.

In conference with the House, which had prohibited any funds for the Nicaraguan program, the Senate conferees agreed to terminate funding for paramilitary activities in Nicaragua until February 28, 1985. The conferees further agreed to permit funding after that date only if—

(1) The President submits to Congress a report—

(A) stating that the Government of Nicaragua is providing material or monetary support to anti-government forces engaged in military or paramilitary operations in El Salvador or other Central American countries;

(B) analyzing the military significance of such support;

(C) stating that the President has determined that assistance for military or paramilitary operations prohibited by subsection (a) is necessary;

(D) justifying the amount and type of such assistance and describing its objectives; and

(E) explaining the goals of United States policy for the Central American region and how the proposed assistance would further such goals, including the achievement of peace and security in Central America through a comprehensive, verifiable and enforceable agreement based upon the Contadora Document of Objectives; and

(2) A joint resolution approving assistance for military or paramilitary operations in Nicaragua is enacted.

Procedures for expedited consideration of any such joint resolution in the House and Senate were also included.

The Conference Report was accepted by the Senate on October 11, 1984. The Continuing Resolution was signed into law the following day. (See Section 8066 of P.L. 98-473.)

After approval of the Conference Report on October 11, provisions concerning Nicaragua in that measure were, in effect, incorporated into the Intelligence Authorization Act for Fiscal Year 1985 which was passed by the Senate and then the House. This measure was signed into law on November 8 (P.L. 98-618).

The Committee considers the procedure followed in the resolution of the Nicaragua issue most unfortunate. Senate Resolution 400, which established the Select Committee on Intelligence, contemplated that appropriations for intelligence activities would be preceeded by enactment of authorizing legislation which is the responsibility of the Select Committee. The Intelligence Oversight Act of 1980 reduced the number of Committees required to receive notification of Presidential Findings on covert actions from eight to the two Intelligence Committees. The clear intent of these measures was that, to the maximum practicable extent, intelligence

funding issues, particularly in the covert action area, should be addressed first in authorizing legislation.

As a consequence of the procedure followed in 1984, Members of the Intelligence Committees, who were most familiar with the diverse intelligence activities concerning Nicaragua, were unable to meet in a conference to resolve differences between the House and the Senate. The Committee urges that every effort be made in the future to assure that intelligence authorizing legislation be advanced before appropriation bills.

OTHER OVERSIGHT ACTIVITIES CONCERNING THE NICARAGUA PROGRAM

During 1984, the Committee conducted inquiries concerning various aspects of the conduct of the Nicaragua program.

In June, the Committee met in closed session to discuss with CIA officials allegations reported in the press that the Agency had exceeded the $24 million spending ceiling imposed by the Intelligence Authorization Act for fiscal year 1984.

The Committee reviewed with the Agency details as to accounting procedures used for the Nicaragua program. These procedures were found to be consistent with those used by CIA for more than three decades. Further, the Committee established for the record that there has been no transfer of accounts or other technical accounting procedures employed by CIA to circumvent Congressional spending restrictions. Based on its review, the Committee reaffirmed its judgment that there have been no improprieties in accounting methods used by CIA relative to the $24 million statutory spending cap. Also, in response to the Committee's request, the CIA submitted a formal legal opinion as to the Agency's compliance with the statute.

On September 1, two Americans were killed in a helicopter crash in Nicaragua while accompanying the Contras on a military operation. On September 11, the Committee received a briefing from representatives of the CIA and the Departments of State and Defense concerning whether there has been any official U.S. Government involvement in this incident.

At the briefing, representatives of the CIA stated that the Agency had no involvement in the mission conducted in Honduras by the group of U.S. volunteers. They also disclaimed any CIA relationship with members of this group.

CIA officials also stated that they had no advance knowledge of the specific mission, although they were aware of a group of U.S. volunteers subsequently identified as the "Civilian Military Assistance." However, no CIA officers were in contact with any member of Civilian Military Assistance prior to the ill-fated event.

In October, following adjournment of the 98th Congress, the press revealed that CIA produced a Psychological Warfare Manual, under the pseudonym "TAYACAN," which offered advice to the Contras on how, among other things, to employ violence to achieve their political goals in Nicaragua. Some of the methods recommended appeared to be contrary to stated CIA policies, and certain passages could have been interpreted to call for assassination, which is prohibited by Executive Order 12333, signed by President Reagan in 1981. In addition, the manual incident raised questions

as to the adequacy of command and control over the Nicaragua program. On this basis, the Chairman wrote to Director Casey on October 17, 1984, asking for a "full briefing" on this matter.

The Committee held a closed session on October 22 to hear testimony from Agency officials concerning the production and distribution of the manual. Subsequently, the matter was the subject of an investigative report of the CIA's Inspector General and the President's Intelligence Oversight Board.

In November, the press reported allegations by a Contra leader that CIA officers arranged visits to Washington for Contra leaders to lobby Members of Congress and advised on whom they should see and what they should say. Such conduct would raise questions of legality and propriety. Therefore, on November 9, 1984, the Vice Chairman of the Committee wrote to DCI Casey asking for a written report. In his reply of December 7, 1984, the DCI stated that, on the basis of "an extensive review of Agency files" and talks with Agency personnel, there is "no record or recollection to support" those charges.

COVERT ACTION REPORTING PROCEDURES

The DCI's failure to give the Committee adequate prior notice of the mining of Nicaragua's harbors raised questions as to whether the Committee and the Executive branch shared a mutual understanding of the Intelligence Community's statutory obligations. The Committee concluded that there was a need for explicit, written procedures to ensure Executive branch compliance with the requirements for reporting covert action activities.

The current statutory obligations of the Intelligence Community with respect to Congressional oversight, popularly referred to as the Intelligence Oversight Act of 1980, were enacted as section 407 of the Intelligence Authorization Act for Fiscal Year 1981 (P.L. 96–450, 14 October 1980). They are set forth in section 662 of the Foreign Assistance Act of 1961 (22 U.S.C. 2422) and in Title V of the National Security Act of 1947 (50 U.S.C. 413).

The oversight legislation represents an agreement between the Executive and Legislative branches to replace a previous requirement for timely reporting of covert actions to as many as eight Congressional committees with a system that centralizes oversight in the Intelligence Committees under a new set of requirements.

This statutory system imposes upon the Director of Central Intelligence and the heads of all other Intelligence Community organizations the obligation, among other things, to:

> Keep the intelligence committees "*fully and currently informed*" of all intelligence activities, including "any significant *anticipated* intelligence activity" (emphasis added).

Section 662 of the Foreign Assistance Act, as amended in 1980, specifies that each covert action operation is to be considered a "significant anticipated intelligence activity." This means that covert action operations must be reported to the Intelligence Committees prior to implementation in accordance with Title V of the National Security Act.

The oversight legislation imposes two additional obligations upon the DCI and other heads of Intelligence Community organizations, as follows:

To furnish any information or material concerning intelligence activities which is requested by either of the intelligence committees in order to carry out its authorized responsibilities; and

To report to the committees in a timely fashion any illegal intelligence activity or significant intelligence failure.

All of the obligations contained in the oversight legislation are conditioned by preambular clauses, which specify that the obligations are to be undertaken:

To the extent consistent with all applicable authorities and duties, including those conferred by the Constitution upon the Legislative and Executive branches; and

To the extent consistent with due regard for the protection of classifed information and intelligence sources and methods from unauthorized disclosure.[3]

The issue that arose with respect to the Nicaraguan harbor mining incident concerned the meaning of the term "significant anticipated intelligence activity." Representatives of the DCI and Committee staff worked together to formulate a number of reporting criteria and procedural mechanisms to enhance the abilities of the DCI and the Senate Select Committee to fulfill their respective responsibilities under the law.

Thus, agreement was reached on the written material that will be provided to the Senate Select Committee when a Presidential Finding is signed, so as to ensure that the Committee will be fully informed regarding the nature of each program approved by the President. Agreement also was reached on the subjects that should be covered by Executive branch witnesses in briefing the Committee on such programs.

A key component of the agreement that ultimately was achieved concerned recognition by the Executive branch that, while each new covert action operation is by definition a "significant anticipated intelligence activity," this is not the exclusive definition of that term. Thus, activities planned to be undertaken as part of ongoing covert action programs should in and of themselves be considered "significant anticipated intelligence activities" requiring prior notification to the intelligence committees if they are inherently significant because of factors such as their political sensitivity, potential for adverse consequences, effect on the scope of an ongoing program, involvement of U.S. personnel, or approval within the Executive branch by the President or by higher authority than that required for routine program implementation. The Senate Select Committee agreed to communicate to the DCI, in connection with each ongoing covert action program, the kinds of activities (in addition to those that change the scope of an operation or require approval by higher authority) that it would consider to merit prior

---

[3] Neither the preambular language, nor the oversight legislation's specific provisions allowing for prior notice of significant anticipated intelligence activities only to eight specified Congressioanl leaders in extraordinary circumstances 9 with subsequnt timely notice of covert actions to the intelligence committees), figured in the controversy over the mining of Nicaraguan harbors.

notice. The DCI agreed to take steps independently to ensure that the Senate Select Committee is also advised of activities that the DCI believes reasonably fall in this category.

It also was agreed that the Committee will be provided with a comprehensive annual briefing on all ongoing covert action operations, as well as regular information on implementation of each ongoing operation. On September 11, 1984, the full Committee met in closed session for this comprehensive briefing. In addition, the DCI and the Senate Select Committee both reaffirmed their commitment to protect information on covert action operations from unauthorized disclosure, with special regard for the extreme sensitivity of these activities.

These agreements, along with a number of additional provisions, were incorporated into a new set of procedures which were signed on June 6, 1984, by Chairman Barry Goldwater and Vice Chairman Daniel Patrick Moynihan, and by DCI William J. Casey for the Administration. As it noted in its announcement of this event at the time, the Committee considers the achievement of the agreements set forth in these procedures to be "an important development which should reduce the chances for a repetition of the kind of problem and misunderstanding which was recently encountered in this area."

The Committee intends to take steps to ensure that the procedures fulfill their intended function. In accordance with provisions in the procedures themselves, the Committee has asked for and received information on how the DCI plans to manage Agency compliance with the procedures. In addition, the procedures provide for an assessment of their effectiveness and impact by the DCI and the SSCI jointly, not later than one year after their effective date.[4]

INVESTIGATION CONCERNING POLITICAL VIOLENCE IN EL SALVADOR

Background

In Spring 1984, increasing public attention focused on continuing political violence in El Salvador, particularly the activities of extreme rightwing "death squads." Of particular concern to Members of the Senate were allegations that officials of the military, intelligence and security services of El Salvador were participating in systematic acts of political violence, and even that elements of the United States government were connected to this violence or had actually supported or encouraged death squad activities.

On April 3, 1984, Senator Kennedy proposed an amendment to H.J. Res. 492, a pending urgent supplemental appropriations bill containing funds for military assistance to El Salvador, which would have called for an investigation of "death squads" in that country, including "the extent of death squad activity; responsibility for organizing, directing and carrying out death squad killings; and progress in prosecuting those responsible for such killings."

Senator Kennedy explained his central concern as,

---

[4] Experience subsequent to adoption of the procedures indicated, however, that further steps were necessary to ensure that delays not inadvertently result in failure to notify the Committee prior to implementation of significant activities. The Chairman and the Vice Chairman called this matter to the attention of the DCI, and he agreed to the establishment of specific time intervals for the notification process.

> . . . whether the CIA is involved in any way, directly or indirectly, in supporting individuals who are involved in any way, directly or indirectly, in death squad acitivities; or, whether any funds from the Central Intelligence Agency, or any agency of the Government, is in any way being used in this particular endeavor[; as well as] whether the CIA is in any way involved with individuals who are associated with death squads.

In response to the amendment introduced by Senator Kennedy, Chairman Goldwater of the Select Committee on Intelligence stated on the Floor of the Senate on April 3, 1984, that the Committee would do everything it could to investigate the matter. Senator Kennedy thereupon withdrew his amendment. Chairman Goldwater and Vice Chairman Moynihan of the Intelligence Committee subsequently initiated a Committee investigation. Accordingly, the Committee organized a working group composed of several professional staff members to conduct the investigation.

The investigation focused on the period following the military reformist coup of October 1979. The following key questions were identified:

> Has any U.S. Government agency or official engaged in activities that could be construed as support for, encouragement of, or complicity or acquiescence in political violence in El Salvador, particularly with respect to death squad acitivity?
>
> Has the quantity and quality of collection, analysis and production of intelligence information on political violence in El Salvador been commensurate with the importance of this issue to U.S. policy?

Conduct of the investigation

The staff working group was organized into separate teams responsible for investigating the programs and activities of the relevant U.S. government agencies and their personnel. These agencies included the Central Intelligence Agency; the Department of Defense, including the Defense Intelligence Agency, the U.S. Southern Command (SOUTHCOM), and the National Security Agency; the Department of State, including the Agency for International Development; and the Department of Justice, including the Federal Bureau of Investigation.

The Committee heard classified testimony from the CIA's Deputy Director for Operations on May 10, 1984, and conducted a closed hearing on June 20, 1984 with testimony from representatives of all concerned agencies. Voluminous questions for the record were submitted and responded to by to the agencies following up on their testimony during the June 20 hearing. Additional specific requests for information were also forwarded in writing.

The investigation relied primarily on review of materials that constitute a detailed record of day-to-day U.S. government activities and decision making. Working group members were given access to a broad range of documents, including relevant messages, reports and memoranda.

Working group members also interviewed numerous Executive branch officials and former officials associated with U.S. govern-

ment activities in El Salvador. Interviewees at the various agencies included senior policy makers, analysts and operational personnel who have served in the field. Committee staff visited San Salvador and interviewed various officials at the U.S. Embassy there, including the Ambassador. Staff also met with military officials at SOUTHCOM headquarters in Panama.

Because the Committee's investigation was conducted in response to concerns about rightwing political violence in El Salvador, particularly death squad activities, the Committee's report concentrated on this phenomenon. The report also recognized, however, the systematic political violence of the armed left. The Committee made clear that by issuing a public report largely on extreme rightwing political violence in El Salvador, it did not mean to imply that rightwing political violence constituted a greater moral or political issue than similar activities by the extreme left.

