Union Calendar No. 942

95TH CONGRESS
2d Session
HOUSE OF REPRESENTATIVES
REPORT
No. 95-1795

ANNUAL REPORT

PURSUANT TO SECTION 3 OF HOUSE RESOLUTION 658,
95TH CONGRESS, 1ST SESSION

REPORT

BY THE

PERMANENT SELECT COMMITTEE ON INTELLIGENCE

OCTOBER 14, 1978.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

---

U.S. GOVERNMENT PRINTING OFFICE
39-006 WASHINGTON : 1978

U.S. HOUSE OF REPRESENTATIVES,
PERMANENT SELECT COMMITTEE ON INTELLIGENCE,
Washington, D.C., October 14, 1978.

Hon. THOMAS P. O'NEILL, Jr.,
Speaker of the House,
Washington, D.C.

DEAR MR. SPEAKER: Pursuant to section 3 of House Resolution 658 (95th Cong., 1st sess.), I submit the following report on behalf of the Permanent Select Committee on Intelligence. The report contains an account of the committee's work in overseeing the intelligence and intelligence-related activities of the U.S. Government, as well as the results of its investigation into specific areas of concern detailed in House Resolution 658. The committee intends to submit similar reports periodically to the House on the intelligence and intelligence-related activities of the Government.

With every good wish, I am
Sincerely yours,

EDWARD P. BOLAND,
Chairman.

Enclosure.

REPORT TO THE HOUSE OF REPRESENTATIVES BY THE PERMANENT SELECT COMMITTEE ON INTELLIGENCE

INTRODUCTION

For the past sixteen months, the House of Representatives, through its Permanent Select Committee on Intelligence, has been conducting a thorough, ongoing examination of the intelligence and intelligence-related activities of the United States Government. This marks the first time such a continuous monitoring of intelligence operations has been performed by a full committee of the House. In establishing the Permanent Select Committee, (H. Res. 658, 95th Cong., 1st sess.), the House charged it with responsibility for overseeing and making continuing studies of the intelligence and intelligence-related activities of the government. In addition, the House directed the Select Committee to assure that the Executive and Legislative Branches receive informed and timely intelligence to support them in making sound decisions affecting the security and vital interests of the nation. One of the major functions of the new intelligence committee is to produce annually a budget authorization bill for all the intelligence and intelligence-related activities of the government.

Recognizing the importance of both its oversight and legislative responsibilities and the complex and diverse nature of our intelli-

gence services, the Committee created four subcommittees to reach across and into all aspects of the intellgence agencies. Those subcommittees are:

Program and Budget Authorization
Bill D. Burlison, (Democrat, Missouri), Chairman.
Norman Y. Mineta (Democrat, California).
Edward P. Boland (Democrat, Massachusetts).
J. Kenneth Robinson (Republican, Virginia).

Legislation
Morgan F. Murphy, (Democrat, Illinois), Chairman.
Romano L. Mazzoli (Democrat, Kentucky).
Edward P. Boland (Democrat, Massachusetts).
Robert McClory (Republican, Illinois).

Oversight
Les Aspin, (Democrat, Wisconsin), Chairman
Clement J. Zablocki (Democrat, Wisconsin).
Edward P. Boland (Democrat, Massachusetts).
Bob Wilson (Republican, California).

Evaluation of Performance
Charles Rose, (Democrat, North Carolina), Chairman.
Wyche Fowler, Jr. (Democrat, Georgia).
Edward P. Boland (Democrat, Massachusetts).
John M. Ashbrook (Republican, Ohio).

To support the Committee and its four subcommittees, a small, highly professional staff has been hired. At present, there are fourteen professionals and thirteen support staff. The staff includes people with experience in Congressional oversight, experience within the Executive Branch in evaluating the performance of intelligence activities and experience within the intelligence community as budget analysts and technical experts.

The Select Committee moved quickly to fulfill its mandate. Even before the President submitted his fiscal year 1979 budget to the Congress, the Program and Budget Authorization Subcommittee of the Permanent Select Committee on Intelligence, chaired by Representative Bill D. Burlison (Democrat, Missouri), began a series of informational hearings on the National Foreign Intelligence Program totaling some 32 hours, in order to familiarize the Members in detail with the activities of our nation's most sensitive foreign intelligence and counterintelligence activities. Once the fiscal year 1979 budget arrived on the Hill, the Subcommittee began what turned out to be one of the most thorough examinations ever given the intelligence and intelligence-related budgets. In all, some 55 hours of hearings were held on the fiscal year 1979 budget.

Recognizing that one of its weightiest functions is to ensure that the intelligence components of our government operate within the bounds of our laws, the Oversight Subcommittee, chaired by Representative Les Aspin (Democrat, Wisconsin), in November 1977 initiated a comprehensive series of hearings—many of them open to the public—on the Central Intelligence Agency's relationship with the media. The Oversight Subcommittee has also delved deeply into the CIA's covert activities program and the mechanism whereby Congress is kept in-

formed of such activities. In its examination of covert operations, the Subcommittee inspected several intelligence stations abroad, reviewing their programs closely.

Another key aspect of the Select Committee's responsibilities is to consider all legislation which may impact on the intelligence and intelligence-related activities of the government. This past year saw the introduction, consideration and passage of the Foreign Intelligence Electronic Surveillance Act (H.R. 7308) which established procedures for conducting electronic surveillance inside the United States for the purpose of gathering foreign intelligence. This is the first major piece of legislation to result from the extensive hearings in 1975 and 1976 by the Church and Pike Committees.

The Legislation Subcommittee, chaired by Representative Morgan Murphy (Democrat, Illinois), carried the responsibility for preparing this legislation for consideration by the Committee and the House.

The question of legislative charters for the components of the intelligence community continues to be closely examined by the Committee which recognizes that this would be one of the most significant pieces of legislation ever to affect the intelligence activities of our government.

The full Committee realized from its inception that one of its most difficult tasks would be to assure that the intelligence community provided high quality and timely support to those who need such support. The Evaluation Subcommittee, chaired by Representative Charles Rose (Democrat, North Carolina), has attacked this problem by pursuing a variety of studies focused on key aspects of the intelligence process. A constant thread running through virtually all of the Subcommittee's efforts has been the problems which have arisen from the vast increase in recent years in amounts of data being collected, primarily by highly technical systems. Processing and evaluating this immense flow of data has presented the intelligence community with certain technical difficulties and with even more intransigent managerial problems. The Evaluation Subcommittee has held a series of briefings and hearings on automated data processing and both Members and staff have spent many hours visiting automated data processing facilities and in discussions with managers of such systems in an effort to ensure improved management through more commanality and less duplicative efforts in this field.

The full Committee expressed its concern over these matters in the classified annex to the bill authorizing appropriations for fiscal year 1979 (H.R. 12240; H. Rept. 95–1075, Public Law 95–370). The annex which is incorporated by reference in the statute has the force and effect of law.

The Committee has also interested itself in a wide variety of other issues which impact on the effectiveness of our intelligence services. These issues range from an investigation into the steps the Executive Branch is taking to protect the communications of both private citizens and the government from being intercepted by foreign powers operating within the United States to an examination of the possible adverse impact on the intelligence services of certain provisions of the Civil Service Reform Act. The Committee has been working closely with the Executive Branch in an effort to develop a joint approach to stemming the flood of unauthorized disclosures of classified and sensitive intelligence information. The Committee has also focused its attention on

the problems of foreign terrorism, international narcotics traffic and the entry of known or suspected terrorists and KGB agents into the United States.

That is a brief summary of the major actions taken by the Permanent Select Committee during the past sixteen months. Further details are provided in the body of the report.

COMMITTEE ORGANIZATION

The Committee recognized from the first that in order to do the job the House had given it, an atmosphere of trust had to be develop between the Committee and officials of the intelligence agencies. Without that trust, the Committee realized it would have a virtually impossible task in getting the information it would need.

At the same time, the Committee realized that in order to exercise vigorous oversight over the intelligence activities of the government, there must, of necessity, be an adversarial relationship between the Committee and the intelligence agencies.

One key element of the relationship of trust would be the way the Committee would go about picking a staff; another would be the way the Committee would handle classified information. The Chairman has insisted on a full background investigation by the Federal Bureau of Investigation of each prospective staff member before he grants a TOP SECRET clearance. He has also made certain that each staff member who is granted access to sensitive intelligence information has met requirements comparable to those established by the Director of Central Intelligence for Executive Branch employees' access to such information. In addition, each staff member as a condition of employment must execute an agreement with the Committee not to disclose any classified information acquired while an employee of the Permanent Select Committee on Intelligence except as authorized by the Committee in accordance with clause 7 of House Rule XLVIII (H. Res. 658) and the Committee rules.

As to physical security, the Committee invited the Director of Central Intelligence's Chief of Security to inspect its secure storage facilities and to certify that they meet the Director of Central Intelligence's requirements for the storage of sensitive intelligence material. That certification was acquired.

Thus far, the heads of most intelligence entities have been forthcoming in their dealings with the Committee and they have provided the Committee information that has been requested, although there have been one or two occasions where it required several efforts before the requested information was forthcoming. The Committee will continue to insist that it be given access to all the information which it needs in order to carry out the responsibilities assigned to it by the House of Representatives.

The National Security Council and the White House Staff have taken the position that they will not turn over to the Committee copies of Presidential decision memoranda on intelligence activities although they will allow Committee Members and staff to read such decision memoranda and to make notes on them. The Committee appreciates the offer to allow its Members and staff to read such documents which are key to an understanding of the President's intelli-

gence policies. The Committee believes, however, that it would be more in the spirit of the President's own Executive Order 12036 for such documents to be provided to the Committee for its reference and use.

STUDIES

H. Res. 658 which created the Select Committee also directed it to conduct a study consisting of some eight separate components.

Section 3. (a) of House Resolution 658 states that:

> The Permanent Select Committee on Intelligence shall make a study with respect to the following matters, taking into consideration with respect to each such matter, all relevant aspects of the effectiveness of planning, gathering, use, security, and dissemination of intelligence:
>
> (1) the quality of the analytical capabilities of United States intelligence and intelligence-related activities and means for integrating more closely analytical intelligence and policy formulation;
>
> (2) the extent and nature of the authority of the departments and agencies of the executive branch to engage in intelligence and intelligence-related activities and the desirability of developing charters for each intelligence agency or department;
>
> (3) the organization of intelligence and intelligence-related activities in the executive branch to maximize the effectiveness of the conduct, oversight, and accountability of intelligence and intelligence-related activities; to reduce duplication or overlap; and to improve the morale of the personnel of the intelligence and intelligence-related agencies;
>
> (4) the conduct of covert and clandestine activities and the procedures by which Congress is informed of such activities;
>
> (5) the desirability of changing any law, House rule or procedure, or any Executive order, rule or regulation to improve the protection of intelligence secrets and provide for disclosure of information for which there is no compelling reason for secrecy;
>
> (6) the desirability of establishing a joint committee of the Senate and the House of Representatives on intelligence and intelligence-related activities in lieu of having separate committees in each House of Congress, or of establishing procedures under which separate committees on intelligence and intelligence-related activities of the two Houses of Congress would receive joint briefings from the intelligence and intelligence-related agencies and coordinate their policies with respect to the safeguarding of sensitive intelligence information;
>
> (7) the authorization of funds for the intelligence and intelligence-related activities of the Government and whether disclosure of any of the amounts of such funds is in the public interest; and

(8) the development of a uniform set of definitions for terms to be used in policies or guidelines which may be adopted by the executive or legislative branches to govern, clarify, and strengthen the operation of intelligence and intelligence-related activities.

(b) The Permanent Select Committee on Intelligence shall report the results of the study provided for by this section to the House, together with any recommendations for legislative or other actions as it deems appropriate, not later than the close of the Ninety-fifth Congress.

The following is submitted in response to the above direction.

QUALITY

The Subcommittee on Evaluation, chaired by Representative Charles Rose (Democrat, N.C.), has taken the lead for the full Committee in assessing the quality of the analytic capabilities of our intelligence and intelligence-related activities and in examining means for integrating more closely analytic intelligence and policy formulation. This is an enormous and complex subject and obviously the Committee in its little more than one year in existence has only scratched the surface in reviewing all the analytic capabilities of the government's intelligence activities.

Thus far, the Committee has focused on organizational and management issues as they impact on the efficiency and effectiveness of intelligence to provide support to its users. It has also examined a number of substantive intelligence products such as the National Intelligence Estimates and reviewed reporting on such trouble spots as Somalia/Ethiopia and most recently Nicaragua. While it finds the reporting generally responsive to user requirements, it has also found that there may be considerable room for improvement—especially in such areas as estimating, forecasting and trend analysis reporting. It plans a detailed study of this problem during the coming year.

Having examined the relationship among collection, processing and analysis in selected areas, the Committee notes that the attention of the intelligence community appears to be directed primarily to increasing collection, while other fundamental problems go relatively unattended. These include analytical problems which cannot be attributed to lack of data.

The Subcommittee on Evaluation has, however, examined several topic areas in depth, areas chosen because their scope and impact affect a wide range of intelligence and policy matters.

One such area is called "Warning", i.e., the range of intelligence collection, processing, analysis and reporting of data which is intended to provide our policy makers sufficient lead time before an event occurs to develop our own course of action to either deter, alter or respond to the impending development. The Subcommittee on Evaluation's study of the performance of warning intelligence has examined the warning process in some detail, focusing on lessons learned from past crises such as Pearl Harbor, the Korean War, the Cuba Missile Crisis, the Soviet invasion of Czechoslovakia and the 1973 Mid-East War. One major conclusion of this study is that great improvements have been made in the collection, processing and dissemination of data useful

in the warning process but that improvements in analysis and the integration of analysis with policy formulation have lagged far behind.

By sharing the findings of the Subcommittee with the Executive Branch, and entering into a dialogue on these issues, the Committee has already seen a positive step taken to provide a leadership focus for warning in the intelligence community. This was a direct result of the Committee calling this inadequacy to the attention of the Director of Central Intelligence.