Committee report

On the basis of its investigation, on October 5, 1984, the Committee issued a public report (Senate Report 98-659) containing a summary of its conclusions and a statement of its key findings based on the classified reports. The summary read as follows:

> The Committee found ample evidence that the policy of the United States throughout the period under review was consistently to oppose political violence in El Salvador, including violence by extreme rightwing death squads. The degree to which Executive branch agencies acted directly with Salvadoran authorities to combat political violence generally reflected their judgments about what was achievable in the Salvadoran political context.
>
> The Committee found that, in the course of carrying out their missions implementing overall U.S. policy to assist the Government of El Salvador in resisting the leftist insurgency, elements of the U.S. government have unavoidably had contact with Salvadoran organizations and individuals strongly suspected of being involved in or associated with political violence. The Committee believes that, for the most part, the problems that have arisen in this regard are of the type which may occur whenever the U.S. government seeks to obtain intelligence on the activities of clandestine organizations such as international terrorist groups or narcotics rings, or to assist foreign governments engaged in violent confrontations with insurgent forces.
>
> The Committee found no evidence to support the allegation that elements of the U.S. government have deliberately supported, encouraged or acquiesced in acts of political violence in El Salvador, including extreme rightwing death squad activity. Indeed, the Committee discovered substantial material indicating that U.S. agencies have attempted to ameliorate political violence by several means, including raising official awareness of the importance of suppressing such activities (especially by members of the Salvadoran political and military establishments), providing assistance to official Salvadoran security organizations to

develop more humane methods of operation, and working directly with Salvadoran authorities to resolve many specific cases of political violence.

The Committee believes that, in nearly all instances, contacts between U.S. agencies and Salvadoran organizations or individuals suspected of being involved in political violence have been managed satisfactorily. The Committee has, however, called to the attention of the Executive branch some instances of concern in the handling of particular relationships.

The Committee also has recommended certain improvements in the way U.S. government agencies coordinate and manage their operations in difficult situations such as that with respect to internal security in El Salvador. The Committee believes it is important for U.S. policies and guidelines concerning relationships with foreign organizations and individuals suspected of involvement in political violence to be as explicit as possible. The Committee also believes that further efforts should be made to verify the accuracy of reports of political violence attributable to local organizations or individuals who are receiving U.S. assistance or with whom the U.S. Government is maintaining contact.

III. Legislation: Freedom of Information Act

One of the Committee's major legislative achievements in the 98th Congress was enactment of a measure to modify the CIA's responsibilities under the Freedom of Information Act. Bills relating to this issue were introduced by Committee Members in 1980 and 1981, and the Committee held hearings in 1981 on a bill sponsored by Senator Chafee to exempt from the FOIA operational files of all U.S. intelligence agencies. No action was taken by the Committee on these proposals in the 97th Congress.

The principal arguments for amending the FOIA regarding U.S. intelligence agencies were the effects of the Act in discouraging individuals, organizations and other countries from providing individuals, organizations and other countries from providing information and cooperating in other matters with U.S. intelligence agencies, and the adverse impact on the effective performance of intelligence functions caused by the diversion of experienced intelligence officers from their primary duties.

The principal arguments against such proposals were that the statutory exemptions for classified information and material relating to intelligence sources and methods adequately protected national security interests, and that the interest in public access to information outweighed any effect FOIA requests might have on the intelligence agencies.

On May 18, 1983, Senator Goldwater introduced S. 1324, the Intelligence Information Act of 1983, which was designed to resolve the CIA's concerns while enabling it to continue meeting its responsibilities under FOIA. The bill sought to exempt from the search and review requirements of FOIA only certain operational files of three CIA components—the Directorate of Operations, the

Directorate of Science and Technology, and the Office of Security. All other CIA files, including the files of the Directorate of Intelligence and the Office of the Director which store the intelligence gathered by the CIA and documents on high-level decisions, would remain subject to FOIA search and review requirements (even if they contained information disseminated from operational files). Operational files on "special activities" (covert action operations) would remain subject to FOIA search and review if the existence of the activity were not exempt from disclosure under FOIA. In addition, U.S. citizens and permanent resident aliens would retain the right to have the CIA search and review all its files for information they request about themselves.

Public hearings on S. 1324 were held on June 21 and 28, 1984. At the June 21 hearings, Senator Strom Thurmond, Chairman of the Judiciary Committee and original cosponsor of S. 1324, testified in support of the bill. He was followed by CIA Deputy Director John N. McMahon and other senior CIA officials including Deputy General Counsel Ernest Mayerfeld, the Deputy Director for Operations, the Deputy Director for Science and Technology, the Director of Security, and the Chief of the Information and Privacy Division. Mr. McMahon urged enactment of S. 1324 as a carefully balanced effort to benefit both the CIA's intelligence mission and the public's access to government information. He stated that the bill should "send a clear signal to our sources and to those we hope to recruit that the information which puts them at risk will no longer be subject to the [FOIA] process." At the same time, he emphasized that the "public would receive improved service from the Agency under the FOIA without any meaningful loss of information now released under the Act."

The CIA contended that the requirement to search and review its sensitive operational files in responses to FOIA requests was causing a serious breakdown in compartmentation, a practice vital to protecting the CIA's sources and methods. Because of the extraordinary sensitivity of operational files, the CIA was compelled to assign highly experienced professional officers to the review task to ensure that no information which could compromise sources and methods was inadvertently released. The CIA argued that the necessity to assign these kinds of resources to FOIA review duties drew key personnel away from their primary functions, impairing the Agency's ability to perform its mission effectively.

The CIA offered to redirect personnel and other resources freed by enactment of S. 1324 to improve its responsiveness to FOIA requests regarding information in CIA files not exempt from search and review by the bill. The CIA estimated that passage of the bill would enable it eventually to reduce significantly the current backlog of FOIA requests awaiting response.

At the hearing on June 28, 1983, S. 1324 was endorsed by Mary C. Lawton, the Counsel for Intelligence Policy in the Justice Department, by the President of the Association of Former Intelligence Officers, and by two members of the American Bar Association's Standing Committee on Law and National Security.

Other witnesses at the June 28 hearing raised questions about the intent and language of the bill. Mark Lynch of the American Civil Liberties Union testified that the ACLU could not support the

legislation without amendments concerning requests for information about operations that had been the subject of "abuse" investigations and judicial review of whether a file was properly characterized as an operational file. Witnesses representing the American Newspaper Publishers Association and the Society of Professional Journalists seconded the points raised by the ACLU and emphasized the importance of obtaining specific CIA commitments regarding improved servicing of FOIA requests. A representative of the National Coordinating Committee for the Promotion of History called for a narrower definition of "operational files," a time limit on the duration of an operational file's exempt status, and clarification of the bill's intent regarding policy memoranda and intelligence disseminated outside of operational files.

In addition to the public hearings, consideration of S. 1324 required the Committee to obtain detailed classified information on the CIA's filing system, the handling of documents in the Agency, and the procedures for responding to FOIA requests. The bill was predicated on the assumption that exempting certain operational files of the CIA from the search and review requirements of FOIA would not diminish the amount of meaningful information actually released to the public. The Committee's task was to determine whether this assumption was correct. Committee Members and staff reviewed in detail the way various types of information are stored and disseminated by the CIA. An analysis was made of a wide range of materials released by the CIA in response to FOIA requests over the previous ten years, in order to find out whether such materials would have been released if the bill had been in effect. By studying the types of files in particular components, it was possible to define more precisely which categories of files could be exempted without diminishing the actual release of information to the public.

Based on this inquiry, the Committee developed amendments and legislative history that took into account special characteristics of the CIA's information storage and retrieval systems. The criteria for defining "operational files" eligible for exemption from FOIA search and review requirements were refined to cover only:

1. Files of the Directorate of Operations which document the conduct of foreign intelligence or counterintelligence operations or intelligence or security liaison arrangements or information exchanges with foreign governments or their intelligence or security services;

2. Files of the Directorate for Science and Technology which documents the means by which foreign intelligence or counterintelligence is collected through scientific and technical systems; and

3. Files of the Office of Security which document investigations conducted to determine the suitability of potential foreign intelligence or counterintelligence sources.

The Committee also learned that highly sensitive documents are sometimes disseminated from the CIA's Operations Directorate to other CIA components and then returned for permanent storage solely in Operations Directorate files. The legislative history of the

bill was written to make clear that materials disseminated from operational files would remain subject to FOIA search and review.[5]

Another amendment dealt with matters covered by official investigations of alleged abuses. It required the CIA to continue to search and review all files, including operational files, for information reviewed and relied upon in an official investigation for illegality or impropriety in the conduct of an intelligence activity. The legislative history indicated that all information directly relevant to the subject of the investigation would remain subject to search and review, even if it had been overlooked or withheld during the investigation.[6]

An especially significant amendment established procedures for judicial review in cases of alleged improper withholding of records because of failure to comply with the law. The Committee believed that judicial review procedures were necessary to assure against any attempt to evade the requirements of the law, such as by improperly storing documents in operational files or by improperly exempting files from search and review. The judicial review procedures, both as proposed by the Committee and as enacted, should not require the CIA to expose through litigation (via discovery or other means) the makeup and contents of sensitive CIA file systems to plaintiffs.

Committee Members and staff held numerous discussions on the bill with representatives of the CIA and of civil liberties, press, historical, and other organizations concerned about any diminution of public access to significant intelligence information used by policymakers. In part, the amendments and legislative history devised by the Committee responded to issues raised by these groups. Senate passage of S. 1324 without significant opposition reflected the efforts of the Committee to allay concerns about the public's "right to know" as well as to meet needs of the CIA.

S. 1324 was reported by the Committee on November 9, 1983, with a unanimous recommendation for favorable Senate action. The Senate passed the bill unanimously by voice vote on November 17, 1983.

On September 19, 1984, the House of Representatives passed H.R. 5164, the Central Intelligence Agency Information Act, which had the same basic features as S. 1324. The Senate adopted H.R. 5164 by unanimous voice vote on September 28, 1984; and it was signed into law by the President on October 15, 1984, as Public Law 98-477.

The legislative history of the Central Intelligence Agency Information Act is set forth in the report of the House Permanent Select Committee on Intelligence (H. Rept. No. 98-726). Additional legislative history reflecting the intent of the Senate Select Committee on Intelligence is contained in the report on S. 1324 (S. Rept. No. 98-305).

Among other things, the Senate report discussed future congressional oversight activities. The Select Committee expressed its in-

---

[5] As enacted, the law provides that "files which are the sole respository of disseminated intelligence are not operational files."

[6] As enacted, the law provides for search and review of information concerning "the specific subject matter" of such an investigation.

tention that it would "regularly and closely scrutinize the CIA's implementation of [its program to enhance responsiveness to FOIA requests] to ensure that concrete results are achieved towards stated objectives." The Committee also stated its expectation that oversight would "be facilitated by periodic progress reports and meetings in which Committee Members will be apprised of the status of the Agency's FOIA processing operations." As enacted, the law requires the Director of Central Intelligence to submit unclassified, semiannual reports on the specific measures established to improve the CIA's processing of FOIA requests. The CIA has also made a written pledge to "establish a specific program designed to substantially reduce, if not entirely eliminate, the current two-to-three year backlog" in processing requests.

Another aspect of the law is a provision requiring the Director of Central Intelligence to report by June 1, 1985, on the feasibility of conducting systematic review for declassification and release of CIA information of historical value. In preparing this report, the Director must consult with the Archivist of the United States, the Librarian of Congress, and appropriate historians selected by the Archivist. This provision supplements a voluntary declassification review program agreed to by the Director of Central Intelligence in an exchange of letters with Senator Durenberger on October 3 and 4, 1983. Director Casey agreed in his letter that, after passage of the bill and given adequate resources, the CIA would institute "a new program of selective declassification review of those materials that we believe would be of greatest historical interest and most likely to result in declassification of useful information."

In the final analysis, the Central Intelligence Agency Information Act appears to have resolved a difficult and complex issue that had confronted the Committee since 1979, when the CIA first requested at least partial exemption from FOIA requirements. The law should substantially enhance the CIA's operational effectiveness and reduce the risks of inadvertent exposure of sources and methods. When the backlog is reduced, the Act should free experienced operational personnel from time-consuming FOIA review responsibilities. At the same time, public access to releasable CIA information should be improved because of the steps taken to improve responsiveness to FOIA requests.

COUNTERINTELLIGENCE AND OFFICIAL REPRESENTATION

In May 1984, Senators Huddleston and Leahy proposed legislation aimed at reducing disparities in numbers, conditions and treatment of U.S. officials serving in countries which conduct hostile intelligence activities in this country, and of the representatives of such countries to the United States. In 1983, similar legislation was offered on the Senate Floor but set aside at the request of the Administration. Instead, a report was requested from the Executive branch on this disparity and any measures being considered or taken to rectify it. That report, received by the Committee in March 1984, reinforced concern in the Committee that further steps were necessary to establish equivalence and reciprocity. A serious imbalance exists, and the large number of hostile intelligence

officers active in the United States presents a significant counterintelligence problem for the FBI and other relevant agencies.

As recommended by Senators Huddleston and Leahy, the Committee sought a means to stimulate the Executive branch to greater efforts to reduce and eventually to eliminate such disparities, consistent with U.S. foreign policy interests. While the Committee's concern extends to all countries which conduct intelligence activities harmful to U.S. interests, the Committee was especially interested in reducing the large imbalance between the numbers of Soviet representatives here and American officials in the Soviet Union. Currently, the Soviet Union employs approximately one hundred more Soviet nationals in its diplomatic and consular establishments in the United States—not counting its mission to the United Nations—than the United States employs U.S. nationals in its establishments in the Soviet Union. According to public estimates by the FBI, at least 30% to 40% of all Soviet officials in the United States engage in intelligence activities. Moreover, the Committee believes that there must be greater reciprocity in the treatment, in terms of living conditions, travel, facilities and the like. The Committee is convinced that practical measures to equalize numbers, conditions and treatment of officials between the United States and the Soviet Union are possible without perturbing U.S.-Soviet relations. Indeed, the Committee is convinced that equivalence and reciprocity are necessary ingredients to a balanced relationship.

Accordingly, the Select Committee unanimously adopted an amendment, offered by Senators Huddleston and Leahy, to the FY 1985 Intelligence Authorization Act intended to demonstrate the Congress's concern and desire for greater action on the part of the Executive branch. The Huddleston-Leahy amendment, as subsequently amended after consideration by the Senate Foreign Relations Committee and the House Permanent Select Committee on Intelligence, and enacted by the Congress in October, 1984, accomplishes the following three objectives:

1. It declares the sense of the Congress that "the numbers, status, privileges and immunities, travel, accommodations, and facilities within the United States of any foreign government that engages in intelligence activities harmful to the national security of the United States should not exceed the respective numbers, status, privileges and immunities, travel, accommodations, and facilities, within such country of official representatives of the United States to such country."

2. It requires an annual report from the President to the Foreign Affairs and Intelligence Committees of the respective Houses of Congress on the facts pertaining to numbers, conditions and treatment of United States and relevant foreign officials, as well as any actions taken by the Executive branch to establish equivalence and reciprocity, so that the Congress will have sufficient information to consider the desirability or necessity for further legislation to reach this objective.

3. It eliminates discrimination against the Intelligence Community by removing the requirement in the Foreign Missions Act that the Director of the Office of Foreign Missions be a Foreign Service Officer of the Department of State. The For-

eign Missions Act is amended to require that either the Director or the Deputy Director of the Office of Foreign Missions shall be a Foreign Service Officer while the other of the two shall be a member of the Intelligence Community. This amendment will ensure that counterintelligence considerations are given adequate weight in the operations of the Office of Foreign Missions.

The Committee intends to keep this problem of imbalance and the Executive branch's response to it under close scrutiny.

POLYGRAPHS

In 1983, the Armed Services Committee reported, as part of the Omnibus Defense Authorization Act of 1984 (S. 675), a section which would have limited the use and scope of polygraph examinations in the Department of Defense. This proposal came in response to two changes in Executive branch policy that appeared to provide for greater use of polygraph examinations and to permit adverse actions against military and civilian employees solely for refusing to submit to a polygraph examination. Since this issue emerged, the Intelligence Committtee has worked closely with the Armed Services Committee to ensure the proper balance between the need for protection of the security of highly sensitive classified information and the requirements of fairness and respect for individual privacy in the treatment of government personnel.

Specifically at issue in 1983 were the so-called Carlucci Guidelines of August 6, 1982, which changed Defense Department polygraph policies in order to remedy security problems growing out of increasing backlogs for employees security clearance background investigations. At the time the guidelines were issued, 147 days were needed to complete background investigations for Defense Department personnel being given access to classified information. The Carlucci Guidelines sought to expand the use of polygraph examinations to expedite initial security clearance background investigations and as part of a new program of aperiodic security reevaluations of personnel who continue to handle sensitive compartmentd information for many years.

In addition to the Carlucci Guidelines, Armed Services Committee Members raised separate issues about National Security Decision Directive 84 (NSDD–84) which was issued by the President on March 11, 1983. NSDD–84 dealth with the use of polygraph examinations in cases of "leaks" of classified information. It directed all agencies with employees having access to classified information to revise their existing regulations and policies, as necessary, so that employees could be required to submit to polygraph examinations, when appropriate, in the course of investigations of unauthorized disclosures of classified information.

Intelligence Committee Members recognized both the serious privacy issues and legitimate security concerns raised by the Carlucci Guidelines and NSDD–84. Several Members objected either to hasty issuance of more permissive regulations or to enactment of statutory restrictions on use of the polygraph without a full opportunity to consider the issue in hearings. The Intelligence Committee also had a direct interest in the security of sensitive intelli-

gence information and the procedures applicable to intelligence components of the Defense Department.

To ensure adequate protection of civil liberties pending further consideration of the issue, Senators Chafee and Leahy of the Intelligence Committee offered a Floor amendment to the Defense Authorization Act suspending implementation of the Carlucci Guidelines and NSDD–84 polygraph provisions for the Defense Department until April 15, 1984. The Chafee-Leahy Amendment was offered as a compromise in place of proposals to restrict permanently the use of the polygraph in the Defense Department.

As adopted by the Senate, the Chafee-Leahy Amendment consisted of three parts. First, it prohibited implementation of any change in the Defense Department regulations in effect before August 5, 1982 (i.e., prior to issuance of the Carlucci Guidelines) that would expand the use of polygraph examinations for civilian employees of the Defense Department and members of the Armed Forces. Second, an exception was made to permit implementation of new polygraph policies for the National Security Agency, a component of the Department of Defense which conducts extremely sensitive intelligence activities. Third, prior to the lifting of the suspension on April 15, 1984, the Intelligence Committee and the Armed Services Committee would hold hearings on the use of polygraphs in the Defense Department. These provisions were eventually enacted as part of the Defense Authorization Act.

On February 22, 1984, the Intelligence Committee held a closed hearing on polygraph practices and procedures, with witnesses from the National Security Agency (NSA), the Central Intelligence Agency (CIA), and the Department of Defense (DOD). Expert witnesses from NSA and the CIA described in detail the experience of both agencies in using polygraph examinations for initial background investigations and for subsequent security re-evaluation after a period of years. The witnesses explained that the oral interview with the subject prior to the polygraph examination is the most significant part of the procedure. During that interview, current or prospective employees have an opportunity to discuss matters that otherwise might elicit negative or ambiguous responses during the polygraph examination. At that time, admissions may be made that can indicate real or potential security breaches. The Director of Central Intelligence submitted a study of the utility of the polygraph that recounted 49 examples of personnel security cases in which polygraph procedures uncovered important security data which was not otherwise obtained through the standard full field investigation. Attempts by foreign intelligence services to penetrate the Intelligence Community were uncovered through polygraph procedures in a significant number of cases.

The NSA and CIA witnesses also discussed their agencies' efforts to ensure careful supervision and quality control in the use of polygraph examinations for personnel security purposes. The measures include procedures to ensure fairness in the administration of polygraph examinations, close monitoring of the performance of examiners, and special arrangements for recruitment and training of high-quality examiners. The so-called "failure" rate is minimized by giving individuals an opportunity to repeat the procedure with a different examiner in cases where the initial examination indicates

possible deception. Both agencies stressed that fairness in the administration of polygraph examinations for personnel security purposes is essential to employee morale and that the "failure" rate is very low.

Another crucial point made by the intelligence agency officials was the interplay between the polygraph procedure and other aspects of personnel security policy, especially the standards governing eligibility for access to sensitive compartmented information. Those standards are set forth in an unclassified regulation (Director of Central Intelligence Directive No. 1/14), revised most recently on September 1, 1983. The criteria for adjudication of security clearance cases apply both to persons under consideration for first-time access to sensitive compartmented information and to persons being readjudicated for continued access. They apply to all U.S. government personnel who require access to such information, although particular agencies may adopt more stringent rules if deemed necessary.

Also testifying at the February 22, 1984, hearing was the Deputy Undersecretary of Defense for Policy, General Richard G. Stilwell, who explained the reasons for the Carlucci Guidelines and described provisions that should take account of Congressional concerns. In particular, he stressed that the proposed wider use of polygraph examinations for personnel security purposes are limited in two ways. First, the questions to be covered in the interview are confined to counterintelligence matters, i.e., knowledge of espionage or sabotage against the United States, unauthorized contact with representatives of foreign governments, or unlawful handling of classified documents. This is a much narrower use of the polygraph than the CIA's use to cover such "lifestyle" matters as criminal offenses generally. Second, the number of Defense Department employees to which the new procedures apply is limited to those requiring access to the most highly sensitive special access programs.

Like the NSA and CIA witnesses, General Stilwell emphasized that the polygraph would ordinarily be used as one of several investigative tools to provide the information needed to ascertain an individual's suitability for jobs requiring access to highly sensitive information. The new draft Defense Department regulation provided that no adverse action would be taken solely on the basis of a polygraph examination chart that indicates deception, except in the most compelling cases. In the latter instance, either the Secretary of the Military Department, the NSA Director, or the Secretary or Deputy Secretary of Defense (for other DOD components) would have to make a written finding in each case "that the information in question is of such extreme sensitivity that access under the circumstances poses an unacceptable risk to the national security." The draft regulation also provided that adverse action could not be taken against a person for refusal to take a polygraph examination in criminal or unauthorized disclosure ("leak" investigation) cases. Employees who refused to take a polygraph examination in connection with a special access program could be denied access to the classified information in question, but (except for employees at NSA) the individual would have to be assigned to another position of equal pay and grade not requiring such access.

Based on this hearing record, the Intelligence Committee worked with the Armed Services Committee to develop additional legislation on polygraphing in the Defense Department Authorization Act for Fiscal Year 1985. Intelligence Committee Members were satisfied that wider use of the polygraph for personnel security screening purposes in the Defense Department, subject to the restrictions in the proposed new regulation, would contribute to better security for the most sensitive programs. However, the potentially large number of personnel affected by the new policy caused some misgivings. Committee Members also stressed the importance of measures, such as those adopted by the CIA and NSA, to ensure careful supervision and quality control of the polygraph process so that employees are treated fairly and with full consideration of their privacy.

The result of this consultation between the two Committees was legislation permitting the Defense Department to implement its new regulation as part of a test program involving no more than 3,500 persons in Fiscal Year 1985. The test program provided an opportunity to assess the impact of the new regulations, especially in light of arguments made against polygraphing by witnesses two testified at Senate Armed Services Committee hearings.

As enacted, section 1307 of the Department of Defense Authorization Act, 1985, prohibits the expenditure of funds to implement new DOD polygraph regulations in Fiscal Year 1985, except for such a test program and except for persons assigned or detailed to the CIA or NSA employees. By December 31, 1985, the Secretary of Defense must submit a report to the Armed Services Committee on the experience under this test program.

The Intelligence Committee also expects to evaluate the Defense Department's use of polygraph examinations under this program and to consult with the Armed Services Committee or other interested Committees on any further legislation that might be considered with regard to polygraphing.

NATIONAL HISTORICAL INTELLIGENCE MUSEUM

Intelligence has long played an important role in the history of nations. As well, it has been a vital force in the history of the United States. General Washington relied very heavily on good intelligence in fighting our Revolutionary War, and intelligence has played an important role in every war which we fought, including the Civil War. To the extent these wars were fought to make or keep our Nation free, intelligence has played a vital role in securing this freedom.

The importance of intelligence to the history of the United States has not been fully appreciated. The secrecy with which intelligence operations are necessarily conducted has limited research on the subject until recently, and the intelligence archives of some governments have been opened only on a limited basis to historians. Little has been done to make the significant intelligence accomplishments of the past widely known to the public.

On this basis, the Committee encouraged private efforts to enhance public knowledge and understanding of the history of intelligence, and on November 1, 1983, Senator Goldwater introduced

Senate Resolution 267, which was a measure to support the establishment of a National Historical Intelligence Museum. All Members of the Committee cosponsored this legislation. In his introductory remarks, Senator Goldwater stated that he supported this legislation because it would "allow the American people . . . insight into a complicated subject that is often misunderstood and unfairly criticized."

On November 3, 1983, the Full Committee held an open hearing (Senate Hearing 98–519) to hear testimony on this resolution from a wide variety of witnesses to include William Casey, Director of Central Intelligence and Director of the CIA. During the course of the hearing, Director Casey noted his preference for a "public but not a governmental museum . . . [to guarantee] such a museum would be entirely free of the constraints of national security classifications . . . [with] all of its holdings freely accessible to the public." He went on to say that the museum should be "independent in managing its affairs, especially in deciding what . . . to exhibit." Other witnesses at the hearing supported the concept of the National Historical Intelligence Museum as well.

On November 17, 1983, the full Senate unanimously passed Senate Resolution 267 by voice vote. Private initiatives are now underway to fulfill the measure's provisions. It is hoped that the achievements of American intelligence can be displayed and explained in a manner that captures the public interest and leads to informed support for these activities.

LEGISLATION TO REQUIRE THAT POSITIONS OF DCI AND DDCI BE FILLED WITH CAREER INTELLIGENCE OFFICERS

On September 25, 1984, the Vice Chairman of the Committee, Senator Moynihan, introduced for himself and the Chairman, Senator Goldwater, S. 3019, a bill which would require that the Director of Central Intelligence (DCI) and Deputy Director of Central Intelligence (DDCI) be appointed from among career civilian or military intelligence officers. This legislation would apply only to future appointments to these positions.

In his floor remarks, Senator Moynihan observed that when the CIA was established in 1947 the United States did not have a career service. Thus, it was pointless to suggest that career officers then fill the new positions of DCI and DDCI. He went on to note that, two generations later and after the major rebuilding program of the last decade, there is now a career cadre of military and civilian intelligence officers from which the President can choose highly competent persons to serve as leaders of the Intelligence Community. The Senator said that, after eight years of service on the Intelligence Committee, he and Senator Goldwater arrived at the considered judgment that the President and the Nation would be best served if the issue of the political activities of the Director and Deputy Director of the CIA should never arise by virtue of the career patterns of the person who hold those positions.

S. 3019 was referred to the Committee for consideration. However, the busy legislative schedule did not permit any action to be taken on the bill in the 98th Congress.

IV. Intelligence and Security Activities

ANALYSIS AND PRODUCTION

In its budget authorization for Fiscal Year 1985, the Committee directed that requested increases in analytical manpower be applied to the compilation of an adequate worldwide intelligence data base. The Committee also directed the expenditure of funds for competitive analysis of intelligence topics of special importance. The Committee took these actions to correct a number of deficiencies identified through its review of Intelligence Community products and resource allocation in the analysis and production function.

The Committee has long viewed with concern the Intelligence Community's uneven production on some basic intelligence topics. Each year the Committee has supported additional analytical manpower in the various agencies in an effort to assist the development of an adequate worldwide intelligence data base. Yet our review continues to indicate that analysts are not producing enough basic data to meet important intelligence requirements. Instead, analytic efforts seem to emphasize short term "current" intelligence products. The Committee's actions should assure a reversal of this situation in the years ahead.

Competitive analysis provides to policymakers at least two analytic assessments based on the same all-source intelligence data on a given topic. The need for competitive analysis is set forth in the President's Executive Order on Intelligence Activities. The value of having alternative assessments from those developed through the standard interagency consensus building process was illustrated by the "B Team"—a group of non-government experts commissioned by the President's Foreign Intelligence Advisory Board in 1976 to examine whether intelligence data could support conclusions different from ones drawn in National Intelligence Estimates.

The Committee's action should assure that competitive analysis, independent of the normal estimate process, is conducted in several areas of vital importance to the national security. This competitive analytical approach not only affords policymakers the benefit of a fresh perspective, but encourages fuller exchange of views within the Intelligence Community. The Committee supports wider use of competitive intelligence analysis in the future and will carefully assess the Community's actions taken pursuant to these concerns.