During its inquiries into the quality of intelligence, the Committee has found one continuing and persistently troubling issue wherever it has looked—namely, what is the requirement for any particular intelligence activity? To make a judgment as to whether or not a specific component of the intelligence community is performing its function adequately, it is imperative to know what requirements the user has levied on that component. The Committee has found to be ineffective the efforts of the Executive Branch to identify gaps in, and take steps to satisfy requirements for, collection or analysis.

The Department of Defense has created a new position, that of the Deputy Under Secretary for Policy, who is charged with the validation of intelligence requirements. The Intelligence Community Staff is also studying this problem on behalf of the Director of Central Intelligence. Likewise, the Policy Review Committee of the National Security Council is charged by Executive Order 12036 with establishing "requirements and priorities for national foreign intelligence." The Committee will be looking closely during the coming year at those Executive Branch efforts which attempt to determine requirements and upon which an evaluation of the effectiveness of our intelligence activities can be built.

The Committee also notes that the subject of requirements is an enormously complex one and one which the steps taken to date by the Executive Branch may not resolve. The Committee points, for example, to the fact that the National Security Council's Policy Review Committee is restricted to establishing requirements and priorities for "national" intelligence. Responsibility for assigning priorities among requirements for both tactical military and "national" intelligence apparently has not been assigned to any official or group of officials within the Executive Branch nor is there any provision for the rapid and smooth transition from a peacetime environment to a wartime footing where intelligence requirements and management is concerned. The Committee intends to look deeper into these issues in the coming year.

LEGISLATIVE CHARTERS

A key aspect of the present structure and functioning of the nation's foreign intelligence activities is the fact that only the Central Intelligence Agency of all the elements engaged in foreign intelligence has been created by legislation. The National Security Agency and the Defense Intelligence Agency have been operating for years without legislative charters. Further, the CIA charter consists only of a few paragraphs in the National Security Act of 1947 and a subsequent CIA Act of 1949 which largely addressed itself to administrative details. For the most part, authority for the conduct of foreign intelligence and counterintelligence collection, dissemination, and analysis

is contained in Executive Order 12036 signed by President Carter on January 26, 1978. After its own examination of this issue, the Senate Select Committee on Intelligence found a need for legislation which would authorize the activities of the various intelligence elements of the United States Government and which would restrict or prohibit certain specific activities. To that end, the Senate Select Committee introduced a comprehensive legislative charters bill in 1978 (S. 2525). An identical bill, H.R. 11245, was introduced in the House.

The House Permanent Select Committee on Intelligence believes this subject is important enough to deserve a thorough review. To that end, a thorough staff examination has been scheduled to examine this matter in detail. Additional briefings and a full complement of hearings will be scheduled in the next Congress. Once the Committee has completed its investigations and hearings, it will be able to decide what legislation to recommend to the full House.

IMPROVE MANAGEMENT

Executive Order 12036 attempted to establish effective mechanisms within the Executive Branch for overseeing the intelligence activities of the government by establishing an Intelligence Oversight Board and by assigning specific responsibilities to the Inspectors General of the intelligence agencies. It also acknowledged the role of Congressional oversight committees. In addition, Executive Order 12036 gave greater responsibility and authority to the Director of Central Intelligence for the preparation of the national foreign intelligence budget, thus enabling him better to reduce unnecessary duplication and overlap.

However, modern technology has to a considerable degree blurred the distinction between so-called "national" intelligence and "departmental" or "tactical" intelligence. Thus, by limiting the Director of Central Intelligence's budget authority to "national" programs, a substantial portion of the nation's intelligence activities are not controlled centrally nor is there an adequate mechanism to guard against unnecessary duplication and overlap between those activities controlled by the Director of Central Intelligence and those controlled by the Secretary of Defense. The Committee has made no decision as to the merits of giving the Director of Central Intelligence authority over more than just the "national" programs and notes that in Executive Order 12036 the President excluded the Director of Central Intelligence from exercising any role in the tactical military intelligence area. The Committee believes, however, that this subject merits further examination in connection with consideration of legislative charters for the intelligence agencies.

The Committee examined the management of intelligence and intelligence-related activities during several days of hearings and through an additional in-depth review of management procedures in conjunction with the authorization of the fiscal year 1979 intelligence and intelligence related budget.

In looking at the management of intelligence analysis and production, the Committee devoted its attention to the National Foreign Assessment Center which was established to assist the Director of Central Intelligence in this area. However, no specific process or structure for

achieving increased productivity and improved quality of analysis emerged from this examination.

As noted earlier, the Committee found inadequate management in the area of "warning" intelligence and it called upon the Director of Central Intelligence to create a full-time position with clear responsibility for warning. One of the problem areas involved in the warning process which the Committee identified is less than free exchange of information between intelligence producers and decision or policy makers.

The Committee also uncovered the lack of an effective management mechanism for making certain that there are no unnecessary duplications or overlaps between intelligence collection systems under the control of the Director of Central Intelligence and those of the Secretary of Defense. The Committee has expressed its concern over this management shortcoming and has informed the Secretary of Defense and the Director of Central Intelligence that it expects them to have developed and implemented the necessary mechanisms to evaluate and validate intelligence collection requirements and affect trade-offs between different collection systems by 1979.

The Executive Branch has implemented a set of procedures to govern the application for and approval of so-called "special activities," which the so-called Hughes-Ryan Amendment (22 U.S.C. 2422) defines as Central Intelligence Agency operations in foreign countries, "other than activities intended solely for obtaining necessary intelligence." Under the provisions of Hughes-Ryan, the President must find that each such operation "is important to the national security of the United States" and he must report, "in a timely fashion, a description and scope of such operation to the appropriate committees of the Congress . . ."

As one result of the investigations of the Pike Committee and the Church Committee, the Secretary of Defense has created an Inspector General for Defense Intelligence to oversee the activities of intelligence components of the Defense Department. Also as a result of Congressional and Executive Branch investigations, the Central Intelligence Agency has strengthened its Inspector General's office.

As noted earlier, the Committee found inadequate management in the area of "warning" intelligence and it called upon the Director of Central Intelligence to create a full-time position with clear responsibility for warning. One of the problem areas involved in the warning process which the Committee identified is less than free exchange of information between intelligence producers and decision or policy makers.

The Oversight Subcommittee has found that those in the Executive Branch who have responsibility in the area of intelligence and intelligence-related activities have a much heightened awareness of the need for such activities to be conducted within the law and appropriate Executive Branch regulations. In fact, some testimony asserted that current Executive Branch guidelines were too restrictive and that CIA and FBI operators are being unduly hampered in the performance of their duties. Testimony was also received to indicate that gaps exist in current laws and guidelines which could allow abuses to creep back in a different political climate. The Committee intends to pursue both of these areas in more detail.

In sum, the Executive Branch is much better organized at present than ever before to conduct its own oversight over intelligence and intelligence-related activities. The Congress, however, must continue to bear a considerable burden in this area.

The Committee also recognizes that restrictions imposed by a President can be lifted or ignored by a President. Therefore, the Committee is diligently reviewing legislative restrictions, those proposed by the Senate Select Committee in S. 2525/H.R. 11245, and those proposed in hearings before the House Permanent Select Committee on Intelligence during the 95th Congress. The Committee anticipates that, given the scope and importance of this subject, further hearings and consideration on this subject will be conducted during the 96th Congress.

MORALE

The Committee found that considering the buffeting that the intelligence agencies and their personnel have been through in recent years, morale in general tends to be good. The Committee believes that the morale of intelligence officers generally is reflective of their own appreciation of the worth of their activities and of the general regard in which they are held by the American public. Revelations that some elements of the intelligence community had engaged in illegal activities naturally affected the regard in which the public, the Congress and the media held intelligence professionals as well as the way intelligence officers looked at themselves. Morale was bound to fall in the wake of such revelations and the public attention which was focused on the hitherto secret activities of our intelligence operatives.

The Committee believes that the best remedy will lie in a period of demonstrated highly professional conduct on the part of our intelligence personnel. Only by their actions can confidence in their professionalism be restored. This may take time since as has been noted frequently—their failures are trumpeted but their successes must remain shrouded in secrecy. This Committee is doing its part to ensure that the performance of our intelligence agencies is in accordance with our laws, is highly professional and, is acknowledged publicly as vital to our national interest.

COVERT ACTIONS

When the Central Intelligence Group (the CIA's predecessor) was established in January 1946, its primary mission was to provide President Truman an independent evaluation of the intelligence collected by the various departments of the government. Before the year was out, however, intelligence collection remnants of the World War II Office of Strategic Service (OSS) were added to the Central Intelligence Group. Soon after the Central Intelligence Agency replaced the Central Intelligence Group in 1947, the Office of Policy Coordination was created to direct covert political and paramilitary operations conducted by CIA. The Cold War and the hot Korean War resulted in a major expansion of CIA's "covert action" programs to the point of consuming a significant portion of CIA's budget.

The covert action program remained a major part of CIA's activities throughout the 1950's and 1960's. With the United States withdrawal from Southeast Asia and the opening of the era of detente, plus increasing criticism of such activities from Congress, the covert actions

program declined drastically in the mid-1970's. Concurrent with that decline—and to some extent occasioning it—has been the development and implementation of procedures for the review and approval of covert or "special" activities within the Executive Branch. Since 1974, for example, the so-called Hughes-Ryan amendment (22 U.S.C. 2422) to the Foreign Assistance Act of 1974 established the legislative requirement for a Presidential finding that each covert activity is important to the national security and that each such finding be reported to the appropriate Committees of Congress "in a timely fashion."

The Oversight Subcommittee conducted an extensive and in-depth examination of the covert action program of the Central Intelligence Agency, the authorities for the conduct of such operations, the procedures within the Executive Branch whereby such activities are approved and the process by which Congress is informed of such activities. A detailed classified study on this subject has been produced by the Committee. The House should know that the Committee has registered with the President its critical analysis of several aspects of the current covert action program. As a result, the Attorney General and the Director of Central Intelligence have been engaged in a dialogue with the Committee over this matter.

The Committee found a rather elaborate mechanism within the Executive Branch to review and approve each covert action proposal. At the top of this mechanism is the President who, under the provisions of the Hughes-Ryan Amendment to the Foreign Assistance Act, must find each such operation is important to the national security and he must report a description and scope of each such operation to the appropriate Committees of Congress. Advising the President on this subject is the Special Coordination Committee of the National Security Council, chaired by the Assistant to the President for National Security Affairs with membership consisting of the Secretary of State, the Secretary of Defense, the Attorney General, the Director of the Office of Management and Budget, the Chairman of the Joint Chiefs of Staff and the Director of Central Intelligence.

The Committee is concerned that the cumbersome bureaucratic mechanism developed by the Executive Branch to approve covert action proposals will result either in a failure to take a necessary action in a timely fashion or in efforts to circumvent both those procedures and the Hughes-Ryan Amendment requirements by interpreting the latter too loosely. The Attorney General and the Director of Central Intelligence have assured the Committee of their willingness to work with the Committee to resolve those difficulties.

In essence, the Subcommittee study on Covert Action highlighted the following points. Executive Order 12036 which governs the conduct of United States intelligence activities defines "special activities" or covert actions as those activities:

> . . . conducted abroad in support of national foreign policy objectives which are designed to further official United States programs and policies abroad and which are planned and executed so that the role of the United States Government is not apparent or acknowledged publicly, and functions in support of such activities, but not including diplomatic activity or the collection and production of intelligence or related support functions.

Also, the Committee study notes that while Executive Order 12036 provides that the President can assign covert or "special" activities to an intelligence agency other than the Central Intelligence Agency, the Hughes-Ryan Amendment applies only to the covert activities of the CIA. Thus, in the future, if a President desires not to inform the Congress of a covert operation, he can assign it to an agency other than the CIA.

SECRECY LEGISLATION

One of the most complex and troubling problems affecting the proper functioning of our nation's intelligence services is that of secrecy. On the one hand, our government seems hard pressed to keep a secret, no matter how sensitive or how damaging public disclosure may be to the nation's security. On the other hand, the classification system often seems incapable of discriminating between information which ought to be classified and that which ought to be released to the public.

Legislation in this area is spotty and infrequently used and then only in cases where classified government information is being passed to a foreign government in violation of 18 U.S.C. 793 and 794. However, intelligence agencies are reluctant to see prosecution of cases under the espionage laws where intelligence sources are involved because discovery rights of defendants may require agencies to disclose additional classified material in order to convict someone under those laws. Even under 18 U.S.C. 798, which makes disclosure of classified cryptologic information to unauthorized persons a criminal offense, and which does not require the government to prove the underlying document or information to prove intent to harm the national interest, the government by the very fact of its prosecution must confirm the veracity of the leaked information, i.e., that it was obtained via cryptologic methods. In short, it would have to confirm the leak and thus risk losing the source and—in the case of intercepted foreign diplomatic messages—risk causing an international incident.

Moreover, the current classification system is rooted in an Executive Order (E.O. 12065), not in legislation. Atomic energy information and the above-mentioned cryptology are the only areas specifically protected by legislation.

Committee hearings this year indicate that the present classification system is widely ignored and appears to be held in poor esteem by the very people it seeks to regulate. Executive Order 12065 lists three categories of classification: "Top Secret," which applies to information the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security; "Secret," which refers to information the unauthorized disclosure of which could reasonably be expected to cause serious damage to the national security and "Confidential," which is information which, if disclosed to unauthorized persons, could reasonably be expected to cause identifiable damage to the national security.

One problem seems to be that there is widespread disagreement among those who have been cleared for access to classified information as to whether or not there would indeed be any damage to the national security if certain information were disclosed. In many cases, disrespect for the classification system stems from the fact that senior Administration officials (as in every recent Administration) disclose

classified information whenever they believe such disclosures will help them win a bureaucratic battle within the Administration or a budget battle with Congress.

Disrespect for the classification system has led to the current situation in which many people who have or who have had access to classified information feel no compunction about deciding for themselves what information ought to be disclosed and to whom.