COUNTERINTELLIGENCE

For several years, the Committee has emphasized the need to improve the U.S. counterintelligence capabilities by, among other things, re-establishment of a career counterintelligence service within the CIA and organizational and policy changes to promote multidisciplinary counterintelligence analysis. In the Intelligence Authorization Act Report for FY 1985, the Congress directed that specific steps be taken to achieve these objectives.

Counterintelligence (CI) requires critical appraisals of the operational security and vulnerability of intelligence collection from human sources and by technical means. This means testing the conclusions and assumptions of intelligence personnel engaged in

collection and in the analysis of intelligence data. For that reason, the job of CI specialist in agencies such as the CIA has not always been popular or career-enchancing. If it is to be done conscientiously, as the Committee desires, it must be done by people whose careers may progress in the ranks of CI specialists, and do not depend on the favor of the collectors whose work they scrutinize. Although CI should not be a force unto itself and the DCI must always judge between contrasting views, it is important to foster and protect the expression of independent views by establishing a career CI service within the CIA.

Additionally, in agencies that collect intelligence by technical means, there is a need to apply CI discipline and provide for the kind of operational security and testing that is traditional for human sources. The need for such operational security and validity-testing is especially important in such agencies, because of the number of recent compromises of technical systems by espionage and unauthorized public disclosure. Inadequate operational security could affect the Committee's willingness to authorize funds for such systems.

COLLECTION

In its budget authorization for Fiscal Year 1985, the Committee began reforms in the Intelligence Community's approach to collection. It is the intent of the Committee to see these reforms through to completion in the years ahead. The need for reform became evident to the Committee given certain adverse trends affecting U.S. intelligence, to include: Potential resource constraints in the future, difficulties in protecting certain major sensitive collection systems from compromise, a growing imbalance between collection and analytic capabilities, and persistent gaps in information on certain subjects of great importance to national security. The actions taken by the Committee included strong support and encouragement of selected collection proposals of the Intelligence Community (at the expense of others), combined with Committee direction to place greater emphasis and resources on certain other activities.

In the technical collection field, the emphasis will be on more focused, secure, and innovative techniques. The Committee is also studying certain major programs for possible modifications in light of a changing operational environment. As regards human collection, the Committee has taken steps to improve the variety, type, and security of cover employed by the Intelligence Community in the conduct of clandestine collection. The Committee has also directed actions which should lead to improved collection, processing, and retrieval of data through overt means.

The importance of these reforms initiated by the Committee, as well as these in itiated by the House Permanent Select Committee on Intelligence, cannot be overstated. They should lead to a reversal of the adverse trends affecting the Intelligence Community's collection capabilities addressed above. As well, they should initiate a shift away from the collection of data that is currently proving to be of diminishing value, and toward the collection of more operationally useful intelligence in the years ahead.

HUMINT COLLECTION

Collection of intelligence from human sources (HUMINT) has received special attention from the Committee. Much of the oversight in this area has been conducted as part of the annual review of the CIA's budget authorization request. Other special inquiries, such as the examination of collection regarding political violence in El Salvador, have also addressed certain HUMINT concerns. These include both the quality of HUMINT collection efforts and the propriety of relationships with sources that could risk involvement of the U.S. Government in human rights violations.

The Committee's oversight of HUMINT collection operations has taken into account the need for tight compartmentation of the most sensitve information about sources and methods. For example, only a small number of staff have been given access to certain types of information.

During the past two years, U.S. military operations in Grenada and the continuing terrorist actions against U.S. military forces and civilian officals in Lebanon raised important questions about the adequacy of HUMINT collection in dealing with such situations. After the Grenada operation, the Committee reviewed several aspects of the collection and dissemination of HUMINT in the period immediately before the dispatch of U.S. forces. Certain collection gaps and dissemination problems were identified, and responsible officials were urged to take the lessons into account in planning for future needs.

In the aftermath of the bombing of the Marine facility in Lebanon in 1983, the Long Commission submitted a lengthy report to the Defense Department on the events surrounding the incident. The Long Commission report indicated a need for better HUMINT collection capabilities in circumstances such as those in Lebanon where U.S. military forces may be deployed. The committee examined the Long Commission's detailed classified report with great interest, and the Defense Intelligence Agency (DIA) provided a briefing on certain measures taken in response to the recommendations of the Commission. Some elements of the Long Commission report and the situation in Lebanon were considered in the context of the Committee's oversight of counter-terrorism intelligence capabilities.

HUMINT collection is not confined to the CIA, nor does it rely solely on clandestine agents. Other agencies in the Intelligence Community, including the Defense Department, play an essential part in the collection of intelligence from human sources. State Department diplomatic reporting is also of value to the Intelligence Community as well as to policymakers. The Committee has been kept informed of the HUMINT collection programs of other agencies and has considered serveral specific policy issues.

Intelligence components of the Defense Department have traditionally collected HUMINT from both open and clandestine sources. Executive Order 12333, Section 1.12(d) authorizes the foreign intelligence and counterintelligence elements of the Army, Navy, Air Force, and Marine Corps to collect "military and military-related foreign intelligence and counterintelligence." The Order also provides:

> When collection is conducted in response to national foreign intelligence requirements, it will be conducted in accordance with guidance from the Director of Central Intelligence. Collection of national foreign intelligence, not otherwise obtainable, outside the United States shall be coordinated with the CIA, and such collection within the United States shall be coordinated with the FBI.

The reference to collection of intelligence "not otherwise obtainable" means collection from clandestine sources, rather than from open sources or contacts. In addition to the intelligence elements of the military services, the Executive Order authorizes collection by the Defense Intelligence Agency. Section 1.12(a) not only makes DIA responsible for the coordination of all Defense Department intelligence collection requirements and for management of the Defense Attaché system, but also gives DIA the authority to collect "military and military-related intelligence" for other Defense components, for non-Defense agencies, and for national intelligence purposes.

The Committee has examined the extent and nature of HUMINT collection activities by Defense Department intelligence components. Among the issues considered specifically by the Committee were the practices and procedures for CIA coordination of any such HUMINT collection by clandestine means abroad. Section 1.8(d) of the Executive Order requires the CIA to "coordinate . . . the collection of information not otherwise obtainable when conducted outside the United States by other departments and agencies." This was one of the subjects addressed at a closed hearing before the Subcommittee on Collection and Foreign Operations in 1984. The Subcommittee heard testimony from senior Defense Department intelligence officials regarding HUMINT collection by Defense Department components. The responsibilities of particular components were explained. Senior CIA officials described the CIA's role with respect to clandestine HUMINT collection by Defense Department components. The Committee is concerned that all clandestine HUMINT collection by U.S. agencies be carefully coordinated by the CIA to avoid overlap or duplication of effort.

Another issue of concern to the Committee was the need to improve the overt HUMINT collection capabilities of the Defense Department. For example, the Committee has examined ways to improve the management and performance of the Defense Attaché System. While many of the Attachés are outstanding and make a great contribution to meeting U.S. intelligence needs, the overall quality has been uneven. DIA has recognized this problem, and the Committee has regularly sought information on the steps taken to remedy deficiencies.

Similarly, the Committee has looked at ways to enhance the quality and extent of Foreign Service diplomatic reporting that can also meet important U.S. intelligence requirements. State Department officials have advised the Committee of new initiatives being implemented or planned to place greater emphasis within the Department on the collection and reporting of information which also satisfies intelligence requirements. Reporting by Foreign Service Officers and Defense Attachés is frequently the only source of certain

types of information, and it should be able to satisfy many information needs with fewer administrative difficulties or risks than collection from clandestine sources.

Other U.S. intelligence needs cannot adequately be met without the maintenance and development of highly sensitive clandestine HUMINT collection capabilities that require the most careful management to ensure operational security and effectiveness. Enhancement of these capabilities is one of the most important and difficult jobs that must be undertaken by the responsible agencies. In this regard, the Committee has encouraged better security for HUMINT personnel. Another Committee initiative, the Intelligence Identities Protection Act, passed in 1982, requires the President to submit an annual report to the Intelligence Committees on measures to protect the identities of covert agents. In addition, the Committee has examined steps that may be taken to expand clandestine HUMINT collection capabilities in order to meet new requirements, as well as to satisfy current requirements more effectively.

COMMUNICATIONS SECURITY PROGRAMS

The Committee maintains a continuing interest in the adequacy of U.S. counterintelligence and security measures to protect the privacy of U.S. communications from Soviet and other interception and exploitation. There were significant developments in this field in 1984, and the Committee received a detailed briefing on the current threat and possible countermeasures.

The National Security Agency plays a leading role in the U.S. Government's communications security (COMSEC) efforts. Executive Order 12333 on U.S. Intelligence Activities states that NSA's responsibilities "shall include . . . [e]xecuting the responsibilities of the Secretary of Defense as executive agent for the communications security of the United States Government." The Committee's oversight of NSA's signals intelligence collection programs has given the Committee an opportunity to become more familiar with COMSEC programs as well. In 1978, the Committee found allegations of NSA harassment of scientists working in the field of public cryptography to be groundless. At the same time, the Committee noted the important of measures to protect the privacy of nonclassified data stored and transmitted by Federal Government computers.

In early 1984, the Committee received the biennial report of the National Security Council's Communications Security Committee which recommended establishment of a vigorous national program to assess the full extent of U.S. communications vulnerabilities and a comprehensive assessment of the requirements for corrective action. Earlier reports from the Intelligence Community had described the nature and extent of the Soviet bloc threat to U.S. communications and the need for more effective countermeasures.

Based on these inter-agency reports and recommendations, the National Security Council undertook a reasssessment of Executive branch policies and the responsibilities of particular agencies. Significant initiatives were taken in 1977 to identify and remedy COMSEC problems, but technological advances and other charges

in communications and automated information systems have occurred since then. The Committee was kept informed of proposals under consideration by the NSC in 1984 and received a briefing from the NSC staff on a new Presidential Directive on National Policy on Telecommunications and Automated Information Systems Security, prior to its issuance on September 17, 1984. (The unclassified text of National Security Decision Directive 145 is included as an appendix to this report).

The Committee was briefed by NSA officials in September, 1984, on the serious Soviet intelligence threat to U.S. communications. Hostile intelligence services have comparatively easy access to some of the nation's most sensitive information. As a result, some of the advantages we hold in advanced technology, strategic policy and planning, nuclear weapons development and deployment, as well as numerous other vital areas have been eroded. A similar problem exists with the security of the nation's automated information systems.

Telephone communications, in particular those sent over microwave lines or through a satellite, are extremely vulnerable to interception and provide a lucrative target of opportunity. In 1978, a Soviet diplomat defected to the U.S. and said that telephone and telex calls were monitored at the Soviet recreational facility in Glen Cove, New York which required the shipment of tons of material to Moscow annually. It is interesting to note that the new Soviet Embassy in Washington, D.C. and the Consulate in San Francisco are ideally situated to monitor sensitive U.S. communications in those areas. Individuals at all levels in government, industry, and the private sector have developed the false sense of security that they can talk around sensitive subjects. Additionally, the telephone companies have the flexibility to route calls via microwave, landline, or satellite, or any combination of the three thus increasing the challenge of protecting sensitive information. Satellite communications are potentially an extremely valuable source of information as they can simultaneously transmit thousands of telephone, TV, and computer to computer transactions. The explosion in computer networks and the electronic transfer of data adds another major area in which there is a significant vulnerability to unauthorized exploitation. The critical deficiencies in our information security posture affect the communications of our national leadership, military and defense industries, tactical military operations, weapons research and development, and economic interests.

After the NSA briefing, the Committee worked with the Armed Services Committee on language regarding communications security to be included in the statement of managers accompanying the Conference Report on the Defense Authorization Act for FY 1985. The conferees requested the Secretary of Defense to provide to the Armed Services and Intelligence Committees by March 1, 1985, a report on the status of measures being implemented to remedy deficiencies in COMSEC planning and execution and an assessment of the additional funds and personnel which would be required to support a national COMSEC effort. The report is also to address the implications of proposals under consideration for the privacy of non-government communications as well as the impact on the full range of governmental functions.

The conferees said that the Armed Services Committees, in concert with the Intelligence Committees, intended to examine in greater detail the subject of U.S. communications security in connection with Congressional review of the Fiscal Year 1986 budget request.

Concerns have been raised about NSA's role in the national COMSEC program. First, the extent of NSA's role with regard to security of unclassified data in federal government computers is unclear. Second, the relationships between NSA and unclassified private sector communications and computer security measures are uncertain. The 1984 Presidential Directive deals only with protection of information for national security reasons, not with other private considerations for either government or private sector data. The intent is to offer help to the private sector on a voluntary basis in protecting unclassified information. Therefore, a proposal that the U.S. Government support private research and development efforts on a low-cost secure telephone system is of special interest to the Committee.

Given the vulnerability of communications and computers to intrusions by hostile intelligence services and others, the Committee expects to continue to follow closely the implementation of national COMSEC policy.

V. General Oversight

FOREIGN INTELLIGENCE SURVEILLANCE ACT

The Foreign Intelligence Surveillance Act of 1978 (FISA) established comprehensive legal standards and procedures for the use of electronic surveillance to collect foreign intelligence and counterintelligence within the United States. The Act provided the first legislative authorization for wiretapping and other forms of electronic surveillance for intelligence purposes against foreign powers and foreign agents in this country. It created the Foreign Intelligence Surveillance Court, composed of seven federal district judges, to review and approve surveillances capable of monitoring United States persons who are in the United States.

Section 108(b) of FISA provides that the Select Committee is to report to the Senate annually concerning the implementation of the Act for the first five years after its effective date. The Select Committee submitted the last of these required reports on October 5, 1984 (S. Rep. No. 98-660). Because this was the last required FISA report to the Senate, the Select Committee took the opportunity to review the whole period since FISA was enacted.