Another aspect of the secrecy issue relates to the nondisclosure agreements which some but not all intelligence agencies require new employees to sign as a condition of employment. It is this type of agreement which allowed the Justice Department to take Frank Snepp to court for publishing his account of the fall of Saigon without submitting it to the CIA for review. The CIA argues that it needs nondisclosure agreements in order to prevent the inadvertent or purposeful disclosure of classified information. Others argue that such agreements amount to a "gag-rule" and infringe upon the right of CIA employees to freedom of speech.

In an effort to bring some order out of this chaos, the Committee will hold a series of hearings in order to assess the present situation and to determine why current laws do not seem to be used. The Committee will attempt to determine if statutes can be written which would both be used and at the same time protect both the constitutional rights of the accused and the need of the government to limit the damage done by the original disclosure. As part of this effort, the Committee is seeking to determine which categories of national security information are so sensitive that they merit being protected by special legislation. Advice will be sought from current and former officials in the White House, the Departments of State and Defense, the present and former Directors of Central Intelligence as well as knowledgeable officials from the Justice Department and other agencies dealing with classified information.

The Committee inquired of the Department of Justice and the Central Intelligence Agency what is being done about the continuing efforts of Philip Agee to publish the identity of CIA clandestine operators. From discussions with representatives of both Justice and CIA, it was apparent that it is very difficult to determine how best to proceed in cases such as that posed by Agee. Moreover, there was no unanimity within the Executive Branch as to whether new legislation is needed in such cases or as to what kind of legislation might be needed. The Committee urged the Executive Branch to do all that it can under existing law to protect our intelligence agents from disclosure and to bring to the Committee any new legislation proposals which it deems necessary in the field of protecting intelligence sources and methods from unauthorized disclosure.

JOINT COMMITTEE ON INTELLIGENCE

The charters of the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence charge the two Committees with very similar tasks in both the oversight and legislative areas. Consequently, there is considerable opportunity for duplication of effort on the part of the two Committees. That may be appropriate when for example, in the annual budget authorization

process, the two Committees take independent looks at the President's budget request for intelligence activities, report separate bills to their respective Houses and then go to conference to resolve any differences.

It can be argued that since each House of Congress has its own responsibilities, each should have its own Committee to oversee the intelligence activities of the Federal government. A counter argument against having two separate intelligence oversight committees is that the probability of leaks of sensitive intelligence information increases in proportion to the number of people who are given access to such information. According to this argument, the chance of leaks, whether inadvertent or purposeful, would be reduced by reducing the number of Members of Congress and staff members having access to sensitive intelligence.

Certain practical problems would face any effort at present to establish a Joint Committee on Intelligence. One major issue would concern the extent of that committee's charter. The House Permanent Select Committee on Intelligence is charged with oversight over and the preparation of annual authorization for the intelligence and intelligence-related activities of the government. Intelligence-related activities are defined by the Secretary of Defense and the Joint Chiefs of Staff as:

> Those activities outside the Consolidated Defense Intelligence Program which:
>
> (a) Respond primarily to operational commanders' tasking for time-sensitive information on foreign entities;
>
> (b) Respond to national intelligence community tasking of systems whose primary mission is support of operating forces;
>
> (c) Train personnel for intelligence duties;
>
> (d) Provide an intelligence reserve; or
>
> (e) Are devoted to research and development of intelligence or related capabilities. Specifically excluded are programs which are so closely integrated with a weapon system that their primary function is to provide immediate use targeting data. Activities included in the intelligence-related category are contained in the regular Department of Defense budget rather than in the National Foreign Intelligence Program budget.

The resolution creating the Senate Select Committee (S. Res. 400), however, does not provide it the same broad authority over intelligence-related activities as does Rule XLVIII of the House. Any effort to establish a joint committee would have to resolve this difference.

As for joint briefings, some progress has been made in this area. On several occasions Members of one Committee have been invited to sit in on briefings arranged by the other. In addition, the two Committees have an agreement on the safeguarding of classified material provided by one Committee to the other.

Some concern, however, has been expressed on the part of the Senate about the implications of House Rule XI which states in part that: "(2) All committee hearings, records, data, charts, and files . . . shall be

the property of the House and all Members of the House shall have access thereto, . . ." That issue would have to be addressed if a joint committee were to be established.

For the immediate future, the Committee believes it best to continue to arrange, where possible, joint briefings with the Senate Select Committee, to exchange with the Senate Select Committee, where appropriate, transcripts of briefings and hearings and Committee studies and reports.

DISCLOSURE OF INTELLIGENCE BUDGET

One question which has vexed the Congress for several years is whether or not it is in the public interest to disclose the total amount of funds appropriated each year for the nation's intelligence activities. The full Committee made an extensive study of this matter, including two days of open hearings. Testifying on this subject were distinguished Members of Congress, former intelligence officials, recognized constitutional scholars, current officials from the Executive Branch and interested citizens from the public sector.

Testimony was received to the effect that the Constitution leaves it up to the Congress to decide what degree of specificity of detail will suffice to satisfy Article I, Section 9 which states that: ". . . a regular statement and account of the receipts and expenditures of all public money shall be published from time to time."

Witnesses also noted that Article I, Section 5, clause 3: "Each house shall keep a journal of the proceedings and from time to time publish the same except such parts as may in their judgment require secrecy" was used early in the Republic to keep certain appropriations secret.

Other witnesses urged the disclosure not only of the total appropriation figure for the National Foreign Intelligence Program but for each component as well, i.e., Central Intelligence Agency, National Security Agency, Defense Intelligence Agency, etc. They argued that the public has a right to know how its money is being spent and they doubted any harm would be done to the national security by such disclosures. Administration witnesses testified that the Administration would not object to the disclosure by Congress of the total budget figure for the entire National Foreign Intelligence Program but they warned that the disclosure of further details could assist foreign intelligence analysts to focus on certain elements of the budget which will disclose the techniques by which the United States intelligence agencies accomplish their missions.

Testimony was also heard that it would be difficult, if not impossible to hold the line at releasing just the total figure for the National Foreign Intelligence Program. Interested parties will want to know more and more details. It was also brought out at the hearings that no other country publicly discloses what it spends on intelligence operations. Reference was also made to the fact that the full House in 1975 rejected by a vote of 267 to 147 publishing the budget of the Central Intelligence Agency.

After considering all the testimony and after reviewing previous debates on this issue in both Houses, the full Committee agreed unanimously that it could find no persuasive reason why disclosure of any or all amounts of the funds authorized for the intelligence and intelligence-related activities of the government would be in the public

interest. Instead, the Committee concluded that disclosure of any such amount of funds would inevitably lead to pressures for the disclosure of additional levels of detail regarding the budgets and activities of our intelligence agencies, information which the Committee believes should remain classified in the interests of the national security.

In its unclassified report to accompany the bill authorizing appropriations for fiscal year 1979 for the intelligence and intelligence-related activities of the United States Government. (H. Rept. No. 95–1075, Part 1), the Committee noted that in making this judgment it fully contemplates that its own continued oversight activities, the drafting of charters legislation for intelligence agencies and the annual budget authorization process will provide ample, needed accountability from intelligence agencies. It further noted that the Committee's reports and recommendations in this area will be made available to the House.

The Committee further expressed its opinion that whether and to what extent budget disclosure is constitutionally mandated is a matter of policy which the Congress is best qualified to judge. Budget disclosure, like any other issue involving the national security, must be considered in the full context of controlling circumstances. The Committee found compelling evidence to convince it that disclosure of budget information as to the intelligence and intelligence-related activities of the government is not justified in the immediate future. However, this is a judgment that the Committee will have to revisit from time to time to determine whether a reassessment of its position is required.

UNIFORM SET OF DEFINITIONS

One of the first problems the Committee faced when it began to study the operations of the intelligence services of our government was understanding the argot used by practitioners of the clandestine arts, particularly their version of bureaucratic acronyms. Thus, Committee Members were beset with briefings replete with references to the NFIP (National Foreign Intelligence Program), GDIP (General Defense Intelligence Program), CCP (Consolidated Cryptologic Program), NFAC (National Foreign Assessment Center), NITC (National Intelligence Tasking Center), COINS (Community Online Intelligence System), FIS (Foreign Instrumentation Signals), ACINT (Acoustic Intelligence), SIGINT (Signals Intelligence), ELINT (Electronic Intelligence) and the like not to mention the plethora of codewords designed to protect intelligence products and systems.

The Committee has been waging a steady campaign against the unnecessary use of acronyms, but victories tend to be few and shortlived. The proliferation of such jargon has reached the stage where even those steeped in the lore of intelligence are having trouble communicating with one another. In an effort to bring some order out of this chaos, if not to restrain the process, the National Foreign Intelligence Board—a group of senior intelligence officers from the various organizations of the intelligence community who act as advisors to the Director of Central Intelligence—compiled the attached Glossary of Intelligence Terms and Definitions. The Committee offers this as a first effort at understanding the acronyms and the definitions of certain terms commonly used by intelligence officers.

AUTHORIZATION OF FUNDS

To effectively conduct oversight of the clandestine activities of the nation's intelligence entities, a congressional committee is greatly aided by having authority over the funds available to those intelligence entities. The House wisely endowed the Permanent Select Committee on Intelligence with the responsibility for considering the annual authorization for appropriation of funds for the intelligence and intelligence-related activities of the government. The latter category is particularly important because, as the Committee discovered, there exists no effective mechanism within the Executive Branch to coordinate and guard against unnecessary duplication of programs by the Director of Central Intelligence on the one hand and the Secretary of Defense on the other.

Several years ago, the House Appropriations Committee became concerned over the fact that a substantial number of intelligence programs were not included in the "National Foreign Intelligence Program" budget submitted by the Administration and defended by the Director of Central Intelligence. Some of the missing items were tactical military intelligence activities, other were so closely related to intelligence that reasonable men could differ as to whether or not they should be counted as intelligence or combat support systems. To give some visibility to these items, a category known as intelligence-related activities was defined by the Secretary of Defense and the Joint Chiefs of Staff. The definition is on pages 18 and 19 of this report.

The Program and Budget Authorization Subcommittee, chaired by Representative Burlison, began hearings on the fiscal year 1979 budget as soon as it was submitted to Congress in January 1978. The Subcommittee conducted what we believe to be the most thorough examination ever given both the national and the intelligence-related budget submits of the President. In all, over 55 hours of testimony was heard on the fiscal year 1979 budget. Witnesses included Admiral Stansfield Turner, the Director of Central Intelligence who presented the national intelligence program budget. That budget encompasses the programs of:

the Central Intelligence Agency;
the National Security Agency;
the Defense Intelligence Agency;
the Offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs;
the Bureau of Intelligence and Research of the Department of State;
the intelligence elements of the military services, the Federal Bureau of Investigation, the Department of the Treasury, the Department of Energy and the Drug Enforcement Administration; and
the staff elements of the Office of the Director of Central Intelligence.

In addition to Admiral Turner, who also defended the budget of the CIA, the Subcommittee heard testimony from the head of each of the components of the National Foreign Intelligence Program, including Vice Admiral B. R. Inman, Director, National Security

Agency; Lieutenant General Eugene F. Tighe, Jr., USAF, Director, Defense Intelligence Agency; Daniel J. Murphy (Admiral, USN Ret.), Deputy Under Secretary of Defense for Policy; Dr. Gerald P. Dinneen, Assistant Secretary of Defense for Communications; Command, Control and Intelligence; Major General Edmund R. Thompson, Assistant Chief of Staff for Intelligence, U.S. Army; Rear Admiral Sumner Shapiro, Director of Naval Intelligence; Major General James L. Brown, Assistant Chief of Staff, Intelligence, USAF; as well as the heads of the reconnaissance programs of the Defense Department; Ambassador William G. Bowdler, Director of the State Department's Bureau of Intelligence and Research; Mr. Thomas Leavitt, Assistant Director, Intelligence Division, Federal Bureau of Investigation; Mr. Donald Moore, Assistant Director, Domestic Security and Terrorism Division, Federal Bureau of Investigation; Mr. Rowland A. Morrow, Director, Defense Investigative Program Office; Dr. Walter McDonald, Principal Deputy Assistant Secretary for International Affairs, Department of Energy; Mr. Richard Davis, Assistant Secretary, Department of the Treasury; and Mr. Peter Bensinger, Administrator, Drug Enforcement Administration.

The Program and Budget Authorization Subcommittee examined each of those programs in considerable detail, focusing particularly on specific issues which consume large portions of the budget or which research and previous briefings had indicated suffered from management problems. In its hearings, the Subcommittee made a special effort to identify the requirements for each intelligence system and activity funded in the budget. The deferral of several proposed new and very expensive systems was recommended by the Subcommittee and approved by both Houses largely due to the failure of Executive Branch witnesses to demonstrate that those systems would fill a needed requirement.

The Subcommittee also directed its attention to the issue of cross-program trade-offs. It found, and the full Committee in its classified report accompanying the budget authorization bill called attention to, the lack of a suitable mechanism within the Executive Branch to make certain that there is no unnecessary duplication between systems funded in the national program and those funded in the intelligence-related category. Consequently, the Subcommittee was forced to make such trade-offs itself based on the testimony and documentary evidence presented to it.

The Subcommittee also found that while the zero base budget concept offers potential for determining the priority in which intelligence programs, systems and components merit funding, the lack of an adequate tie between requirements and resources and the tendency to look at intelligence activities program by program rather than across programs has limited its effectiveness.

As a result of the Subcommittee's work in this area, the full Committee expressed its concern that not enough is being done in the management of the human source intelligence collection programs to determine their cost effectiveness compared to technical collection systems. Nor, is enough being done to determine the degree of interagency coordination and duplication of human source intelligence collection that exists.

The Committee called to the attention of the Executive Branch a series of topics which it requested the Executive Branch to address with the fiscal year 1980 budget submission. Included were:

Assured access to and wartime control of national intelligence collection systems on the part of military commanders.