The Subcommittee on Legislation and the Rights of Americans held two closed hearings on FISA and an additional closed hearing on FBI guidelines which covered physical search techniques. At these hearings, the Subcommittee heard testimony from both policy-makers and working-level officials of the principal agencies involved—the Department of Justice, the FBI, and the National Security Agency. The presiding judge of the FISA Court, Honorable John Lewis Smith, Jr., Senior Judge, U.S. District Court, District of Columbia, also testified before the Subcommittee. The hearings were supplemented by written questions and staff briefings. The

Subcommittee also asked witnesses who testified at the hearings on FISA in 1976–77 to submit any views they might have on the Act. Finally, the Committee received the regular semiannual reports from the Attorney General for the periods July-December, 1982, January-June, 1983, and July-December, 1983, supplemented by staff briefings. Based on these oversight efforts, the Subcommittee prepared and the Committee adopted both the unclassified report and a longer classified report.

The Committee's report found:

> ". . . the Act has achieved its principal objectives. Legal uncertainties that had previously inhibited legitimate electronic surveillance were resolved, and the result was enhancement of U.S. intelligence capabilities. At the same time, the Act has contributed directly to the protection of the constitutional rights and privacy interests of U.S. persons."

Noting that the number of applications for surveillance orders approved by the FISA Court has increased steadily since 1980, the Committee stated that it was "convinced that this increase does not reflect any relaxation in strict protections for the privacy of U.S. persons." The report emphasized the information provided to the Committee on electronic surveillance of U.S. persons:

> "The Committee has been fully briefed on the number of U.S. persons who have been subjected to FISA surveillance, as well as the time periods and the methods involved and, in summary form, the justification for each such surveillance."

The report on FISA implementation did not recommend any changes in the Act at this time:

> "Some technical revisions in FISA would appear warranted, especially if they could be considered without reopening debate on the basic framework of the Act. The Justice Department and the agencies that conducted FISA surveillance do not believe, however, that these comparatively minor problems justify amending FISA at this time. The Committee recommends, therefore, that the Act should remain in effect without amendment until such time as the Executive branch submits new proposals for specific changes."

Issues discussed in the Committee's report included how FISA applications and implementation of minimization procedures are reviewed, how one decides whether to conduct electronic surveillance under FISA or under Title III of the Omnibus Crime Control Act of 1968, standards for non-FISA surveillance of persons in the United States and U.S. persons abroad, and the use of physical searches. On the physical search issue, the report stated:

> "The Committee is persuaded that a court order procedure for physical searches in the United States, using either the FISA procedure or a procedure comparable to FISA, ought to be established. . . . The Committee intends

to develop a legislative proposal . . . in consultation with the Attorney General."

The closed hearing that dealt with physical searches also considered other issues raised by revisions in the FBI Guidelines on Foreign Intelligence Collection and Foreign Counterintelligence Investigations. Of particular concern was the effect of changes in the guidelines, pursuant to Executive Order 12333, which removed the criterion of clandestinity from definitions of "foreign counterintelligence" and "intelligence activities." The Justice Department emphasized that although overt intelligence activities of foreign powers could warrant investigative interest, this "does not, in our view, justify the inference that perfectly legitimate exercises of First Amendment rights are subject to investigation under the Guidelines." The Committee was assured that there was not intention to investigate any form of political activity not investigated under the previous guidelines.

UNAUTHORIZED DISCLOSURE AND ESPIONAGE CASES

The Select Committee on Intelligence has become extremely concerned about the increasing frequency of unauthorized disclosure of classified information, commonly referred to as leaks. During the past two years, the Committee has held a number of hearings and briefings regarding various aspects of the unauthorized disclosure problem including the efforts of the Administration to cope with this situation.

A leak is defined as the knowing unauthorized disclosure of classified information by a cleared person (one having authorized access to the information) to one who is not cleared. Sometimes, this occurs under circumstances which would reasonably lead to a conclusion that the information could have been declassified through regular, formal channels than published on an unattributed basis. In several cases, however, the information conveyed on such a basis is highly sensitive leading to the conclusion or inference that it would not have been eligible for declassification. Unauthorized disclosures of classified information directly to foreign governments or foreign intelligence services are not considered leaks but conventional espionage, which will be addressed later in this section.

The Administration has expressed concern about the growing problem of unauthorized disclosures and has proposed a number of initiatives to address the situation. In addition to increased efforts to investigate leaks and prosecute individuals guilty of unauthorized disclosure, the Administration proposed increased use of prepublication review agreements and consent to the polygraph testing as a condition of employment in sensitive positions. Both are currently in use in various segments of the Intelligence Community. The Congress expressed concern about the use and possible abuse of these methods, and proposed legislation to prohibit or delay wider utilization of them. The President deferred implementation of a new pre-publication review agreement pending further consultation with the Congress.

In February, 1984, the Select Committee held a hearing to review the experience of components of the Intelligence Community with

leaks and prepublication review agreements. The results of that hearing were beneficial to the Members of the Committee and other Senators in assessing the methods available to protect the security of classified intelligence information.

The Committee has also focused on specific cases of unauthorized disclosures in an effort to better understand the complexity of the problem. Using specific cases, the Committee reviewed each step of the process from the discovery of a leak, through the investigation of that leak, to the decision as to whether to prosecute a leaker if discovered. By this exercise, the Committee has become more appreciative of the complexity of the problem as well as of the limitations on resources of the Intelligence Community in this area and the problem of prosecution in some cases.

As a result of these hearings, the Select Committee has worked closely with the Intelligence Community to strengthen its investigative resources. The Committee remains concerned that unauthorized disclosure of classified information continues to pose a problem to the security of the United States.

A recent case of particular interest to the Committee is the prosecution of a civilian Naval intelligence analyst, Samuel L. Morison, on charges relating to the unauthorized disclosure of classified photographs of Soviet ships to the British publication Jane's Defense Weekly. This is the first case in recent years of federal prosecution for unauthorized disclosure of classified information to the news media.

The Select Committee has continued to monitor cases of espionage against the United States and its allies. The Intelligence Community has kept the Committee informed about the various cases within the United States and in other countries, including a damage assessment of each espionage instance. The cases in the United States include those involving James Durward Harper, Jr., Richard Craig Smith, F.B.I. agent Richard W. Miller, Penyu B. Kostadinov (Bulgarian), Ernst Ludwig Forbrich (West German), Alice Michelson (East German), Aleksandr N. Mekheyev (Soviet), and Oleg V. Konstantinov (Soviet), the two Soviets being diplomats associated with the United Nations. During 1983–1984, over 150 Soviet diplomats and other citizens were expelled from various countries after being accused of spying. The FBI and other agencies in the Intelligence Community have kept the Committee current on those cases, as well as cases abroad affection U.S. and allied security interests.

The Select Committee remains concerned about the extensive nature of Soviet espionage efforts against the United States, its allies, and organizations such as NATO. In addition to the use of human espionage, the Soviet Union is involved in extensive technical espionage efforts including the interception of telephone calls in areas of the United States where the Soviet Union maintains official facilities.

Increased efforts and resources must be devoted to countering this increasing threat. The Select Committee has taken initiatives to strengthen the capabilities of the Intelligence Division of the F.B.I. Those initiatives, the efforts of the Administration, and the cooperation of our allies have resulted in increased detection and prosecution of espionage cases. The Select Committee shall contin-

ue to support increased efforts to safeguard classified information and U.S. security concerns.

TERRORISM

International terrorism increasingly commands the attention of Members of Congress, the Administration and the public. The nature, goals, tactics and seriousness of terrorist activities have changed in the last five years. 271 U.S. citizens were killed in terrorist incidents abroad in 1983, more than the total killed in the preceding 15 years. The 1983 bombing attacks on the U.S. Embassy and the Multinational Force Headquarters in Beirut, Lebanon, the 1981 attempted assassination of Pope John Paul II, and the bombing of the Senate wing at the Capitol, underscore the magnitude of the terrorist threat facing the United States and its allies. The Committee believes that developing effective policies and means to combat international terrorism, including state-sponsored terrorism, must be a top priority of the United States Government.

On April 27, 1983, Senator Goldwater introduced S. Res. 116, a resolution condemning the April 18 bombing of the U.S. Embassy in Beirut. In addition to paying tribute to the families and the victims who lost their lives in the attack, the resolution reflected Congressional concern for the continual safety and welfare of U.S. officials assigned to the Middle East. Further, the measure expressed unanimous contempt for the perpetrators of such "brutal and cowardly" acts of violence.

In order to better understand international terrorism, the Committee and staff received briefings and reports from the Intelligence Community on this subject. These helped clarify the changing scope and nature of the terrorism threat worldwide. All agencies asked have been cooperative in providing information relating to terrorism.

The Committee found that intelligence about and assessments of the threat play a critical role in planning protective measures against terrorist acts. Moreover, intelligence concerning the activities and objectives of foreign terrorist groups contributes to overall estimates of political stability in areas considered vital to U.S. national security interests. Without adequate intelligence about the terrorist threat, policymakers are unable to devise effective counterterrorism policies and mechanisms.

In general, the Committee believes the Intelligence Community has been making improvements in its collection against the terrorist threat. In spite of the unusual collection difficulties, the quantity of available information has steadily increased. As the data base has expanded, the quality of analysis has also improved. Nevertheless, the Committee recognizes that much remains to be done in strengthening the collection, analysis and dissemination of intelligence on terrorism.

In addition to monitoring and evaluating the quantity and quality of intelligence and analysis on terrorism, the Committee has the responsibility to address the dedication and coordination of terrorism-related resources within the Intelligence Community. During the 1983–1984 period, with the support of the Committee in the budget review, changes were initiated within agencies to pro-

vide more timely and better collection, analysis, and presentation of intelligence concerning terrorist incidents. For example, the Committee approved new positions for terrorism analysts to work in conjunction with regional specialists in the Bureau of Intelligence and Research (INR) in the Department of State. Furthermore, in the summer of 1984, INR created a twenty-four hour terrorism watch office to ensure all source, relevant current intelligence was made available to policymakers.

Intra-agency initiatives during 1983 and 1984 were complemented by an effort to improve Community coordination at all levels, including linking terrorism analysts through a computer system which has provided a continuous and rapid exchange of information and ideas. A senior inter-agency working group on terrorism has been reorganized and strengthened in order to improve coordination of counterterrorism efforts.

While most examples of the coordination of Community capabilities are classified, the Committee notes the exceptional performance of all active agencies during the months preceding the summer Olympics in Los Angeles. Given the number and combination of agencies tasked to collect and evaluate intelligence and possibly take law enforcement action, inter-agency jurisdictional differences and coordination problems were of concern to the Committee. However, following hearings held before the Senate Judiciary Subcommittee on Security and Terrorism and briefings provided the Senate Intelligence Committee in which problems were identified and reviewed, cooperation improved. During the course of the Olympic Games, intelligence information was collected, evaluated and effectively channelled to the appropriate agencies. The Committee expects to continue to review and assist in the resolution of inter-agency problems relating to special cases which develop.

Because of the Committee's concern about terrorism, a briefing was provided by members of the State Department and National Security Council staff on National Security Decision Directive 138 (NSDD–138). This Directive outlined a policy context for terrorism initiatives anticipated by the Administration. While the Committee recognizes the President's National Security Decisions do not require the Committee's approval, it appreciates the opportunity to review and provide comments on those decisions which have a bearing on the Intelligence Community. In the case of NSDD–138, the requirements clearly affect Community activities. The Committee is continuing to work with the Administration in refining its understanding of the terms and objections of NSDD–138. At the time this Committee report was being prepared, the Administration was still considering the comments contributed by various agencies with terrorism related responsibilities. The Committee anticipates being apprised of the final terms for implementation of NSDD–138.

The Committee has also followed the developments in the case of the attempted assassination of Pope John Paul II. A closed hearing was held in 1983 to review the information then available to the United States Government on this case and to obtain an assessment of the possibility of Bulgarian and Soviet involvement in the plot to assassinate the Pope. As further information has come to light, the Committee has continued to examine the facts bearing on

this question. The Committee has also been advised of the desire of Italian Government authorities that there be no outside interference with their investigation and other legal proceedings on the case.

Another matter of interest to the Committee was the Attorney General's issuance of new guidelines for FBI domestic terrorism investigations on March 7, 1983. Committee Members and staff made inquiries regarding the intent and meaning of the new guidelines. The FBI has kept the Committee informed of its implementation of the new guidelines and the Committee is regularly advised concerning the domestic and international organizations that are the subjects of FBI terrorism and counter-intelligence investigations.

CHEMICAL AND BIOLOGICAL WEAPONS

The Committee held hearings on February 2, 1984, and September 18, 1984, regarding the use of chemical/biological weapons (CBW) by the Soviet Union, by Soviet-supported regimes in Afghanistan and Southeast Asia, and by combatants in the Middle East. These sessions and subsequent staff investigations, which included extensive staff travel in Southeast Asia and Europe, focused on the Intelligence Community's response to reported use of CBW in the past, their current collection and analysis capabilities, and an examination of what additional resources might be needed to insure adequate capabilities against future CBW targets. The difficulties and complexities of the environment dictate that the Intelligence Community must continue to dedicate substantial resources to the CBW collection and analysis effort. The implications of the current use of chemical and biological weapons and risks of future use by both nation states and terrorists, are substantial. While the Committee believes that the Intelligence Community has begun to identify the scope of the threat, it now needs to take steps which would enable it to provide policymakers with more timely information on this vital subject.

KAL 007

On September 1, 1983, Soviet military aircraft destroyed a Korean Air Lines (KAL) Boeing 747 on a commercial flight from Anchorage, Alaska to Seoul, South Korea, killing all 269 passengers and crew. KAL Flight 007 had diverged from its scheduled route over international waters and entered Soviet territory twice, initially over Kamchatka Peninsula and later over Sakhalin Island.

Soviet authorities claimed that KAL 007 was conducting a mission for U.S. intelligence and that the airliner was destroyed after intruding into Soviet airspace and failing to heed signals to land. The U.S. Government denied that KAL 007 was on any official mission whatsoever and indicated that it had inadvertently strayed over Soviet territory, probably because of a navigational error or malfunction.

Shortly after the event, the Committee was briefed on the KAL 007 tragedy by the appropriate U.S. intelligence agencies. Subsequently, Committee staff received periodic updates. Individual Committee Members also pursued the matter in separate meetings with intelligence and State Department officials.

The Intelligence Community was not monitoring the KAL flight, and was not in a position to inform civil aviation authorities of its course. The Committee concludes that there was no direct or indirect involvement by the U.S. Intelligence Community in the events leading to the KAL 007 disaster. The Committee has seen no intelligence derived from this tragedy—except that Soviet authorities shoot down airliners and continue to defend their "right" to do so.