The degree to which current security restrictions on the availability and use of specially restricted or "compartmented" intelligence deter the full and effective use of national intelligence collection systems in combat.

The effectiveness of current and planned collection and exploitation management systems to support the military commander.

The possibility of joint Department of Defense/National Foreign Intelligence Program funding of projects whose priority does not warrant sole NFIP funding.

Recognizing that in the area of intelligence-related activities, the Permanent Select Committee on Intelligence shares jurisdiction with the House Armed Services Committee, the Subcommittee on Program and Budget Authorization worked closely with Members and staff of that Committee to ensure that no unnecessary duplication is occurring between the program proposed by the Director of Central Intelligence on the one hand and the Secretary of Defense on the other. Both Committees also bent every effort to make certain that any gaps in our requirements for combat support intelligence are filled. Both Committees are concerned over the need for our combat forces to have the best possible battlefield intelligence support.

The budget total authorized by the Permanent Select Committee on Intelligence for the National Foreign Intelligence Program and the total authorized by both the Permanent Select Committee on Intelligence and the Armed Services Committee for intelligence-related activities were close to that requested in his budget by the President. Some deletions were made, however, in programs which did not appear to be fully justified. Additions were made to other programs which the Committee felt had not received adequate priority from the Administration. The House passed H.R. 12240 on July 6, 1978.

After a conference with the Senate Select Committee on Intelligence and after the House and Senate Armed Services conference on intelligence-related activities in which the House Permanent Select Committee on Intelligence conferees participated, both Houses passed H.R. 12240 authorizing appropriations for the intelligence and intelligence-related activities of the government. That marked the first time such an intelligence authorization bill was considered and passed by both Houses. The President signed the bill into law on September 18, 1978.

The Committee is also concerned over the drastic imbalance in the distribution of supergrade positions among the intelligence agencies. The Central Intelligence Agency has by far the most supergrade positions—more than all the other agencies put together. The Committee recognizes that the quality of the performance of an intelligence component cannot be measured solely on the basis of the number of supergrades it has but the potential or lack thereof for promotion does affect the ability of any organization to attract and keep top quality

personnel. Pending further analysis of this situation by the Committee, a ceiling on supergrades was placed by the Committee at the currently authorized levels.

OTHER COMMITTEE ACTIONS

In addition to the eight topics identified for study by H. Res. 658, the Committee addressed a number of other significant issues. In addressing those issues, the Committee has made a conscious effort not to rehash old items which have already been examined in full by other committees. Instead we have concentrated on present problems and those matters which will affect the future activities of our intelligence services.

One such issue is that of terrorism. The Committee has held several hearings on the question of how well our foreign intelligence, counterintelligence and domestic law enforcement agencies work together to thwart the activities of terrorists. The Committee is also investigating the extent, if any, to which recently enacted laws and guidelines issued by the Attorney General may be hampering the effective operation of our nation's counterterrorist services.

The Committee is not yet satisfied that our intelligence services are cooperating as fully as they should in the area of counterterrorism, especially in the exchange of automated data bases. It is far from convinced that the meshing of necessary guidelines and effective operations on the part of our counterterrorism agencies has occurred. It is not certain that obtaining intelligence on terrorist groups has been given a high enough priority. There appears to be a greater focus on managing a terrorist incident once it has occurred than on preventing it from taking place. Consequently, during the coming year, the Committee will continue to devote attention to this problem area.

Another area which is of concern to the Committee is that of our counterintelligence capability. The Committee is concerned that for a variety of reasons, the nation's defenses against penetration by foreign intelligence services may have been lowered well beyond an acceptable level. The Committee has had abundant evidence presented to it regarding the activities of the Soviet KGB within the United States.

For years, the Executive Branch has lacked a coordinating body to ensure that the Federal Bureau of Investigation, the Central Intelligence Agency and the military services cooperate fully in the counterintelligence area. Executive Order 12036, signed by President Carter on January 26, 1978 assigns to the Special Coordination Committee of the National Security Council responsibility for developing policy with respect to the conduct of counterintelligence activities and with resolving interagency differences concerning implementation of counterintelligence policy. The Committee will be watching this new procedure with special interest.

LEGISLATION

The Committee has found that a great many pieces of legislation, although aimed at resolving problems having nothing to do with intelligence, can in fact impact rather dramatically on the intelligence services. For example, legislation regarding a mandatory retirement

age for Federal government employees focused our Committee's attention on the fact that the Central Intelligence Agency has its own retirement and disability system with its own standards separate from the regular Civil Service retirement system. The Committee held an open hearing on the CIA Retirement and Disability System on October 13, 1977 to examine the reasons why CIA needs a separate system and why the CIA should be allowed to retain a mandatory retirement age provision. The Committee was satisfied that CIA continues to require a separate retirement and disability act for a limited number of its employees who are exposed to hazardous conditions in their overseas assignments. Public Law 95–256 passed on April 6, 1978 leaves undisturbed CIA's separate retirement system and a mandatory retirement age.

The House also passed a Civil Service Reform Bill (H.R. 11280) which contains a provision for a Special Counsel of the Merit System Review Board to whom "whistleblowers" within the government can report illegal or improper activities of which they are aware. The Special Counsel was given broad authority to investigate such matters when they are brought to his attention. Representatives from the CIA expressed their concern to the Permanent Select Committee on Intelligence over the security implications of a Special Counsel having the authority to make detailed investigations into the clandestine operations of the Central Intelligence Agency. After consultations with the House Committee on the Post Office and Civil Service, Chairman Boland of the Permanent Select Committee on Intelligence offered an amendment, passed on a voice vote, which provides that whenever the Special Counsel receives reports from "whistleblowers" involving foreign intelligence or counterintelligence information the disclosure of which is specifically prohibited by law or by executive order, or in any case in which the Special Counsel in consultation with appropriate Executive Branch authorities determines that information involved is prohibited from disclosure, the Special Counsel shall transmit such information to the Permanent Select Committee of the House of Representatives and the Select Committee on Intelligence of the Senate. In offering that amendment, Chairman Boland noted that the various intelligence agencies have Inspectors General and that there is a Presidentially created Intelligence Oversight Board, to which the Inspectors General report. In addition, both Houses have oversight committees which have, and ought to exercise, jurisdiction in matters that involve improprieties but which also concern intelligence information.

Acting out of a similar concern to limit the number of people having access to sensitive intelligence information, the Permanent Select Committee on Intelligence has worked with the Committee on Government Operations to amend H.R. 12171 to eliminate the provision that would have allowed the General Accounting Office (GAO)—on its own initiative—to audit the CIA's sensitive contingency fund which is used to support some of its most clandestine operations. This provision was not considered necessary since the Permanent Select Committee on Intelligence through its Program and Budget Authorization

Subcommittee keeps close account of how the CIA expends those funds.

In addition to its work on formal pieces of legislation, the Permanent Select Committee on Intelligence monitors certain executive orders which impact on the intelligence activities of the government. For example, the Committee staff had several meetings with representatives of the Executive Branch regarding draft provisions of Executive Order 12065 which sets forth the criteria for classifying national security information. The Administration does not undertake routinely to seek Committee advice on executive order drafts nor does it commit itself to accepting such advice. Nonetheless, both sides can benefit from informal exchanges of views prior to the formal issuance of such executive orders.

ADMISSION OF CERTAIN EXCLUDABLE ALIENS

Witnesses from the Federal Bureau of Investigation in testimony before the Committee noted that under the provisions of an amendment to the Foreign Relations Authorization Act for fiscal year 1978 (Sec. 112), the Secretary of State was directed to recommend the admission of aliens who are excludable from the United States by reason of their involvement with espionage or terrorist activities unless the Secretary determines that such admission would be contrary to the security interests of the United States and so certifies to the Speaker of the House of Representatives and the chairman of the Committee on Foreign Relations of the Senate. In other words, spies or members of terrorist groups would be allowed to enter the United States unless the Secretary of State sends a certification to the contrary to the Speaker and the chairman of the Senate Foreign Relations Committee.

The House Permanent Select Committee on Intelligence found that as a result of that amendment, the recommendations of the Federal Bureau of Investigation against admitting aliens who pose a threat to the national security were ignored and those aliens were admitted. In 1977, 99 percent of those whom the Federal Bureau of Investigation recommended be denied admission were, in fact, admitted to our country, and during the first part of 1978 100 percent of those aliens the Federal Bureau of Investigation recommended be denied admission because they belong to groups proscribed by law were allowed in.

The Committee is deeply concerned over this seeming insensitivity to the counterintelligence priorities of the nation. Therefore, the Committee included a requirement in H.R. 12240 that the Attorney General notify the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence whenever he notifies the Secretary of State that he knows or has reason to believe that an alien applying for admission to the United States is an excludable alien under the terms of section 212(a) (27), (28), or (29) of the Immigration and Nationality Act (8 U.S.C. 1182(a)) and that alien is subsequently admitted into the United States.

That language was modified in conference with the Senate Select Committee to require a one-time report from the Attorney General to

the select committees on intelligence by October 30, 1979 describing those cases during fiscal year 1979 in which the Director of the Federal Bureau of Investigation has notified the Attorney General that the Director has reason to believe an alien is excludable under the above provisions of the Immigration and Nationality act and that alien is subsequently admitted to the United States.

The Senate and House conferees noted that they hoped this legislation will stress the need to bring about a balanced perspective in the interagency decisionmaking process regarding the Federal Bureau of Investigation's recommendations for visa denials. The bill containing this provision was passed by both Houses and was assigned into law by the President on September 18, 1978.

CIA AND THE MEDIA

One of the most sensitive areas of concern has been the relationship between the Central Intelligence Agency and the news media. In December 1977, the Oversight Subcommittee began a lengthy series of hearings—most of them in public session—on this issue. Chairman Boland of the full Committee opened those hearings by noting that "we are a nation that values a free press above many other highly prized rights." Mr. Boland went on to state that "at the same time it is also appropriate to mention that our national interest, our position as a world power, and indeed our very survival in this nuclear age, make it imperative that our government and our policymakers have the necessary intelligence to enable them to act in an informed fashion for the common good."

Representative Les Aspin (Democrat, Wisconsin), who chaired the Subcommittee's hearings, pointed out that the hearings were designed to try to determine what, if any, is the proper relationship between the media and the Central Intelligence Agency. A wide range of witnesses testified before the Oversight Subcommittee, including former Director of Central Intelligence William E. Colby; Mr. John Maury, former Legislative Counsel to the Director of Central Intelligence; Dr. Ray S. Cline, Executive Director of Studies, The Center for Strategic and International Studies, Georgetown University; Mr. David A. Phillips, Association of Former Intelligence Officers; Mr. Joseph Fromm, Deputy Editor, U.S. News and World Report; Mr. Herman Nickel, Board of Editors, Fortune Magazine, Mr. Ward Just, freelance writer; Mr. Tad Szulc, freelance writer; Ambassador William C. Trucheart; Ambassador L. Dean Brown; Ambassador William Porter; Mr. Morton H. Halperin, Director, Center for National Security Studies; Mr. Stuart Loory, Managing Editor, Chicago Sun-Times; Mr. Clayton Kirkpatrick, Editor, the Chicago Tribune; Mr. Robert Meyers, Publisher, the New Republic; Mr. Eugene Patterson, Editor, St. Petersburg Times; Mr. Gilbert Cranberg, Editor, the Des Moines Register-Tribune; and Admiral Stansfield Turner, Director of Central Intelligence.

The hearings focused on the various types of activities media representatives might become engaged in with the Central Intelligence Agency such as swapping information, getting pre-trip briefings from

Agency employees, post-trip debriefings to the Agency, access by CIA to media files, and a wide range of support activities on behalf of the CIA. The hearings also delved deeply into possible problems of propaganda planted by CIA through media contacts "flowing back" into United States newspapers, television news and the like. The hearings also highlighted efforts both by current Director of Central Intelligence Admiral Turner and his predecessor George Bush to regularize CIA's relations with the media.

Finally, the hearings brought out the fact that the Soviet Union's intelligence arm—the KGB—makes extensive use of domestic and foreign media in order to spread its propaganda throughout the world.

GLOSSARY OF INTELLIGENCE TERMS AND DEFINITIONS PUBLISHED BY THE INTELLIGENCE COMMUNITY STAFF FOR THE DIRECTOR OF CENTRAL INTELLIGENCE WITH ADVICE OF THE NATIONAL FOREIGN INTELLIGENCE BOARD, JUNE 15, 1978

PREFACE

This publication is the product of an interagency working group formed by the National Foreign Intelligence Board in September 1977, and composed of representatives from the organizations which constitute the Intelligence Community.

This publication is designed to be a reference and guidance document for interdepartmental communications and understanding within the Intelligence Community and is a means of fostering communication with other Executive Branch organizations and with the Congress and the Judiciary. The glossary reflects only those intelligence terms commonly used within and definitions commonly accepted by the Community. It does not include organizationally peculiar terms or definitions nor does it include such details as could be addressed only in a classified document.

The value of this document is dependent upon its currency and completeness; thus, it is expected that changes will occur as new terms evolve and as definitions change. Users are encouraged to submit proposed corrections, additions, deletions, or amendments through their Intelligence Community representative to the Executive Secretary, National Foreign Intelligence Board. The interagency working group will support the Executive Secretary and will be responsible for a review of proposed changes, an annual review of the entire document for currency and adequacy, and the submission of recommended changes to the National Foreign Intelligence Board.

Although this document has been designed to enhance the efficiency of communications within the Intelligence Community, it is hoped that it will also contribute to language commonality throughout the intelligence field. In this regard, authors of other intelligence glossaries and of other special-use glossaries which contain intelligence terms are encouraged to consider the terms and definitions contained herein.

The definitions in this glossary may not coincide precisely with definitions used elsewhere for departmental or legal purposes, especially where definitions were devised for the purpose of supporting and clarifying the language of a legal document. However, terms which have been given other definitions have been annotated with a reference to

Appendix B, which contains the term and the definition or definitions and cites the source document. Current publications and documents known to contain intelligence terms and definitions, to include those definitions contained in Appendix B, are listed in the index at Appendix C.

CONTENTS

METHODOLOGY

The definitions in this glossary have been devised by intelligence officers, not by philologists or semanticists. Some definitions, therefore, may have limited applicability outside the Intelligence Community, while other definitions may be restricted to the single use of a word which has intelligence significance; as, for example, in the word "source." Insofar as possible, however, the definitions included here contain a measure of consistency of form, and an attempt has been made to establish relationships among important intelligence words and terms. A basic example exists in the relationships to be found among the terms "information," "intelligence information" and "intelligence." William R. Corson, in his The Armies of Ignorance, observed:

> A word of caution about the term intelligence is in order. Too often it is used synonymously or interchangeably with information. This is inaccurate and quite misleading. Information until and unless it has been analyzed and evaluated remains nothing more than a fact. Information may be interesting, amusing, or hitherto unknown to the person receiving it, but by and in itself it is inappropriate to call it intelligence. The three terms intelligence, intelligence information, and information need to remain distinct. Intelligence by itself refers to the meaning of, or a conclusion about, persons, events, and circumstances which is derived from analysis and/or logic. Intelligence information consists of facts bearing on a previously identified problem or situation, the significance of which has not been completely established. And information is made of raw facts whose relationship to other phenomena has yet to be considered or established. Similarly, the methods involved in acquiring information and/or intelligence information by any means and turning it into intelligence constitute the intelligence process or cycle. The distinctions between these terms are important to remember. . . .

This glossary makes similar distinctions: information is unevaluated material of every description, intelligence information is information of potential intelligence value, and intelligence is the knowledge de-

rived from a cyclical processing of information. The articulation of these differences is fundamental to the repeated use of these terms in defining other terms. One will find, for example, that nuclear intelligence is defined as intelligence derived from the collection and analysis of radiation, etc., whereas communications intelligence is defined as technical and intelligence information derived from the intercept of foreign communications, etc. (not yet analyzed, it is not yet intelligence). Such fine distinctions are expected to contribute to a broader understanding of the common meanings of many such terms.

Arriving at a suitable definition for the word intelligence is a challenge unto inself. In Sherman Kent's Strategic Intelligence for American World Policy, intelligence is characterized as having three definitional subsets: knowledge, organization, and activity. This concept is particularly useful in establishing the fact that intelligence in the current context has multiple meanings.

Intelligence, he says, is the knowledge that our nation must possess regarding other nations in order to assure itself that its interests will not fail because of planning or decisionmaking done in ignorance; and upon which knowledge our national foreign policy is based. Intelligence is also an institution; . . . a physical organization of living people which pursues the special kind of knowledge at issue. And intelligence is the activity which the organization performs: research, analysis, collection, evaluation, study, presentation, and myriad others.

As helpful as they are, Kent's definitions are excessively delimiting for purposes of this glossary. In the sense that intelligence is knowledge, for example, one cannot assume that all intelligence is "our" intelligence. It is necessary, therefore, to fashion the most basic definition possible for the word intelligence in this sense of its meaning, trusting in the utilizer's ability to select a proper modifier to give the word more precise meaning when that is necessary. More definitional flexibility results from such an approach.

But intelligence is more than the knowledge contained in an intelligence product. It encompasses the intelligence organizations and activities that Kent refers to, and other activities—and their resultant products—which are known as counterintelligence. For these reasons, one might be tempted to define intelligence simply as a generic term which encompasses both foreign intelligence and foreign counterintelligence, thence to formulate spearate definitions for each of those terms. One quickly discovers, however, that such a simplistic approach is insufficiently satisfying because it fails to provide for several shades of meaning and subsequent use.

The problem is compounded by the scores of different types of intelligence that are used commonly and which must be broadly understood, and by the variety of headings under which these types of intelligence are classified. Some types of intelligence are source-oriented (such as human intelligence or signals intelligence), some form-oriented (as in raw or unfinished intelligence), some system-oriented (electronic or telemetric), some subject-oriented (medical, economic), some use-oriented (military, tactical), and a probable host of others. But the point to be made here is how essential the basic definition of intelligence is to further understanding of the many, many ways in which it can be used. The definition of intelligence as it appears in this glossary attempts to account for all of the foregoing.

Some types of intelligence

Acoustic(al) Intelligence (ACOUSTINT or ACINT)
Actionable Intelligence
Basic Intelligence
Biographic(al) Intelligence
Cartographic Intelligence
Combat Intelligence
Communications Intelligence (COMINT)
Counterintelligence
Critical Intelligence
Current Intelligence
Department(al) Intelligence
Economic Intelligence
Electro-Optical Intelligence (ELECTRO-OPTINT)
Electronic Intelligence (ELINT)
Energy Intelligence
Estimative Intelligence
Evasion and Escape Intelligence
Finished Intelligence
Foreign Counterintelligence (FCI)
Foreign Instrumentation Signals Intelligence (FISINT)
Foreign Intelligence (FI)
Foreign Materiel (FORMAT) Intelligence
Geographic(al) Intelligence
Human Intelligence (HUMINT)
Imagery Intelligence (IMINT)
Joint Intelligence
Laser Intelligence (LASINT)
Measurement and Signature Intelligence (MASINT)
Medical Intelligence (MEDINT)
Military Intelligence (MI)
National Intelligence
Nuclear Intelligence (NUCINT)
Nuclear Proliferation Intelligence
Operational Intelligence (OPINTEL)
Optical Intelligence (OPTINT)
Photographic Intelligence (PHOTINT)
Political Intelligence
Positive Intelligence
Radar Intelligence (RADINT)
Radiation Intelligence (RINT)
Raw Intelligence
Scientific and Technical (S&T) Intelligence
Signals Intelligence (SIGINT)
Special Intelligence (SI)
Strategic Intelligence
Tactical Intelligence (TACINTEL)
Target Intelligence
Technical Intelligence (TI)
Telemetry Intelligence (TELINT)

The reader will notice frequent cross-referencing between terms and their definitions. In addition to providing an intelligence lexicon, the glossary purports to be tutorial, inasmuch as it is possible, and frequent cross-referencing is a technique employed intentionally to that end.

The term cross-referenced most often is intelligence cycle which, with its separately defined steps, is conceptually fundamental to understanding the vocabulary of intelligence. The definitional technique is to list the steps in the cycle as subsets of it (rather than in their normal alphabetical order in the glossary), and to refer many related terms to the cycle and its various steps. The desired result is to keep the reader's focus on the intelligence cycle in order to maintain the conceptual integrity of its component steps.

The drafters of the definitions contained in this glossary were not constrained by existing definitions or by the narrow meaning of terms where broader significance could be achieved by redefinition. Known definitions were nevertheless accommodated to the greatest extent possible. The primary objective of the drafters was to define those terms that lacked definition and to improve on those definitions extant.

GLOSSARY OF INTELLIGENCE TERMS AND DEFINITIONS

Acoustical intelligence* (ACOUSTINT): Intelligence information derived from analysis of acoustic waves radiated either intentionally or unintentionally by the target into the surrounding medium. (In Naval usage, the acronym ACINT is used and usually refers to intelligence derived specifically from analysis of underwater acoustic waves from ships and submarines.)

Actionable intelligence: Intelligence information that is directly useful to customers without having to go through the full intelligence production process; it may address strategic or tactical needs, close-support of U.S. negotiating teams, or action elements dealing with such matters as international terrorism or narcotics.

Administratively controlled information: Privileged but unclassified material bearing designations such as "For Official Use Only," or "Limited Official Use," to prevent disclosure to unauthorized persons.

Advisory tasking: A non-directive statement of intelligence interest or a request for intelligence information which is usually addressed by an element of the Intelligence Community to departments or agencies having information collection capabilities or intelligence assets not a part of the National Foreign Intelligence Program.

Agent*: A person who engages in clandestine intelligence activity under the direction of an intelligence organization but who is not an officer, employee, or co-opted worker of that organization.

Agent of influence*: A person who is manipulated by an intelligence organization to use his position to influence public opinion or decision-making in a manner which will advance the objective of the country for which that organization operates.

Alert memorandum: A document issued by the Director of Central Intelligence to National Security Council-level policymakers to warn them of possible developments abroad, often of a crisis nature, of major concern to the U.S.; it is coordinated within the Intelligence Community to the extent time permits.

Analysis*: A process in the production step of the intelligence cycle in which intelligence information is subjected to systematic examination in order to identify significant facts and derive conclusions therefrom. (Also see intelligence cycle.)

Assessment*: (1) (General use) Appraisal of the worth of an intelligence activity, source, information, or product in terms of its contribution to a specific goal, or the credibility, reliability, pertinency, accuracy, or usefulness of information in terms of an intelligence need. When used in contrast with evaluation assessment implies a weighing against resource allocation, expenditure, or risk. (See evaluation.) (2) (Production context) See intelligence assessment. (Also see net assessment.)

Asset*: See intelligence asset. (Also see national intelligence asset and tactical intelligence asset.)

Authentication: (1) A communications security measure designed to provide protection against fraudulent transmission and hostile imitative communications deception by establishing the validity of a transmission, message, station, or designator. (2) A means of identifying or verifying the eligibility of a station, originator, or individual

*See Appendix B, Alternate Definitions.

to receive specific categories of information. (Also see communications deception.)

Automatic data processing system security: All of the technological safeguards and managerial procedures established and applied to computer hardware, software, and data in order to ensure the protection of organizational assets and individual privacy; it includes: all hardware/software functions, characteristics, and features; operational procedures, accountability procedures, and access controls at the central computer facility; remote computer and terminal facilities, management constraints, physical structures and devices; and the personnel and communication controls needed to provide an acceptable level of protection for classified material to be contained in the computer system.

Basic intelligence*: Comprises general reference material of a factual nature which results from a collection of encyclopedic information relating to the political, economic, geographic, and military structure, resources, capabilities, and vulnerabilities of foreign nations.

Biographical intelligence: Foreign intelligence on the views, traits, habits, skills, importance, relationships, health, and curriculum vitae of those foreign personalities of actual or potential interest to the United States Government.

Cartographic intelligence: Intelligence primarily manifested in maps and charts of areas outside the United States and its territorial waters.

Case officer*: A professional employee of an intelligence organization who is responsible for providing direction for an agent operation. (See agent.)

Central Intelligence Agency Program (CIAP): See National Foreign Intelligence Program.

Cipher*: A cryptographic system in which the cryptographic treatment (i.e., the method of transforming plain text by predetermined rules to obscure or conceal its meaning) is applied to plain text elements such as letters, digits, polygraphs, or bits which either have no intrinsic meaning or are treated without regard to their meaning in cases where the element is a natural-language word.

Clandestine: Secret or hidden; conducted with secrecy by design.

Clandestine activity: Secret or hidden activity conducted with secrecy by design. (The phrase clandestine operation is preferred. Operations are pre-planned activities.)

Clandestine collection: The acquisition of intelligence information in ways designed to assure the secrecy of the operation.

Clandestine communication: Any type of communication or signal originated in support of clandestine operations. (Also see illicit communication.)

Clandestine operation*: A pre-planned secret intelligence information collection activity or covert political, economic, propaganda, or paramilitary action conducted so as to assure the secrecy of the operation; encompasses both clandestine collection and covert action.

Clandestine Services: That portion of the Central Intelligence Agency (CIA) that engages in clandestine operations; sometimes used as synonymous with the CIA Operations Directorate.

*See Appendix B, Alternate Definitions.

Classification: The determination that official information requires, in the interest of national security, a specific degree of protection against unauthorized disclosure, coupled with a designation signifying that such a determination has been made; the designation is normally termed a security classification. (Also see declassification.)

Classification authority: Those officials within the Executive Branch who have been authorized pursuant to an Executive Order to originally classify information or material.

Classified information*: Official information which has been determined to require, in the interests of national security, protection against unauthorized disclosure and which has been so designated.

Code*: A cryptographic system in which the cryptographic equivalents (usually called code groups), typically consisting of letters or digits (or both) in otherwise meaningless combinations, are substituted for plain text elements such as words, phrases, or sentences.

Code word*: Generally, a word or term which conveys a prearranged meaning other than the conventional one; specifically, a word or term chosen to conceal the identity of a function or action, as distinguished from a cover name which conceals the identity of a person, organization, or installation. (Also see cover.)

Codeword*: Any of a series of designated words or terms used with a security classification to indicate that the material so classified was derived through a sensitive source or method, constitutes a particular type of sensitive compartmented information (SCI), and is therefore accorded limited distribution.

Collateral: All national security information classified under the provisions of an Executive Order for which special Intelligence Community systems of compartmentation (i.e., sensitive compartmented information) are not formally established.

Collection*: See intelligence cycle.

Collection guidance: See guidance.

Collection requirement: An expression of an intelligence information need which requires collection and carries at least an implicit authorization to commit resources in acquiring the needed information. (Also see intelligence requirement.)

Combat information: Unevaluated data, gathered by or provided directly to the tactical commander which, due to its highly perishable nature or the criticality of the situation, cannot be processed into tactical intelligence in time to satisfy the customer's tactical intelligence requirements.

Combat intelligence: That knowledge of the enemy, weather, and geographical features required by a commander in the planning and conduct of combat operations. (Also see tactical intelligence.)

Committee on Exchanges (COMEX): See Director of Central Intelligence Committee. (Also see DCID 2/6.)

Committee on Imagery Requirements and Exploitation (COMIREX): See Director of Central Intelligence Committee. (Also see DCID 1/13.)

Communications cover: See manipulative communications cover.

Communications deception: The deliberate transmission, retransmission, alteration, absorption, or reflection of telecommunications in a

*See Appendix B, Alternate Definitions.

manner intended to cause a misleading interpretation of these telecommunications. It includes:

a. Imitative communications deception—Intrusion into foreign communications channels for the purpose of deception by introducing signals or traffic in imitation of the foreign communications.

b. Manipulative communications deception—The alteration or simulation of friendly telecommunications for the purpose of deception.