GRENADA

The Select Committee received a briefing on October 28, 1983, concerning the United States' military action in Grenada. The Committee heard testimony from State Department and Intelligence Community witnesses concerning the action, the events leading to it, and the situation on Grenada in its wake.

During the course of the hearing, the Committee concentrated on questions related to the extent of Cuban activity and presence on Grenada, the level of Soviet and Cuban weaponry on the island, the legal basis for the U.S. action, and the existing security situation on Grenada.

Members of the Select Committee pursued, with Administration witnesses, questions related to the quality and effectiveness of tactical intelligence throughout the course of the operation. Committee Members made recommendations for improving tactical intelligence and the ability of commanders to use it effectively as possible in operations such as the one on Grenada.

ARMS CONTROL

The Select Committee receives periodic reports from the Intelligence Community and various arms control agencies on Soviet military activities relevant to various arms limitation agreements and ongoing arms control talks. Pursuant to its obligations under Senate Resolution 400 (94th Congress), the Committee has continued to report to other relevant Committees, and Senators not on the Select Committee, about such developments. During the past two years, the Committee staff has actively monitored developments and Soviet activities of concern to: the SALT I Agreement; the ABM Treaties; the Nuclear Threshold Test Ban Treaty; the Geneva Protocol on Chemical Weapons and the Biological Weapons Convention; the informal policy of not undercutting the SALT II Agreement; the ongoing Mutual and Balanced Force Reduction talks; and the suspended talks on Strategic and Intermediate Range Nuclear Weapons.

In 1983 and 1984, the Committee and staff held many hearings and briefings on arms control matters, with particular emphasis on the implications of arms control monitoring requirements for future Intelligence Community budgets and on Soviet compliance with existing agreements. Both Members and staff held discussions with U.S. negotiators and their delegations, as well as with representatives of some of our allies involved in multilateral negotiations. Committee Members, Senators Cohen, Biden and Leahy, also spoke directly with Soviet leaders to stress the central role of the Committee in advising the Senate on whether agreements can be monitored, and on the Committee's strong commitment to effective

verification provisions. In these discussions, Committee Members also emphasized to Soviet leaders the importance of a satisfactory resolution of U.S. questions concerning Soviet compliance with its arms control obligations and commitments.

ARMS CONTROL VIOLATIONS

In January 1984, at the behest of Congress, the President submitted a report on seven Soviet violations and probable violations of arms control agreements. The Committee held hearings on the report, and since has had more detailed briefings on the evidence presented. The Congress also requested that the President release a more extensive study on Soviet violations done in 1983 by the General Advisory Committee on Arms Control and Disarmament. That report, on which the Committee had earlier been fully briefed, has been released and the Committee will continue to examine it into the next Congress.

The intent of the Select Committee is to be fully informed on all aspects of arms control agreements currently in effect and on those in the negotiating stage, with emphasis on monitoring and verification. It is expected that any future agreements brought before the Senate will be subject to full review by the Select Committee. Moreover, the Committee will continue to stress the requirements for arms control monitoring during its review of the Intelligence Community's budget.

ANTI-SATELLITE (ASAT) ARMS CONTROL

On June 6, 1984, the Committee held a hearing on intelligence and policy assessments concerning the issue of space arms control. Testifying before the Committee were officials from the Central Intelligence Agency, the Arms Control and Disarmament Agency, and the Department of Defense.

The Committee was briefed on the role of space in Soviet military doctrine and the range of Soviet ASAT programs and capabilities. In addition, the hearing included a review of the principal issues related to monitoring Soviet compliance with an ASAT arms control agreement. Officials from the Arms Control and Disarmament Agency highlighted key points from the President's ASAT report ("Report to the Congress on U.S. Policy on ASAT Arms Control" March 31, 1984) and briefed the Committee on the Administration's policy concerning the potential for negotiations with the Soviets on space arms control. Finally, an overview of the U.S. ASAT program was provided by an official from the Department of Defense.

The Committee noted the difficulties in devising a comprehensive ASAT arms control proposal that would: 1) be effectively verifiable in light of the wide range of Soviet capabilities to attack or interfere with U.S. satellites; and 2) be consistent with the national security interests of the U.S. and its allies. The Committee also noted the potential conflict between an ASAT accord and the preservation of research options currently envisoned by President Reagan's Strategic Defense Initiative, a program designed to explore the potential for defense against ballistic missile attack.

The Committee discussed the verifiability of more limited ASAT agreements, and encouraged the Administration to continue its review of ASAT arms control options. The Committee expressed its intention to pursue this further following the completion of such a review.

SOVIET SPACE PROGRAM

During the past two years, the Select Committee focused on Soviet military activities in space both through normal budget oversight of the Intelligence Community and through a series of special briefings. The briefings focused not only on the space systems, both operational and in the research and development phase, but also on Soviet intentions in space and how these systems could be utilized for war-fighting capability. Lastly, the Select Committee reviewed the ability of the United States to adequately collect intelligence on Soviet activities and intentions in space.

The Select Committee's special interest in the Intelligence Community's capabilities vis a vis the Soviet space program was prompted by a December, 1982, Senate Committee on Commerce, Science, and Transportation report entitled "Soviet Space Programs 1976–1980." This report concluded that "the military establishment in the Soviet Union plays a large, possible dominant, role in the space program," that Soviet space expenditures are "considerably larger than the present U.S. program," and "that the Soviet Union devotes a much larger proportion of its space budget to military applications than the United States." Further, the Soviet space program was also addressed in "Soviet Military Power 1984". It concluded that "there has been no change in heavy Soviet emphasis on the military applications of space, reflecting their view, noted as early as two decades ago in the Soviet military publication, Military Thought, that 'the mastering of space (is) a prerequisite for achieving victory in war.' " In addition, the Soviet operational ASAT system, the high Soviet launch rate (about five times that of the United States), and the claims that 85% of Soviet space launches are either military or military/civilian in nature makes it vital that the Intelligence Community be able to provide timely intelligence information on Soviet space activities and intentions to U.S. policymakers.

The Select Committee has strongly supported increased efforts by the Intelligence Community to improve its capabilities in this area. The Committee has also recommended some new initiatives to the Community that would further improve collection capability on Soviet space activities. Finally, in a related action, the Committee has strongly supported the Department of Defense program to provide assured access to space for vital national security missions.

The Committee shall continue to review Soviet space activities and monitor the maturing capability of the United States to understand Soviet space programs.

VI. Budget Authorization

The Committee utilizes the annual budget authorization process as one of the principal means to fulfill its responsibility of Congressional oversight of U.S. intelligence activities. Through this proc-

ess, the Committee reviews and evaluates U.S. intelligence in terms of general policy and trends as well as the specific activities for which authorization is requested. As a result, the Committee is able to influence the scope and long-term direction of U.S. intelligence in a manner which improves and strengthens the overall effort. This report covers the Committee's authorization of appropriations for Fiscal Years 1984 and 1985.

THE BUDGET AUTHORIZATION PROCESS

Annually, the Committee conducts a detailed and extensive evaluation of U.S. intelligence activities in the National Foreign Intelligence Program (NFIP). The NFIP includes all intelligence activities designed to serve the foreign intelligence and counterintelligence needs of the policymaking officials of the U.S. government. The Committee's recommendations of the NFIP are incorporated in the annual Intelligence Authorization Bill. In addition, the Committee also reviews intelligence activities funded in the Tactical Intelligence and Related Activities (TIARA) portion of the Department of Defense budget. TIARA programs are designed to meet the needs of military commanders in combat. The Committee recommendations on TIARA are submitted to the Armed Services Committee for its consideration in the Department of Defense Authorization Bill.

The Committee's annual review consisted of a series of hearings with the Director of Central Intelligence, the Deputy Director of Central Intelligence, senior level Department of Defense officials, and each of the principal intelligence program managers. For the FY 1985 Authorization, the Committee also held a hearing with the consumers of intelligence—those senior officials in the U.S. government who actually use the intelligence gathered—to determine how well the intelligence discipline is responding to their needs. In addition, a special budget hearing on intelligence supporting arms control was held.

In addition to the budget hearings, the annual process involved:

Review of 17 volumes of budget justification material which totaled more than 3000 pages of detail;

Review of written responses to several hundred questions for the record;

Special analyses and studies; and

Both formal and informal staff briefings and interviews.

The Committee continued to conduct the budget review process along functional lines which entails examining all programs throughout the Intelligence Community which involve similar missions. For example, the functional areas addressed include: technical and human intelligence collection, analysis and production, foreign counterintelligence, and support activities. This functional approach affords the opportunity to understand and evaluate the relationships, scope, and effectiveness of various organizations involved in the functional missions of U.S. intelligence and thus enables the Committee to identify strengths and weakness. The Committee holds the view that the overall intelligence effort benefits greatly from this evaluation.

The Committee continues to believe that intelligence is the first line of defense and that its continued growth should remain among the nation's highest priorities. The Committee is deeply concerned about potential resource constraints and the lack of forward planning in certain Intelligence Community activities in a future environment which poses more difficult and demanding tasks. The Committee, throughout this reporting period, continued to support major investments needed to respond to challenges U.S. foreign policymakers will face in the late 1980's and 1990's. Additional investment will be required in future years to bring these capabilities on-line as well as initiate new programs required to keep pace with the changing threat to national security. No lessening of tension with our principal adversaries is expected, and the growing threat posed by them to the security of the U.S. and its allies, as well as certain developments in Third World countries, continues to grow in complexity and importance.

In general, the Committee's recommendations for the Fiscal Years 1984 and 1985 Intelligence Authorization included actions to:

Strengthen the Intelligence Community's counterintelligence capablities to deal with a growing foreign intelligence threat;

Improve the quality, timeliness, and scope of intelligence estimates and analyses;

Expand and strengthen human source collection activities while continuing to support technical collection initiatives;

Focus the Intelligence Community's attention on the challenges that lie ahead and ensure adequate investment for the future; and

Lower overall costs of U.S. intelligence by eliminating activities that were found to be unnecessary.

CLASSIFIED BUDGET AUTHORIZATION REPORT

The specific details of the Committee's budgetary recommendations cannot be made public because of the classified nature of intelligence activities. The Committee does, however, prepare a classified report each year which describes in detail the full scope and intent of its recommendations as well as the specific amounts authorized.

Under the provisions of Senate Resolution 400, 94th Congress, the Committee is obligated to ensure that all Members of the Senate are provided the information necessary to make informed judgments on the intelligence budget authorization. Accordingly, each year the Committee makes its classified report available to Members. Copies of the classified report are also provided to the Senate Armed Services Committee, the Senate and House Appropriations Committees, the House Permanent Select Committee on Intelligence, and the President.

STATUTORY AUTHORIZATION

The Intelligence Authorizations enacted into law for Fiscal Years 1984 and 1985 contained a number of important legislative initiatives formulated by the Committee to strengthen intelligence capabilities or help the Intelligence Community resolve problems im-

pacting on intelligence effectiveness. These initiatives are discussed in detail elsewhere in this report.

OTHER ACTIVITIES

During this period, the Committee completed a number of other activities related to the budget including:

Review and approval of requests to reprogram resources;

Review of releases of funds from the CIA's Contingency Reserve;

Actions on supplemental budget requests and budget amendments; and

Periodic on-site review of programs and facilities which are being funded.

JURISDICTION RELATING TO INTELLIGENCE AUTHORIZATION

Past distinctions between so-called "national" and "tactical" intelligence programs are becoming increasingly blurred primarily as a result of advances in both automatic data processing and communications support technology. Intelligence support to DOD operations in Grenada and Lebanon in 1983 clearly demonstrate that both national and tactical intelligence activities must be considered in their totality in crafting effective intelligence support to military operations.

During the 98th Congress, the Committee considered making recommendations to the Senate for certain changes in Senate Resolution 400 which established the Select Committee on Intelligence. The House Permanent Select Committee on Intelligence is assigned authorization responsibility for both national and tactical intelligence activities. In the Senate, under Senate Resolution 400, the Select Committee has authorization responsibility only for national programs. In a letter signed by the Chairman and Vice Chairman on June 5, 1984, the Select Committee recommended to the Armed Services Committee that it consider adoption in the Senate of a procedure under which the Select Committee would authorize both tactical as well as national intelligence programs. The current practice of providing sequential review of the NFIP budget authorization by the Intelligence and Armed Services Committees has served the Senate well and could be adopted as the procedure for TIARA programs.

No action on this recommendation was taken by the Armed Services Committee in the 98th Congress. It is, however, the intention of the Committee to further pursue this matter during the 99th Congress.

LEGISLATION ENACTED IN THE INTELLIGENCE AUTHORIZATION ACTS FOR FISCAL YEARS 1984 AND 1985

The Intelligence Authorization Acts reported from the Select Committee and enacted during the 98th Congress contained a number of important permanent legislative functions.

The Fiscal Year 1984 Authorization Act contained provisions to clarify and expand CIA and DIA administrative authorities, and an amendment to the National Security Act of 1947 dealing with ap-

pointment of a commissioned officer of the Armed Forces as Director of the Intelligence Community Staff.

Explicit authorization for the establishment of age criteria for appointment to operational positions at the Central Intelligence Agency.—Section 401 of the Fiscal Year 1984 Intelligence Authorization Act amended section 5 of the Central Intelligence Agency Act of 1949 to explicitly authorize the CIA to establish age criteria for initial appointments to certain positions. The Committee recognized the CIA's crucial need to attract and retain a core career group of highly motivated individuals capable of being trained in unique skills. The demands of overseas intelligence work require that these individuals have special combinations of age and experience. The stresses and strains of uneven and uncertain hours of work, of duty in unhealthy locations, and of arduous assignments performed under difficult and often dangerous conditions require personnel who possess vigor, vitality, and endurance, as well as emotional maturity. An operational career group with such physical and emotional characteristics is essential to the mission of the Agency.

Unfortunately, there is little indication that the CIA has availed itself of the age criteria authority enacted in the Fiscal Year 1984 Authorization Act, and the Committee notes that the CIA has failed to implement an administrative measure that ostensibly was the key rationale behind the Agency's effort to secure the authority in the first place. Such failures to follow through with measures allegedly dependent upon enactments of new statutory authorities cannot help but make the Committee more skeptical of future legislative proposals of this kind.