Communications intelligence* (COMINT): Technical and intelligence information derived from intercept of foreign communications by other than the intended recipients; it does not include the monitoring of foreign public media or the intercept of communications obtained during the course of counterintelligence investigations within the United States.

Communications security* (COMSEC): The protection resulting from any measures taken to deny unauthorized persons information of value which might be derived from telecommunications, or to ensure the authenticity of such telecommunications.

Communications security signals acquisition and analysis: The acquisition of radio frequency propagation and its subsequent analysis to determine empirically the vulnerability of the transmission media to interception by hostile intelligence services; it includes cataloging the transmission spectrum and taking signal parametric measurements as required but does not include acquisition of information carried on the system; it is one of the techniques of communications security surveillance. (Also see communications security surveillance.)

Communications security surveillance: The systematic examination of telecommunications and automatic data processing systems to determine the adequacy of communications security measures: to identify communications security deficiencies, to provide data from which to predict the effectiveness of proposed communications security measures, and to confirm the adequacy of such measures after implementation.

Community On-Line Intelligence System (COINS): A network of Intelligence Community computer-based information storage and retrieval systems that have been interconnected for interagency sharing of machine formatted files.

Compartmentation*: Formal systems of restricted access to intelligence activities, such systems established by and/or managed under the cognizance of the Director of Central Intelligence to protect the sensitive aspects of sources, methods, and analytical procedures of foreign intelligence programs. (Also see decompartmentation.)

Compromise*: The exposure of classified official information or activities to persons not authorized access thereto; hence, unauthorized disclosure. (Also see classified information.)

Compromising emanations: Unintentional emissions which could disclose information being transmitted, received, or handled by any information-processing equipment.

Computer security*: The computer-driven aspects of automatic data processing system security encompassing the mechanisms and techniques that control access to or use of the computer or information stored in it. (Also see automatic data processing system security.)

*See Appendix B, Alternate Definitions.

Consolidated Cryptologic Program (CCP): See National Foreign Intelligence Program.

Consolidated Intelligence Resources Information System (CIRIS): The automated management information system used to identify and display the expected distribution of all intelligence resources within the National Foreign Intelligence Program.

Consumer*: See customer.

Co-opted worker: A national of a country but not an officer or employee of the country's intelligence service who assists that service on a temporary or regular basis. (In most circumstances a co-opted worker is an official of the country but might also be, for example, a tourist or student.)

Coordination: (1) (In general) The process of seeking concurrence from one or more groups, organizations, or agencies regarding a proposal or an activity for which they share some responsibility, and which may result in contributions, concurrences, or dissents. (2) (In intelligence production) The process by which producers gain the views of other producers on the adequacy of a specific draft assessment, estimate, or report; it is intended to increase a product's factual accuracy, clarify its judgments, resolve disagreement on issues that permit, and sharpen statements of disagreement on, major unresolved issues.

Counterintelligence*: See foreign counterintelligence.

Cover: Protective guise used by a person, organization, or installation to prevent identification with clandestine operations.

Covert: See clandestine.

Covert action: A clandestine operation designed to influence foreign governments, events, organizations, or persons in support of United States foreign policy; it may include political, economic, propaganda, or paramilitary activities. Covert action is referred to in Executive Order No. 12036 as special activities. (See special activities.)

Covert operations: See clandestine operation (preferred term). A covert operation encompasses covert action and clandestine collection.

Critical Collection Problems Committee (CCPC): See Director of Central Intelligence Committee. (Also see DCID 2/2.)

Critical intelligence*: Intelligence information or intelligence of such urgent importance to the security of the United States that it is transmitted at the highest priority to the President and other national decisionmaking officials before passing through regular evaluative channels.

Critical Intelligence Communications System (CRITICOMM): Those communications facilities under the operational and technical control of the Director, National Security Agency which have been allocated for the timely handling of critical intelligence. (Also see critical intelligence.)

Critical intelligence message* (CRITIC): A message designated as containing critical intelligence. (Also see critical intelligence.)

Cryptanalysis (CA): The steps or processes involved in converting encrypted messages into plain text without initial knowledge of the system or key employed in the encryption.

*See Appendix B, Alternate Definitions.

CRYPTO: A designation which is applied to classified, cryptographic information which involves special rules for access and handling. (Also see cryptographic information.)

Cryptographic information: All information significantly descriptive of cryptographic techniques and processes or of cryptographic systems and equipment, or their functions and capabilities, and all cryptomaterial ("significantly descriptive" means that the information could, if made known to unauthorized persons, permit recovery of specific cryptograhpic features of classified crypto-equipment, reveal weaknesses of associated equipment which could allow recovery of plain text or of key, aid materially in the cryptanalysis of a general or specific cryptosystem, or lead to the cryptanalysis of an individual message, command, or authentication). (Also see CRYPTO.)

Cryptographic security: The component of communications security that results from the provision of technically sound cryptographic systems and which provides for their proper use.

Cryptographic system: All associated items of cryptomaterial (e.g., equipment and their removable components which perform cryptographic functions, operating instructions, and maintenance manuals) that are used as a unit to provide a single means of encryption and decryption of plain text so that its meaning may be concealed; also any mechanical or electrical device or method used for the purpose of disguising, authenticating, or concealing the contents, significance, or meanings of communications; short name: cryptosystem.

Cryptography*: The branch of cryptology used to provide a means of encryption and deception of plain text so that its meaning may be concealed.

Cryptologic activities: The activites and operations involved in the production of signals intelligence and the maintenance of signals security.

Cryptology: The science of producing signals intelligence and maintaining signals security. (Also see cryptanalysis and cryptography.)

Cryptomaterial*: All material (including documents, devices, or equipment) that contains cryptographic information and is essential to the encryption, decryption, or authentication of telecommunications.

Cryptosecurity: Shortened form of cryptographic security. See above.

Cryptosystem: Shortened form of cryptographic system. See above.

Current intelligence*: Intelligence of all types and forms of immediate interest to the users of intelligence; it may be disseminated without the delays incident to complete evaluation, interpretation, analysis, or integration.

Customer: An authorized person who uses intelligence or intelligence information either to produce other intelligence or directly in the decisionmaking process; it is synonymous with consumer and user.

Damage assessment: (1) (Intelligence Community context.) An evaluation of the impact of a compromise in terms of loss of intelligence information, sources, or methods, and which may describe and/or recommend measures to minimize damage and prevent future compromises. (2) (Military context.) An appraisal of the effects of an attack on one or more elements of a nation's strength (military,

*See Appendix B, Alternate Definitions.

economic, and political) to determine residual capability for further military action in support of planning for recovery and reconstitution.

DCID ½ Attachment: An annual publication by the Director of Central Intelligence (DCI) which establishes a priorities classification system; it presents requirements categories and foreign countries in a geotopical matrix, against which priorities are assigned which provide the Intelligence Community with basic substantive priorities guidance for the conduct of all U.S. foreign intelligence activities; it includes a system for adjusting priorities between annual publications; priorities are approved by the DCI with the advice of the National Foreign Intelligence Board. (Also see priority.)

Deception: Those measures designed to mislead a foreign power, organization, or person by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests. (Also see communications deception, electronic countermeasures, and manipulative deception.)

Declassification: Removal of official information from the protective status afforded by security classification; it requires a determination that disclosure no longer would be detrimental to national security. (Also see classification.)

Decode: To convert an encoded message into plain text.

Decompartmentation: The removal of information from a compartmentation system without altering the information to conceal sources, methods, or analytical procedures. (Also see compartmentation.)

Decrypt: To transform an encrypted communication into its equivalent plain text.

Decipher: To convert an enciphered communication into its equivalent plain text.

Defector*: A national of a designated country who has escaped from its control or who, being outside its jurisdiction and control, is unwilling to return and who is of special value to another government because he is able to add valuable new or confirmatory intelligence information to existing knowledge about his country. (Also see emigre, refugee, and disaffected person.)

Defense Intelligence Community*: Refers to the Defense Intelligence Agency (DIA), the National Security Agency (NSA) and the Military Services' intelligence offices including Department of Defense (DoD) collectors of specialized intelligence through reconnaissance programs.

Departmental intelligence*: Foreign intelligence produced and within a governmental department or agency in meeting its assigned responsibilities.

Direction finding (DF): A procedure for obtaining bearings of radio frequency emitters with the use of a directional antenna and display unit on an intercept receiver or ancillary equipment.

Director of Central Intelligence (DCI): The President's principal foreign intelligence adviser appointed by him with the consent of the Senate to be the head of the Intelligence Community and Director of the Central Intelligence Agency and to discharge those authorities and responsibilities as they are prescribed by law and by Presidential and National Security Council directives.

*See Appendix B, Alternate Definitions.

Director of Central Intelligence Committee: Any one of several committees established by the Director of Central Intelligence (DCI) to advise him and to perform whatever functions he shall determine; DCI Committees usually deal with Intelligence Community concerns, and their terms of reference ordinarily are specified in DCI Directives; members may be drawn from all components of the Intelligence Community. (Also see Director of Central Intelligence Directive.)

Director of Central Intelligence Directive (DCID): A directive issued by the Director of Central Intelligence which outlines general policies and procedures to be followed by intelligence agencies and organizations which are under his direction or review.

Disaffected person: A person apparently disenchanted with his current situation who may therefore be exploitable for intelligence purposes; e.g., by the willingness to become an agent or defector. (Also see walk-in.)

Disclosure: The authorized release of classified information through approved channels.

Dissemination*: See intelligence cycle.

Domestic collection: The acquisition of foreign intelligence information within the United States from governmental or nongovernmental organizations or individuals who are willing sources and choose to cooperate by sharing such information.

Double agent*: An agent who is cooperating with an intelligence service of one government on behalf of and under the control of an intelligence or security service of another government, and is manipulated by one to the detriment of the other.

Downgrade: To change a security classification from a higher to a lower level.

Economic intelligence*: Foreign intelligence concerning the production, distribution and consumption of goods and services, labor, finance, taxation, and other aspects of the international economic system.

Economic Intelligence Committee (EIC): See Director of Central Intelligence Committee. (Also see DCID 3/1.)

Electro-optical intelligence (ELECTRO-OPTINT): Intelligence information derived from the optical monitoring of the electromagnetic spectrum from ultraviolet (0.01 micrometers) through far (long wavelength) infrared (1,000 micrometers). (Also see optical intelligence.)

Electronic countermeasures (ECM): That division of electronic warfare involving actions taken to prevent or reduce an adversary's effective use of the electromagnetic spectrum. Electronic countermeasures include electronic jamming, which is the deliberate radiation, reradiation, or reflection of electromagnetic energy with the object of impairing the uses of electronic equipment used by an adversary; and electronic deception, which is similar but is intended to mislead an adversary in the interpretation of information received by his electronic system.

Electronic counter-countermeasures (ECCM): The division of electronic warfare involving actions taken to ensure the effective use of

*See Appendix B, Alternate Definitions.

the electromagnetic spectrum despite an adversary's used of electronic countermeasures. (Also see electronic warfare.)

Electronic emission security: Those measures taken to protect all transmissions from interception and electronic analysis.

Electronic intelligence* (ELINT): Technical and intelligence information derived from foreign noncommunications electromagnetic radiations emanating from other than atomic detonation or radioactive sources.

Electronic order of battle* (EOB): A listing of noncommunications electronic devices including site designation, nomenclature, location, site function, and any other pertinent information obtained from any source and which has military significance when related to the devices.

Electronic security* (ELSEC): The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from their intercept and analysis of non-communications electromagnetic radiations; e.g., radar.

Electronic surveillance*: Acquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication or, in the case of a nonelectronic communication, without the consent of a person who is visibly present at the place of communication, but not including the use of radio direction finding equipment solely to determine the location of a transmitter.

Electronic warfare (EW): Military action involving the use of electromagnetic energy to determine, exploit, reduce, or prevent hostile use of the electromagnetic spectrum, and action which retains friendly use of the electromagnetic spectrum. (The three divisions of electronic warfare are: electronic warfare support measures, electronic countermeasures, and electronic counter-countermeasures.)

Electronic warfare support measures (ESM): That division of electronic warfare involving actions to search for, intercept, locate, record, and analyze radiated electromagnetic energy for the purpose of exploiting such radiations in support of military operations; thus, electronic warfare support measures provide a source of electronic warfare information which may be used for immediate action involving conduct of electronic countermeasures, electronic counter-countermeasures, threat detection and avoidance, target acquisition, homing, and other combat support measures.

Emanations security (EMSEC): The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from intercept and analysis of compromising emanations from other than cryptographic equipment and telecommunications systems. (Also see emission security.)

Emigre: A person who departs from his country for any lawful reason with the intention of permanently resettling elsewhere. (Also see refugee and defector.)

Emission security: The component of communications security resulting from all measures taken to deny to unauthorized persons information of value which might be derived from intercept and analysis of compromising emanations from cryptographic equipment and telecommunications systems. (Also see emanations security.)

Encode: To convert plain text into a different form by means of a code.

---

*See Appendix B, Alternate Definitions.

Encipher*: To encrypt plain text by means of a cipher. (Also see cipher.)

Encrypt*: To convert plain text into a different form in order to conceal its meaning.

End product: See finished intelligence. (Also see product.)

Energy intelligence: Intelligence relating to the technical, economic and political capability and programs of foreign countries to engage in development, utilization, and commerce of basic and advanced energy technologies; it includes: the location and extent of foreign energy resources and their allocation; foreign government energy policies, plans, and programs; new and improved foreign energy technologies; and economic and security aspects of foreign energy supply, demand, production distribution, and utilization.

Espionage*: Intelligence activity directed toward the acquisition of information through clandestine means and proscribed by the laws of the country against which it is committed.

Essential elements of information (EEI): Those items of intelligence information essential for timely decisions and for enhancement of operations and which relate to foreign power, forces, targets, or the physical environment.

Estimative intelligence: A category of intelligence which attempts to project probable future foreign courses of action and developments and their implications for U.S. interests; it may or may not be coordinated and may be either national or departmental intelligence.

Evaluation*: Appraisal of the worth of an intelligence activity, information, or product in terms of its contribution to a specific goal; or the credibility, reliability, pertinency, accuracy, or usefulness of information in terms of an intelligence need. Evaluation may be used without reference to cost or risk, particularly when contrasted with assessment. (Also see assessments); it is also a process in the production step of the intelligence cycle. (See intelligence cycle.)

Evasion and escape (E&E): The procedures and operations whereby military personnel and other selected individuals are enabled to emerge from enemy-held or hostile areas to areas under friendly control.

Evasion and escape intelligence: Processed intelligence information prepared to assist personnel to avoid capture if lost in enemy-dominated territory or to escape if captured.

Exploitation*: The process of obtaining intelligence information from any source and taking advantage of it for intelligence purposes. (Also see source.)

Finished intelligence: The result of the production step of the intelligence cycle; the intelligence product. (Also see intelligence cycle and end product.)

Foreign affairs community: Those U.S. Government departments, agencies, and other organizations which are represented in U.S. diplomatic missions abroad, and those which may not be represented abroad but are significantly involved in international activities with the governments of other nations.

Foreign counterintelligence (FCI): Intelligence activity, with its resultant product, intended to detect, counteract, and/or prevent espionage and other clandestine intelligence activities, sabotage, international terrorist activities, or assassinations conducted for or on be-

*See Appendix B, Alternate Definitions.

half of foreign powers, organizations or persons; it does not include personnel, physical, document, or communications security programs.

Foreign instrumentation signals (FIS): Electromagnetic emissions associated with the testing and operational deployment of non-U.S. aerospace, surface, and subsurface systems which may have either military or civilian application; it includes but is not limited to the signals from telemetry, beaconry, electronic interrogators, tracking/fusing/arming/command systems, and video data links.

Foreign instrumentation signals intelligence (FISINT): Technical and intelligence information derived from intercept of foreign instrumentation signals (see above).

Foreign intelligence* (FI): The product resulting from collection, evaluation, analysis, integration, and interpretation of intelligence information about a foreign power and which is significant to the national security, foreign relations, or economic interests of the United States, and which is provided by a government agency that is assigned an intelligence mission (i.e., an intelligence agency). (Also see intelligence cycle.)

Foreign intelligence service: An orgnaization of a foreign government which engages in intelligence activities.

Foreign materiel (FORMAT) intelligence: Intelligence derived from the exploitation of foreign materiel.

Foreign official: A person acting in an official capacity on behalf of a foreign power, attached to a foreign diplomatic establishment or an establishment under the control of a foreign power, or employed by a public international organization.

Forward-looking infrared (FLIR) system: An infrared imaging system which raster scans the scene viewed by internal means, both horizontally and vertically; it can be spaceborne, airborne, seaborne, mounted on a ground vehicle, or placed at a fixed site; and its field of view is determined by the optics used, the scanning mechanism, and the dimensions of the detector array.

Fusion: The blending of intelligence information from multiple sources to produce a single intelligence product.

Fusion center: A term used within the Department of Defense referring to an organization having the responsibility of blending both compartmented intelligence information with all other available information in order to support military operations. (Also see actionable intelligence and tactical intelligence.)

General Defense Intelligence Program (GDIP): See National Foreign Intelligence Program.

Geographic(al) intelligence: Foreign intelligence dealing with the location, description, and analysis of physical and cultural factors of the world, (e.g., terrain, climate, natural resources, transportation, boundaries, population distribution) and their changes through time.

General medical intelligence (GMI): See medical intelligence.

Guidance*: Advice which identifies, interprets, clarifies, and/or expands upon an information need. (Also see information need.)

Human intelligence (HUMINT): A category of intelligence information derived from human sources. (Also see human source reporting and human resources collection.)

* See Appendix B, Alternate Definitions.

Human resources collection: All activities which attend collection of intelligence information from human sources. (See human intelligence and human source.)

Human Resources Committee (HRC): See Director of Central Intelligence Committee. (Also see DCID 1/17.)

Human source: A person who wittingly or unwittingly conveys by any means information of potential intelligence value to an intelligence activity.

Human source reporting: The flow of intelligence information from those who gather it to the customer; it may come from information gathering activities either within or outside the Intelligence Community. (A form of the term is also used to denote an item of information being conveyed, as in human source report). (Also see human intelligence.)

Illegal: An officer or employee of an intelligence organization who is dispatched abroad and who has no overt connection with the intelligence organization with which he is connected or with the government operating that intelligence organization.

Illegal agent: An agent operated by an illegal residency or directly by the headquarters of an intelligence organization. (Also see illegal residency.)

Illegal communication: An electronic communication or signal made without the legal sanction of the nation where it originates.

Illegal residency: An intelligence apparatus established in a foreign country and composed of one or more intelligence officers, and which has no apparent connection with the sponsoring intelligence organization or with the government of the country operating the intelligence organization. (Also see legal residency.)

Illicit communication: An electronic communication or signal originated in support of clandestine operations; it is a type of clandestine communication.

Imagery: Representations of objects reproduced electronically or optical means on film, electronic display devices, or other media.

Imagery intelligence (IMINT): The collected products of imagery interpretation processed for intelligence use. (Also see imagery interpretation below.)

Imagery interpretation (II): The process of locating, recognizing, identifying, and describing objects, activities, and terrain represented in imagery; it includes photographic interpretation.

Imitative communications deception: See communications deception.

Imitative deception: The introduction into foreign channels of electromagnetic radiations which imitate his own emissions.

Indications and warning (I&W): Those intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that could involve a threat to U.S. or allied military, political, or economic interests, or to U.S. citizens abroad. It encompasses forewarning of: enemy hostile actions or intentions; the imminence of hostilities; serious insurgency; nuclear/nonnuclear attack on the U.S., its overseas forces, or allied nations; hostile reactions to U.S. reconnaissance activities, terrorist attacks; and other similar events.

Information: Unevaluated material of every description, at all levels of reliability, and from any source which may contain intelligence information. (Also see intelligence information.)

See Appendix B, Alternate Definitions.

Information handling: Management of data or information which may occur in connection with any step in the intelligence cycle; such management may involve activities to transform, manipulate, index, code, categorize, store, select, retrieve, associate or display intelligence materials; it may involve the use of printing, photographic, computer or communications equipment, systems or networks; it may include software programs to operate computers and process data and/or information; and may include information contained in reports, files, data bases, reference services and libraries.

Information security: Safeguarding knowledge against unauthorized disclosure; or, the result of any system of administrative policies and procedures of identifying, controlling, and protecting from unauthorized disclosure or release to the public, information the protection of which is authorized by executive order or statute.

Information need: The requirement of an official involved in the policymaking process or the intelligence production process for the best available information and intelligence on which to base policy decisions, recommendations, or intelligence production.

Infrared imagery: A likeness or impression produced as a result of sensing electromagnetic radiations emitted or reflected from a given target surface in the infrared portion of the electromagnetic spectrum.

Integration*: A process in the production step of the intelligence cycle in which a pattern is formed through the selection and combination of evaluated intelligence information. (Also see intelligence cycle.)

Intelligence*: (1) A body of evidence and the conclusions drawn therefrom which is acquired and furnished in response to the known or perceived requirements of customers; it is often derived from information which is concealed or not intended to be available for use by the acquirer; it is the product of a cyclical process. (Also see intelligence cycle.)

Examples:

Policy development requires good intelligence.

Timely intelligence is important to informed decisionmaking.

(2) A term used to refer collectively to the functions, activities, organizations which are involved in the process of planning, gathering, and analyzing information of potential value to decisionmakers and to the production of intelligence as defined in (1) above. (Also see foreign intelligence and foreign counterintelligence.)

Examples:

Human source collection is an important intelligence activity of the Central Intelligence Agency.

Intelligence is a demanding profession.

Intelligence activity(ies)*: A generic term used to encompass any or all of the efforts and endeavors undertaken by intelligence organizations. (Also see intelligence organization.)

Intelligence agency: A component organization of the Intelligence Community. (Also see Intelligence Community.)

Intelligence assessment: A category of intelligence production that encompasses most analytical studies dealing with subjects of political significance; it is thorough in its treatment of subject matter—as distinct from building-block papers, research projects, and reference

*See Appendix B, Alternate Definitions.

aids—but unlike estimative intelligence need not attempt to project future developments and their implications; it is usually coordinated within the producing organization but may not be coordinated with other intelligence agencies. (Also see estimative intelligence).

Intelligence asset: Any resource—person, group, instrument, installation, or technical system—at the disposal of an intelligence organization.

Intelligence collector: A phrase sometimes used to refer to an organization or agency that engages in the collection step of the intelligence cycle. (Also see intelligence cycle.)

Intelligence Community (IC): A term which, in the aggregate, refers to the following Executive Branch organizations and activities: the Central Intelligence Agency (CIA); the National Security Agency (NSA); the Defense Intelligence Agency (DIA); offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs; the Bureau of Intelligence and Research (INR) of the Department of State; intelligence elements of the military services; intelligence elements of the Federal Bureau of Investigation (FBI); intelligence elements of the Department of Treasury; intelligence elements of the Department of Energy; intelligence elements of the Drug Enforcement Administration; and staff elements of the Office of the Director of Central Intelligence.

Intelligence Community Staff (IC Staff): A term referring to an organization under the direction and control of the Director of Central Intelligence (DCI) formed to assist the DCI in discharging his responsibilities relating to the Intelligence Community.

Intelligence consumer: See customer.

Intelligence cycle*: The processes by which information is acquired and converted into intelligence and made available to customers. There are usually five steps in the cycle:

a. Planning and direction—determination of intelligence requirements, preparation of a collection plan, issuance of orders and requests to information collection entities, and a continuous check on the productivity of collection entities.

b. Collection*—acquisition of information or intelligence information and the provision of this to processing and/or production elements.

c. Processing*—conversion of collected information and/or intelligence information into a form more suitable for the production of intelligence.

d. Production*—conversion of information or intelligence information into finished intelligence through the integration, analysis, evaluation, and/or interpretation of all available data and the preparation of intelligence products in support of known or anticipated customer requirements.

e. Dissemination*—conveyance of intelligence in suitable form to customers.

Intelligence estimate*: The product of estimative intelligence.

Intelligence information*: Information of potential intelligence value concerning the capabilities, intentions, and activities of any foreign power, organization, or associated personnel.

*See Appendix B, Alternate Definitions.

Intelligence Information Handling Committee (IHC): See Director of Central Intelligence Committee. (Also see DCID 1/4.)

Intelligence information report: A product of the collection step of the intelligence cycle. (Also see intelligence report.)

Intelligence officer: A professional employee of an intelligence organization who is engaged in intelligence activities.

Intelligence organization: A generic term used to refer to any organization engaged in intelligence activities; it may include either an intelligence agency or a foreign intelligence service, or both. (Also see intelligence agency and foreign intelligence service.)

Intelligence Oversight Board (IOB): A body formed by appointment of the President to provide him and the Attorney General with reports and advice on the legality and propriety of intelligence activities; membership and duties are expressed in Executive Order No. 12036.

Intelligence producer: A phrase usually used to refer to an organization or agency that participates in the production step of the intelligence cycle. (Also see intelligence cycle.)

Intelligence related activities (IRA): Those activities specifically excluded from the National Foreign Intelligence Program which: respond to departmental or agency tasking for time-sensitive information on foreign activities, respond to national Intelligence Community advisory tasking of collection capabilities which have a primary mission of supporting departmental or agency missions or operational forces, of training personnel for intelligence duties, or are devoted to research and development for intelligence and related capabilities.

Intelligence report*: A product of the production step of the intelligence cycle. (Also see intelligence information report.)

Intelligence requirement*: Any subject, general or specific, upon which there is a need for the collection of intelligence information or the production of intelligence. (Also see collection requirement.)

Intelligence Research and Development Council (IR&DC): See Director of Central Intelligence Committee. (Also see DCID 1/12.)

Intelligence user: See customer.

Interagency Defector Committee (IDC): See Director of Central Intelligence Committee. (Also see DCID 4/1.)

Interagency intelligence memorandum (IIM): A national intelligence assessment or estimate issued by the Director of Central Intelligence with the advice of appropriate National Foreign Intelligence Board components.

Intercept(ion)*: Acquisition for intelligence purposes of electromagnetic signals (such as radio communications) by electronic collection equipment without the consent of the signallers.

Intercept station: A station which intercepts communications or non-communications transmissions for intelligence purposes.

International lines of communications (ILC): Those communications services which are under the supervision of the International Telecommunication Union and which carry paid public communications traffic between different countries; also known as: International Civil Communications, International Commercial Communications, Internationally-Leased Communications, International Service of Public Correspondence, and commercial communications.

*See Appendix B, Alternate Definitions.

International terrorist activity*: The calculated use of violence, or the threat of violence, to attain political goals through fear, intimidation or coercion; usually involves a criminal act, often symbolic in nature, and is intended to influence an audience beyond the immediate victims. International terrorism transcends national boundaries in the carrying out of the act, the purpose of the act, the nationalities of the victims, or the resolution of the incident; such an act is usually designed to attract wide publicity in order to focus attention on the existence, cause, or demands of the perpetrators.

Interpretation: A process in the production step of the intelligence cycle in which the significance of information or intelligence information is weighed relative to the available body of knowledge. Also see intelligence cycle.)

Joint Atomic Energy Intelligence Committee (JAEIC): See Director of Central Intelligence Committee. (Also see DCID 3/3.)

Joint intelligence: (1) (Military context.) Intelligence produced by elements of more than one military service of the same nation. (2) (Intelligence Community context.) Intelligence produced by intelligence organizations of more than one country.

Laser intelligence (LASINT): Technical and intelligence information derived from laser systems; it is a subcategory of electro-optical intelligence. (See electro-optical intelligence.)