Eligibility for incentive awards.—Section 402 of the Fiscal Year 1984 Intelligence Authorization Act extended the authority of the Director of Central Intelligence to pay awards under section 4503 of title 5, United States Code, in recognition of outstanding service, to include within the scope of that authority employees of other government agencies and members of the Armed Forces detailed or assigned to the Central Intelligence Agency or to the Intelligence Community Staff. Under section 4503, an agency head could pay such awards to employees, but it was not clear that this included individuals detailed or assigned to the agency, particularly if they were members of the Armed Forces.

Defense Intelligence Agency benefits and allowances.—Section 501 of the Fiscal Year 1984 Intelligence Authorization Act provided authority to the Director of DIA to provide to military or civilian personnel of the Defense Attache System benefits and allowances comparable to those provided under the Foreign Service Act of 1980 to officers and employees of the State Department stationed abroad. This provision brought the Defense Attache System into line with other intelligence personnel overseas who were eligible for similar allowances and benefits under existing law.

Appointment of a commissioned officer of the Armed Forces as Director of the Intelligence Community Staff.—Section 403 of the Fiscal Year 1984 Intelligence Authorization Act amended section 102 of the National Security Act of 1947 to provide the same treatment (pay, independence from his Service while at IC Staff) for a commissioned officer of the Armed Forces appointed Director of the

Intelligence Community Staff as was already provided under the National Security Act of 1947 for commissioned officers serving as either Director or Deputy Director of Central Intelligence.

The amendment further provided for a commissioned officer serving as Director of the Intelligence Community Staff to be exempt from the limit on the number of commissioned officers of his rank applicable to the Service of which he is a member, except that only one commissioned officer who occupies the position of Director or Deputy Director of Central Intelligence or the position of Director of the Intelligence Community Staff can be exempt from the applicable limit at any one time. This provision was designed to help ensure that the Armed Service from which an officer might be appointed as Director of the Intelligence Community Staff would not by virtue of such appointment by deprived of an authorized senior officer billet necessary for effective military personnel management.

The Fiscal Year 1985 Intelligence Authorization contained additional provisions related to CIA and DIA authorities.

CIA Retirement and Disability System rules and regulations.—Section 302 of the Fiscal Year 1985 Intelligence Authorization Act contained an amendment to the Central Intelligence Agency Retirement Act of 1964 changing a statutory provision requiring approval of the leadership of the House and Senate Armed Services Committees for CIA regulations implementing the CIA Retirement and Disability System. The amendment was necessary because the legislative veto character of the existing law posed a risk to the CIA retirement system and because it was a jurisdictional anomaly. The amendment made by section 302 will protect the past, present, and future rights and benefits of participants in the CIA Retirement and Disability System.

The amendment to the CIA Retirement Act made by section 302 requires reporting of CIA regulations to the Intelligence Committees of the Congress prior to their effective date. This avoids the constitutional infirmity of a legislative veto/approval requirement, while ensuring that the Intelligence Committees have an opportunity to review the CIA regulations and make their views known before the regulations take effect.

Physical security of CIA facilities.—Section 401 of the Fiscal Year 1985 Intelligence Authorization Act added a new section 15 to the Central Intelligence Agency Act of 1949 to provide the effective physicial security of CIA installations within the United States. This new section grants to CIA physical security personnel powers currently exercised by GSA personnel performing physical security duties at CIA facilities, enabling the CIA to assume from the General Services Administration reponsibility for physical security at CIA installations.

The transfer of physical security authority and responsibility from GSA to the CIA would normally have been accomplished simply by GSA delegating its authority to the CIA. The CIA, however, is subject to a unique provision in the National Security Act of 1947 (section 102(d)(3)) which states that the CIA may not have "police, subpoena, law-enforcement powers, or internal-security functions." That provision conceivably could have been construed to prevent CIA security personnel, acting under delegated GSA au-

thority, from detaining trespassers or even arresting terrorists attacking a CIA installation, or from issuing federal parking citations for illegally parked automobiles at CIA Headquarters. To remove any ambiguity which could have arisen concerning the authority of CIA to exercise the powers necessary to perform the physical security functions, it was appropriate to provide a clear legislative grant of these powers to CIA physical security personnel when they are within the boundaries of installations owned, leased, occupied, or otherwise used by the CIA.

The grant of authority contained in the new section 15 of the CIA Act was not meant in any way to detract from the fundamental thrust of the proviso in section 102(d)(3) of the National Security Act of 1947 prohibiting the Agency's exercise of internal security functions. Section 15 of the CIA Act will enable CIA guards to stop, detain, and question persons found on Agency property without reasonable explanation, and to conduct physical searches and make arrests on Agency facilities in appropriate circumstances. But the limited authority conferred by section 15 does not extend beyond Agency facilities, and section 15 does not authorize any expansion of Agency intelligence collection activities that are governed by Executive Order 12333 and related procedures.

Defense Intelligence Agency personnel management improvements.—Section 501 of the Fiscal Year 1985 Intelligence Authorization Act was intended to improve the management of civilian personnel within the Defense Intelligence Agency by amending chapter 83 of title 10, United States Code, to exempt DIA from civil service classification provisions, authorize compensation for DIA civilian personnel, and authorize the Secretary of Defense, during fiscal years 1985 and 1986, to terminate the employment of DIA civilian personnel when he considers such action to be in the interests of the United States and he determines that other relevant provisions of law cannot be invoked in a manner consistent with the national security.

The Defense Intelligence Agency did not have flexibility in personnel matters similar to that available to the CIA and NSA under applicable statutes. As a consequence, DIA had been significantly handicapped in its ability to recruit and reward outstanding analysts and other intelligence specialists and otherwise to operate an equally effective civilian personnel system.

The additions to chapter 83 of title 10 contained in section 501 will enhance DIA's capabilities to attract and retain high quality personnel in competition with other intelligence agencies. Classification authority is granted to permit establishment of compensation based on individual capabilities and to ensure timely assignment and utilization of high quality personnel to meet changing intelligence requirements. DIA also will achieve maximum utilization of authorized manpower through enhanced and simplified authority for termination of employees.

The limited duration of the termination authority was designed to provide the Congress with an opportunity to assess the use made of the authority during a two year period in order that an informed decision can be made as to whether the authority should be made permanent.

VII. Administrative Issues

CONSIDERATION OF FUTURE COMMITTEE MEMBERSHIP IN LIGHT OF THE EIGHT-YEAR LIMITATION ESTABLISHED IN SENATE RESOLUTION 400 (1976)

Senate Resolution 400 (1976), which established the Select Committee on Intelligence, limited Members' tenure on the Committee through section 2(b) to eight years of consecutive service commencing at the beginning of the Ninety-Fifth Congress. It also provided that, to the maximum extent practicable, new Members should be appointed during each Congress to constitute one-third of the Membership of the Committee. Throughout the current Congress, the Chairman, Vice Chairman and Members of the Committee have deliberated over the advisability of implementing this rule at the beginning of the Ninety-Ninth Congress, and several Members have communicated their views through oral comments and letters.

On July 25, 1984, the Committee met to discuss this issue. Thereafter, the Chairman submitted a report to the Senate, which was reprinted in the Congressional Record on September 20, 1984. Copies of the text of this report, which left the issue in abeyance until the next Congress, are available from the Committee.

COMMITTEE FACILITIES AND STAFF

Committee Reporter

In 1983, after consultation with the Senate Leadership, the Select Committee established the staff position of Committee Reporter. This decision was made in light of the highly sensitive nature of the matters within the jurisdiction of the Committee, the need for time-sensitive production of transcripts, and the interest in enhancing overall Committee security. The Committee Reporter provides verbatim transcripts of all Committee meetings, hearings and briefings, as well as on-the-record staff briefings. Having this function performed by a Senate Committee staff member allows the Committee and the Senate to maintain heretofore unavailable levels of control over classified and proprietary information. With the completion of the Committee's secure hearing room, other Senate Committees and the Senate as a whole may use the services of the Committees Reporter and hearing room, affording a higher level of control and security over sensitive information than has been previously available.

New committee staff office and hearing room

From the time of its establishment in 1976 through the Fall of 1983, the Select Committee staff had been temporarily quartered in the auditorium of the Dirksen Senate Office Building. In the Fall of 1983, the Committee staff moved into new permanent offices in the Hart Senate Office Building. This secure office provides ample space and facilities for the conduct of business by Committee staff. In addition, enhanced safeguards are provided for the maintenance of classified information, preparation and production of sensitive materials, secure communication and for control of visitors. Facilities are also available for all Members of the Senate as well as ap-

propriately cleared Senate staff members to review materials in the possession of the Select Committee under the provisions of Senate Resolution 400.

In the Fall of 1984, the Select Committee's hearing room, adjacent to the Committee staff office, was also completed. This hearing room, the most advanced secure hearing room in the Legislative Branch, is available to all Senate Committees when special security precautions are necessary. it also provides a secure area where all Members of the Senate can meet for consideration of classified matters.

With the completion of the hearing room and staff office, the Select Committee will be able to pursue its oversight functions in a physical environment more conducive to the transaction of business concerning the most sensitive intelligence information of the United States Government.

Map Library

As an aid to the Committee and to the Senate, the Committee has begun work on a Map Library. This collection will include geographic, national and urban maps of all areas of the world. The library is being established with the assistance and cooperation of those elements of the Intelligence Community responsible for the production of such materials, and will include both classified and unclassified products. The library will include both maps and source documents. Procedures have been established with the production segments of the Community which will enable the Committee to acquire specialized maps on a timely, as-needed basis.

VIII. Appendix I

NATIONAL POLICY ON TELECOMMUNICATIONS AND AUTOMATED INFORMATION SYSTEMS SECURITY

Recent advances in microelectronics technology have stimulated an unprecedented growth in the supply of telecommunications and information processing services within the government and throughout the private sector. As new technologies have been applied, traditional distinctions between telecommunications and automated information systems have begun to disappear. Although this trend promises greatly improved efficiency and effectiveness, it also poses significant security challenges. Telecommunications and automated information processing systems are highly susceptible to interception, unauthorized electronic access, and related forms of technical exploitation, as well as other dimensions of the hostile intelligence threat. The technology to exploit these electronic systems is widespread and is used extensively by foreign nations and can be employed, as well, by terrorist groups and criminal elements. Government systems as well as those which process the private or proprietary information of US persons and businesses can become targets for foreign exploitation.

Within the government these systems process and communicate classified national security information and other sensitive information concerning the vital interests of the United States. Such information, even if unclassified in isolation, often can reveal highly

classified and other sensitive information when taken in aggregate. The compromise of this information, especially to hostile intelligence services, does serious damage to the United States and its national security interests. A comprehensive and coordinated approach must be taken to protect the government's telecommunications and automated information systems against current and projected threats. This approach must include mechanisms for formulating policy, for overseeing systems security resources programs, and for coordinating and executing technical activities.

This Directive: Provides initial objectives, policies, and an organizational structure to guide the conduct of national activities directed toward safeguarding systems which process or communicate sensitive information from hostile exploitation; establishes a mechanism for policy development; and assigns responsibilities for implementation. It is intended to assure full participation and cooperation among the various existing centers of technical expertise throughout the Executive Branch, to promote a coherent and coordinated defense against the hostile intelligence threat to these systems, and to foster an appropriate partnership between government and the private sector in attaining these goals. This Directive specifically recognizes the special requirements for protection of intelligence sources and methods. It is intended that the mechanisms established by this Directive will initially focus on those automated information systems which are connected to telecommunications transmission systems.

1. *Objectives.*—Security is a vital element of the operational effectiveness of the national security activities of the government and of military combat readiness. Assuring the security of telecommunications and automated information system which process and communicate classified national security information, and other sensitive government national security information, and offering assistance in the protection of certain private sector information are key national responsibilities. I, therefore, direct that the government's capabilities for securing telecommunications and automated information systems against technical exploitation threats be maintained or improved to provide for:

a. A reliable and continuing capability to assess threats and vulnerabilities, and to implement appropriate, effective countermeasures.

b. A superior technical base within the government to achieve this security, and support for a superior technical base within the private sector in areas which complement and enhance government capabilities.

c. A more effective application of government resources and encouragement of private sector security initiatives.

d. Support and enhancement of other policy objectives for national telecommunications and automated information systems.

2. *Policies.*—In support of these objectives, the following policies are established:

a. Systems which generate, store, process, transfer or communicate classified information in electrical form shall be secured by such means as are necessary to prevent compromise or exploitation.

b. Systems handling other sensitive, but unclassified, government or government-derived information, the loss of which could adversely affect the national security interest, shall be protected in proportion to the threat of exploitation and the associated potential damage to the national security.

c. The government shall encourage, advise, and, where appropriate, assist the private sector to: identify systems which handle sensitive non-government information, the loss of which could adversely affect the national security; determine the threat to, and vulnerability of, these systems; and formulate strategies and measures for providing protection in proportion to the threat of exploitation and the associated potential damage. Information and advice from the perspective of the private sector will be sought with respect to implementation of this policy. In cases where implementation of security measures to non-governmental systems would be in the national security interest, the private sector shall be encouraged, advised, and, where appropriate, assisted in undertaking the application of such measures.

d. Efforts and programs begun under PD–24 which support these policies shall be continued.

3. *Implementation.*—This Directive establishes a senior level steering group; an interagency group at the operating level; an executive agent and a national manager to implement these objectives and policies.

4. *Systems Security Steering Group.*—

a. A Systems Security Steering Group consisting of the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, the Attorney General, the Director of the Office of Management and Budget, the Director of Central Intelligence, and chaired by the Assistant to the President for National Security Affairs is established. The Steering Group shall:

(1) Oversee this Directive and ensure its implementation. It shall provide guidance to the Executive Agent and through him to the National Manager with respect to the activities undertaken to implement this Directive.

(2) Monitor the activities of the operating level National Telecommunications and Information Systems Security Committee and provide guidance for its activities in accordance with the objectives and policies contained in this Directive.

(3) Review and evaluate the security status of those telecommunications and automated information systems that handle classified or sensitive government or government-derived information with respect to established objectives and priorities, and report findings and recommendations through the National Security Council to the President.

(4) Review consolidated resources program and budget proposals for telecommunications systems security, including the COMSEC Resources Program, for the US Government and provide recommendations to OMB for the normal budget review process.

(5) Review in aggregate the program and budget proposals for the security of automated information systems of the departments and agencies of the government.

(6) Review and approve matters referred to it by the Executive Agent in fulfilling the responsibilities outlined in paragraph 6 below.

(7) On matters pertaining to the protection of intelligence sources and methods be guided by the policies of the Director of Central Intelligence.

(8) Interact with the Steering Group on National Security Telecommunications to ensure that the objectives and policies of this Directive and NSDD–97, National Security Telecommunications Policy, are addressed in a coordinated manner.

(9) Recommend for Presidential approval additions or revisions to this Directive as national interests may require.

(10) Identify categories of sensitive non-government information, the loss of which could adversely affect the national security interest, and recommend steps to protect such information.

b. The National Manager for Telecommunications and Information Systems Security shall function as executive secretary to the Steering Group.

5. *The National Telecommunications and Information Systems Security Committee.*—

a. The National Telecommunications and Information Systems Security Committee (NTISSC) is established to operate under the direction of the Steering Group to consider technical matters and develop operating policies as necessary to implement the provisions of this Directive. The Committee shall be chaired by the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) and shall be composed of a voting representative of each member of the Steering Group and of each of the following:

The Secretary of Commerce
The Secretary of Transportation
The Secretary of Energy
Chairman, Joint Chiefs of Staff
Administrator, General Services Administration
Director, Federal Bureau of Investigation
Director, Federal Emergency Management Agency
The Chief of Staff, United States Army
The Chief of Staff, United States Air Force
Commandant, United States Marine Corps
Director, Defense Intelligence Agency
Director, National Security Agency
Manager, National Communications System

b. The Committee shall:

(1) Develop such specific operating policies, objectives, and priorities as may be required to implement this Directive.

(2) Provide telecommunication and automated information systems security guidance to the departments and agencies of the government.

(3) Submit annually to the Steering Group an evaluation of the status of national telecommunications and automated information systems security with respect to established objectives and priorities.

(4) Identify systems which handle sensitive, non-government information, the loss and exploitation of which could adversely affect the national security interest, for the purpose of encouraging, ad-

vising and, where appropriate, assisting the private sector in applying security measures.

(5) Approve the release of sensitive systems technical security material, information, and techniques to foreign governments or international organizations with the concurrence of the Director of Central Intelligence for those activities which he manages.

(6) Establish and maintain a national system for promulgating the operating policies, directives, and guidance which may be issued pursuant to this Directive.

(7) Establish permanent and temporary subcommittees as necessary to discharge its responsibilities.

(8) Make recommendations to the Steering Group on Committee membership and establish criteria and procedures for permanent observers from other departments or agencies affected by specific matters under deliberation, who may attend meetings upon invitation of the Chairman.

(9) Interact with the National Communications System Committee of Principals established by Executive Order 12472 to ensure the coordinated execution of assigned responsibilities.

c. The Committee shall have two subcommittees, one focusing on telecommunications security and one focusing on automated information systems security. The two subcommittees shall interact closely and any recommendations concerning implementation of protective measures shall combine and coordinate both areas where appropriate, while considering any differences in the level of maturity of the technologies to support such implementation. However, the level of maturity of one technology shall not impede implementation in other areas which are deemed feasible and important.

d. The Committee shall have a permanent secretariat composed of personnel of the National Security Agency and such other personnel from departments and agencies represented on the Committee as are requested by the Chairman. The National Security Agency shall provide facilities and support as required. Other departments and agencies shall provide facilities and support as requested by the Chairman.

6. *The Executive Agent of the Government for Telecommunications and Information Systems Security.*—The Secretary of Defense is the Executive Agent of the Government for Communications Security under authority of Executive Order 12333. By authority of this Directive he shall serve an expanded role as Executive Agent of the Government for Telecommunications and Automated Information Systems Security and shall be responsible for implementing, under his signature, the policies developed by the NTISSC. In this capacity he shall act in accordance with policies and procedures established by the Steering Group and the NTISSC to:

a. Ensure the development, in conjunction with NTISSC member departments and agencies, of plans and programs to fulfill the objectives of this Directive, including the development of necessary security architectures.

b. Procure for and provide to departments and agencies of the government and, where appropriate, to private institutions (including government contractors) and foreign governments, technical security material, other technical assistance, and other related serv-

ices of common concern, as required to accomplish the objectives of this Directive.

c. Approve and provide minimum security standards and doctrine, consistent with provisions of the Directive.

d. Conduct, approve, or endorse research and development of techniques and equipment for telecommunications and automated information systems security for national security information.

e. Operate, or coordinate the efforts of, government technical centers related to telecommunications and automated information systems security.

f. Review and assess for the Steering Group the proposed telecommunications systems security programs and budgets for the departments and agencies of the government for each fiscal year and recommend alternatives, where appropriate. The views of all affected departments and agencies shall be fully expressed to the Steering Group.

g. Review for the Steering Group the aggregated automated information systems security program and budget recommendations of the departments and agencies of the US Government for each fiscal year.

7. *The National Manager for Telecommunications Security and Automated Information Systems Security.*—The Director, National Security Agency is designated the National Manager for Telecommunications and Automated Information Systems Security and is responsible to the Secretary of Defense as Executive Agent for carrying out the foregoing responsibilities. In fulfilling these responsibilities the National Manager shall have authority in the name of the Executive Agent to:

a. Examine government telecommunications systems and automated information systems and evaluate their vulnerability to hostile interception and exploitation. Any such activities, including those involving monitoring of official telecommunications, shall be conducted in strict compliance with law, Executive Orders and applicable Presidential Directives. No monitoring shall be performed without advising the heads of the agencies, departments, or services concerned.

b. Act as the government focal point for cryptography, telecommunications systems security, and automated information systems security.

c. Conduct, approve, or endorse research and development of techniques and equipment for telecommunications and automated information systems security for national security information.

d. Review and approve all standards, techniques, systems and equipments for telecommunications and automated information systems security.

e. Conduct foreign communications security liaison, including agreements with foreign governments and with international and private organizations for telecommunications and automated information systems security, except for those foreign intelligence relationships conducted for intelligence purposes by the Director of Central Intelligence. Agreements shall be coordinated with affected departments and agencies.

f. Operate such printing and fabrication facilities as may be required to perform critical functions related to the provision of cryptographic and other technical security material or services.

g. Assess the overall security posture and disseminate information on hostile threats to telecommunications and automated information systems security.

h. Operate a central technical center to evaluate and certify the security of telecommunications systems and automated information systems.

i. Prescribe the minimum standards, methods and procedures for protecting cryptographic and other sensitive technical security material, techniques, and information.

j. Review and assess annually the telecommunications systems security programs and budgets of the departments and agencies of the government, and recommend alternatives, where appropriate, for the Executive Agent and the Steering Group.

k. Review annually the aggregated automated information systems security program and budget recommendations of the departments and agencies of the US Government for the Executive Agent and the Steering Group.

l. Request from the heads of departments and agencies such information and technical support as may be needed to discharge the responsibilities assigned herein.

m. Enter into agreements for the procurement of technical security material and other equipment, and their provision to government agencies and, where appropriate, to private organizations, including government contractors, and foreign governments.

8. *The Heads of Federal Departments and Agencies shall:*

a. Be responsible for achieving and maintaining a secure posture for telecommunications and automated information systems within their departments or agencies.

b. Ensure that the policies, standards and doctrine issued pursuant to this Directive are implemented within their departments or agencies.

c. Provide to the Systems Security Steering Group, the NTISSC, Executive Agent, and the National Manager, as appropriate, such information as may be required to discharge responsibilities assigned herein, consistent with relevant law, Executive Order, and Presidential Directives.

9. *Additional Responsibilities.*—

a. The Secretary of Commerce, through the Director, National Bureau of Standards, shall issue for public use such Federal Information Processing Standards for the security of information in automated information systems as the Steering Group may approve. The Manager, National Communications System, through the Administrator, General Services Administration, shall develop and issue for public use such Federal Telecommunications Standards for the security of information in telecommunications systems as the National Manager may approve. Such standards, while legally applicable only to Federal Departments and Agencies, shall be structured to facilitate their adoption as voluntary American National Standards as a means of encouraging their use by the private sector.

b. The Director, Office of Management and Budget, shall:

(1) Specify data to be provided during the annual budget review by the departments and agencies on programs and budgets relating to telecommunications systems security and automated information systems security of the departments and agencies of the government.

(2) Consolidate and provide such data to the National Manager via the Executive Agent.

(3) Review for consistency with this Directive, and amend as appropriate, OMB Circular A-71 (Transmittal Memorandum No. 1), OMB Circular A-76, as amended, and other OMB policies and regulations which may pertain to the subject matter herein.

10. Nothing in this Directive:

a. Alters the existing authorities of the Director of Central Intelligence, including his responsibility to act as Executive Agent of the Government for technical security countermeasures (TSCM).

b. Provides the NTISSC, the Executive Agent, or the National Manager authority to examine the facilities of other departments and agencies without approval of the head of such department or agency, nor to request or collect information concerning their operation for any purpose not provided for herein.

c. Amends or contravenes the provisions of existing law, Executive Orders, or Presidential Directives which pertain to the privacy aspects or financial management of automated information systems or to the administrative requirements for safeguarding such resources against fraud, abuse, and waste.

d. Is intended to establish additional review processes for the procurement of automated information processing systems.

11. For the purposes of this Directive, the following terms shall have the meanings indicated:

a. *Telecommunications* means the preparation, transmission, communication or related processing of information by electrical, electromagnetic, electromechanical, or electro-optical means.

b. *Automated Information Systems* means systems which create, prepare, or manipulate information in electronic form for purposes other than telecommunication, and includes computers, word processing systems, other electronic information handling systems, and associated equipment.

c. *Telecommunications and Automated Information Systems Security* means protection afforded to telecommunications and automated information systems, in order to prevent exploitation through interception, unauthorized electronic access, or related technical intelligence threats, and to ensure authenticity. Such protection results from the application of security measures (including cryptosecurity, transmission security, emission security, and computer security) to systems which generate, store, process, transfer, or communicate information of use to an adversary, and also includes the physical protection of sensitive technical security material and sensitive technical security information.

d. *Technical security material* means equipment, components, devices, and associated documentation or other media which pertain to cryptography, or to the securing of telecommunications and automated information systems.

13. The functions of the Interagency Group for Telecommunications Protection and the National Communications Security Com-

mittee (NCSC) as established under PD-24 are subsumed by the Systems Security Steering Group and the NTISSC, respectively. The policies established under the authority of the Interagency Group or the NCSC, which have not been superseded by this Directive, shall remain in effect until modified or rescinded by the Steering Group or the NTISSC, respectively.

14. Except for ongoing telecommunications protection activities mandated by and pursuant to PD/NSC-24, that Directive is hereby superseded and cancelled.

APPENDIX II

I. SUMMARY OF COMMITTEE ACTIVITIES—JANUARY 1, 1983, TO DECEMBER 31, 1984

A. Total number of meetings, hearings and briefings: 127.

B. Bills and Resolutions: Total 12:

1. S. Con. Res. 28, to support the establishment of a National Historical Intelligence Museum.

2. S. Res. 36, authorizing expenditures by the Select Committee on Intelligence.

3. S. Res. 267, to support the establishment of a National Historical Intelligence Museum.

4. S. Res. 317, authorizing expenditures by the Select Committee on Intelligence.

5. S. 1230, to authorize appropriations for the Fiscal Year 1984 for intelligence activities of the United States Government, the Intelligence Community Staff, the Central Intelligence Agency Retirement and Disability System, and for other purposes.

6. S. 1324, to amend the National Security Act of 1947 to regulate public disclosure of information held by the Central Intelligence Agency.

7. S. 1713, to amend the Intelligence Authorization Act for Fiscal Year 1983 to prohibit United States support for military or paramilitary operations in Nicaragua and to authorize assistance, to be openly provided to governments of countries in Central America, to interdict the supply of military equipment from Nicaragua and Cuba to individuals, groups, organizations, or movements seeking to overthrow governments of countries in Central America.

8. S. 1927, to amend the Intelligence Authorization Act for Fiscal Year 1984 to prohibit United States support for military or paramilitary operations in Nicaragua and to authorize assistance, to be openly provided to governments of countries in Central America, to interdict the supply of military equipment from Nicaragua and Cuba to individuals, groups, organizations, or movements seeking to overthrow governments of countries in Central America.

9. S. 1963, to amend the Intelligence Authorization Act for Fiscal Year 1984 to prohibit United States support for military or paramilitary operations in Nicaragua and to authorize assistance, to be openly provided to governments of countries in Central America, to interdict the supply of military equipment from Nicaragua and Cuba to individuals, groups, organizations, or movements seeking to overthrow governments of countries in Central America.

10. S. 2671, to establish a ten-year term for the position of Director of Central Intelligence and a five-year term for the position of Deputy Director of Central Intelligence.

11. S. 2713, to authorize appropriations for the Fiscal Year 1985 for intelligence activities of the United States Government, the Intelligence Community Staff, the Central Intelligence Agency Retirement and Disability System, and for other purposes.

12. S. 3019, to require that the positions of Director and Deputy Director of Central Intelligence be filled by career intelligence officers.

II. PUBLICATIONS OF THE SELECT COMMITTEE, JANUARY 1, 1983, TO DECEMBER 31, 1984

1. Senate Report 98–10, Report to the Senate covering the period January 1, 1981 to December 31, 1982.

2. Senate Report 98–39, Rules of Procedure for the Select Committee on Intelligence (Committee Print) amended February 28, 1983.

3. Senate Report 98–77 on S. 1230, authorizing appropriations for Fiscal Year 1984 for intelligence activities of the United States Government, the Intelligence Community Staff, the Central Intelligence Agency Retirement and Disability System (CIARDS), and for other purposes.

4. Senate Hearing 98–464, hearings on S. 1324, an amendment to the National Security Act of 1947, June 21, 28, October 4, 1983.

5. Senate Report 98–305 on S. 1324, Intelligence Information Act of 1983

6. Senate Hearing 98–519, hearing on National Historical Intelligence Museum, November 3, 1983.

7. Senate Report 98–481 on S. 2713, authorizing appropriations for Fiscal Year 1985 for intelligence activities of the United States Government, the Intelligence Community Staff, the Central Intelligence Agency Retirement and Disability System (CIARDS), and for other purposes.

8. Senate Report 98–659, Recent Political Violence in El Salvador.

9. Senate Report 98–660, the Foreign Intelligence Surveillance Act of 1978: The First Five Years.

10. Senate Report 98–665, Report to the Senate covering the period January 1, 1983 to December 31, 1984.

○