Legal residency: An intelligence apparatus in a foreign country and composed of intelligence officers assigned as overt representatives of their government but not necessarily identified as intelligence officers. (Also see illegal residency.)

Manipulative communications cover: Those measures taken to alter or conceal the characteristics of communications so as to deny to any enemy or potential enemy the means to identify them. Also known as communications cover.

Manipulative communications deception: See communications deception.

Manipulative deception: The alteration or simulation of friendly electromagnetic radiations to accomplish deception.

Measurement and signature intelligence* (MASINT): Scientific and technical intelligence information obtained by quantitative and qualitative analysis of data (metric, angle, spatial, wavelength, time dependence, modulation, plasma, and hydromagnetic) derived from specific technical sensors for the purpose of identifying any distinctive features associated with the source, emitter, or sender and to facilitate subsequent identification and/or measurement of the same.

Medical intelligence* (MEDINT): Foreign intelligence related to all aspects of foreign natural and man-made environments which could influence the health of military forces; it incorporates general medical intelligence which is concerned with foreign biological medical capabilities and health situations, and medical scientific and technical intelligence which assesses and predicts technological advances of medical significance, to include defense against Chemical, Biological, Radiological Warfare; it applies to both tactical and strategic planning and operations, including military and humanitarian efforts. (Also see biographical intelligence.)

*See Appendix B, Alternate Definitions.

Military intelligence (MI): Basic, current, or estimative intelligence on any foreign military or military-related situation or activity.

Monitor: To observe, listen to, intercept, record, or transcribe any form of communication or media for collection of intelligence information or communications security purposes, either overtly or covertly.

Multi-level security: (For automatic data processing (ADP) systems.) Provisions for the safeguarding of all information within a multilevel information handling system. The multilevel information handling system permits various levels, categories, and/or compartments of material to be concurrently stored and processed in a remotely-accessed resource-sharing ADP system, while simultaneously permitting material to be selectively accessed and manipulated from variously controlled terminals by personnel having different security clearances and access approvals. Security measures are therefore aimed at ensuring proper matches between information security and personnel security. (Also see uni-level security.)

National estimate: See national intelligence estimate.

National Foreign Assessment Center (NFAC): An organization established by and under the control and supervision of the Director of Central Intelligence, which is responsible for production of national intelligence.

National Foreign Intelligence Board (NFIB): A body formed to provide the Director of Central Intelligence (DCI) with advice concerning: production, review, and coordination of national foreign intelligence; the National Foreign Intelligence Program budget; interagency exchanges of foreign intelligence information; arrangements with foreign governments on intelligence matters; the protection of intelligence sources or methods; activities of common concern; and such other matters as are referred to it by the DCI. It is composed of the DCI (chairman), and other appropriate officers of the Central Intelligence Agency, the Office of the DCI, Department of State, Department of Defense, Department of Justice, Department of the Treasury, Department of Energy, the offices within the Department of Defense for reconnaissance programs, the Defense Intelligence Agency, the National Security Agency, and the Federal Bureau of Investigation; senior intelligence officers of the Army, Navy, and Air Force participate as observers; a representative of the Assistant to the President for National Security Affairs may also attend meetings as an observer.

National Foreign Intelligence Program (NFIP): Includes the programs listed below, but its composition shall be subject to review by the National Security Council and modification by the President.

(a) The programs of the Central Intelligence Agency;

(b) The Consolidated Cryptologic Program, the General Defense Intelligence Program, and the programs of the offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance except such elements as the Director of Central Intelligence and the Secretary of Defense agree should be excluded;

(c) Other programs of agencies within the Intelligence Community designated jointly by the Director of Central Intelligence and the head of the department or by the President as national foreign intelligence or counterintelligence activities:

(d) Activities of the staff elements of the Office of the Director of Central Intelligence.

(e) Activities to acquire the intelligence required for the planning and conduct of tactical operations by the United States military forces are not included in the National Foreign Intelligence Program.

National intelligence*: Foreign intelligence produced under the aegis of the Director of Central Intelligence and intended primarily to be responsive to the needs of the President, the National Security Council, and other Federal officials involved in the formulation and execution of national security, foreign political, and/or economic policy.

National intelligence asset: An intelligence asset funded in the National Foreign Intelligence Program, the primary purpose of which is the collection or processing of intelligence information or the production of national intelligence. (Also see intelligence asset and national intelligence.)

National Intelligence Estimate* (NIE): A thorough assessment of a situation in the foreign environment which is relevant to the formulation of foreign, economic, and national security policy, and which projects probable future courses of action and developments; it is structured to illuminate differences of view within the Intelligence Community; it is issued by the Director of Central Intelligence with the advice of the National Foreign Intelligence Board. (Also see Special National Intelligence Estimate.)

National Intelligence Officer (NIO): The senior staff officer of the Director of Central Intelligence (DCI) and the DCI's Deputy for National Intelligence for an assigned area of substantive responsibility; he manages estimative and interagency intelligence production on behalf of the DCI; he is the principal point of contact between the DCI and intelligence consumers below the cabinet level; he is charged with monitoring and coordinating that portion of the National Foreign Assessment Center's production that involves more than one office or that is interdisciplinary in character; and is a primary source of national-level substantive guidance to Intelligence Community planners, collectors, and resource managers.

National Intelligence Tasking Center (NITC): The central organizational mechanism established under the direction, control and management of the Director of Central Intelligence for coordinating and tasking national foreign intelligence collection activities, and for providing advisory tasking to other intelligence and information gathering activities.

National security: The territorial integrity, sovereignty, and international freedom of action of the United States. (Intelligence activities relating to national security encompass all the military, economic, political, scientific and technological, and other aspects of foreign developments which pose actual or potential threats to U.S. national interests.)

National/tactical interface: A relationship between national and tactical intelligence activities encompassing the full range of fiscal, technical, operational, and programmatic matters.

Near-real-time: The brief interval between the collection of information regarding an event and reception of the data at some other

*See Appendix B, Alternate Definitions.

location, caused by the time required for processing, communications, and display.

Net assessment: A comparative review and analysis of opposing national strengths, capabilities, vulnerabilities, and weaknesses. (An intelligence net assessment involves only foreign countries.)

Nuclear intelligence (NUCINT): Intelligence derived from the collection and analysis of radiation and other effects resulting from radioactive sources.

Nuclear proliferation intelligence: Foreign intelligence relating to (1) scientific, technical, and economic capabilities and programs and the political plans and intentions of nonnuclear weapons states or foreign organizations to acquire nuclear weapons and/or to acquire the requisite special nuclear materials and to carry on research, development, and manufacture of nuclear explosive devices, and; (2) the attitudes, policies, and actions of foreign nuclear supplier countries or organizations within these countries toward provision of technologies, facilities, or special nuclear materials which could assist nonnuclear weapon states or foreign organizations to acquire or develop nuclear explosive devices.

Official: See foreign official.

Official information: Information which is subject to the control of the United States Government.

Open source information: A generic term describing information of potential intelligence value (i.e., intelligence information) which is available to the general public.

Operational control (OPCON): (military context) The authority delegated to a commander to direct forces assigned so that the commander may accomplish specific missions or tasks which are usually limited by function, time, or location; to deploy the forces concerned; and to retain or assign tactical control of those forces. (It does not, of itself, include administrative or logistic control.)

Operational intelligence* (OPINTEL): Intelligence required for planning and executing operations.

Operations security (OPSEC): Those measures designed to protect information concerning planned, ongoing, and completed operations against unauthorized disclosure.

Optical intelligence (OPTINT): That portion of electro-optical intelligence that deals with visible light. (Also see electro-optical intelligence.)

Order of battle (OB): Intelligence pertaining to identification, strength, command structure, and disposition of the personnel, units, and equipment of any foreign military force. (Also see technical intelligence.)

Overt: Open; done without attempt at concealment.

Overt collection: The acquisition of intelligence information from public media, observation, government-to-government dialogue, elicitation, and from the sharing of data openly acquired. the process may be classified or unclassified; the target and host governments as well as the sources involved normally are aware of the general collection activity although the specific acquisition, sites, and processes may be successfully concealed.

Penetration: (1) (clandestine operations.) The recruitment of agents within or the infiltration of agents or introduction of technical

*See Appendix B, Alternate Definitions.

monitoring devices into an organization or group or physical facility for the purpose of acquiring information or influencing its activities (2) (automatic data processing (ADP) operations.) The unauthorized extraction and identification of recognizable information from a protected ADP system.

Personnel security: The means or procedures—such as selective investigations, record checks, personal interviews, and supervisory controls—designed to provide reasonable assurance that persons being considered for or granted access to classified information are loyal and trustworthy.

Photographic intelligence (PHOTINT): The collected products of photographic interpretation classified and evaluated for intelligence use; it is a category of imagery intelligence.

Photographic interpretation (PI): The process of locating, recognizing, identifying, and describing objects, activities, and terrain represented on photography; it is a category of imagery interpretation.

Physical security*: Physical measures—such as safes, vaults, perimeter barriers, guard systems, alarms and access controls—designed to safeguard installations against damage, disruption or unauthorized entry; information or material against authorized access or theft; and specified personnel against harm.

Plain text*: Normal text or language, or any symbol or signal, that conveys information without any hidden or secret meaning.

Planning and direction: See intelligence cycle.

Policy Review Committee (As pertains to intelligence matters) (PRC(I)): A committee established under the National Security Council which when meeting under the chairmanship of the Director of Central Intelligence is empowered to establish requirements and priorities for national foreign intelligence and to evaluate the quality of the intelligence product; it is sometimes referred to as the Policy Review Committee (Intelligence); its specific duties are defined in Executive Order No. 12036.

Political intelligence*: Intelligence concerning the dynamics of the internal and external political affairs of foreign countries, regional groupings, multilateral treaty arrangements and organizations, and foreign political movements directed against or impacting upon established goverenments or authority.

Positive intelligence: A term of convenience sometimes applied to foreign intelligence to distinguish it from foreign counterintelligence.

Priority: A value denoting a preferential rating or precedence in position which is used to discriminate among competing entities; the term normally used in conjunction with intelligence requirements in order to illuminate importance and to guide the actions planned, being planned, or in use, to respond to the requirements.

Processing*: See intelligence cycle.

Product: (1) An intelligence report disseminated to customers by an intelligence agency. (2) In SIGINT usage, intelligence information derived from analysis of SIGINT materials and published as a report or translation for dissemination to customers (Also see production in Appendix B.)

*See Appendix B, Alternate Definitions.

Production*: See intelligence cycle.

Proprietary: A business entity owned, in whole or in part, or controlled by an intelligence organization and operated to provide private commercial cover for an intelligence activity of that organization. (Also see cover.)

Radar intelligence (RADINT): Intelligence information derived from data collected by radar.

Radiation intelligence* (RINT): The functions and characteristics derived from information obtained from unintentional electromagnetic energy emanating from foreign devices; excludes nuclear detonations or radioactive sources.

Raw intelligence: A colloquial term meaning collected intelligence information which has not yet been converted into intelligence. (Also see intelligence information.)

Reconnaissance (RECCE or RECON): An operation undertaken to obtain by visual observation or other detection methods information relating to the activities, resources or forces of a foreign nation; or to secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area.

Recruitment-in-place: A person who agrees to become an agent and retain his position in his organization or government while reporting on it to an intelligence or security organization of a foreign country.

RED/BLACK Concept: The separation of electrical and electronic circuits, components, equipment, and systems which handle classified plain language information in electric signal form (RED) from those which handle encrypted or unclassified information (BLACK); RED and BLACK terminology is used to clarify specific criteria relating to and differentiating between such circuits, components, equipment, and systems and the areas in which they are contained.

Refugee: A person who is outside the country or area of his former habitual residence and who, because of fear of being persecuted or because of hostilities in that country or area, is unwilling or unable to return to it. (Also see defector and emigre.)

Report: See intelligence report and intelligence information report.

Requirement*: See intelligence requirement or collection requirement.

Residence: See illegal residency and legal residency.

Sabotage: Action against material, premises or utilities, or their production, which injures, interferes with, or obstructs the national security or ability of a nation to prepare for or carry on a war.

Safe house: A house or premises controlled by an intelligence organzation that affords—at least temporarily—security for individuals involved or equipment used in clandestine operations.

Sanitization: The process of editing or otherwise altering intelligence information or reports to protect sensitive intelligence sources, methods, capabilities, analytical procedures, or privileged information in order to permit wider dissemination.

Scientific and technical (S&T) intelligence*: Intelligence concerning foreign developments in basic and applied scientific and technical research and development including engineering and production techniques, new technology, and weapon systems and their capabilities and characteristics; it also includes intelligence which requires scientific

*See Appendix B, Alternate Definitions.

or technical expertise on the part of the analyst, such as medicine, physical health studies, and behavioral analyses.

Scientific and Technical Intelligence Committee (STIC): See Director of Central Intelligence Committee. (Also see DCID 3/5.)

Security: Establishment and maintenance of protective measures which are intended to ensure a state of inviolability from hostile acts or influences.

Security classification: See classification.

Security Committee (SECOM): See Director of Central Intelligence Committee. (Also see DCID 1/11.)

Sensitive*: Requiring special protection from disclosure to avoid compromise or threat to the security of the sponsor.

Sensitive compartmented information* (SCI): All information and material requiring special controls for restricted handling within compartmented intelligence systems and for which compartmentation is established. (Also see compartmentation.)

Sensitive intelligence sources and methods: A collective term for those persons, organizations, things, conditions, or events that provide intelligence information and those means used in the collection, processing, and production of such information which, if compromised, would be vulnerable to counteraction that could reasonably be expected to reduce their ability to support U.S. intelligence activities.

Service Cryptologic Agency(ies) (SCA): See Service Cryptologic Elements.

Service Cryptologic Elements: A term used to designate separately or together those elements of the U.S. Army, Navy, and Air Force which perform cryptologic functions; also known as Service Cryptologic Agencies and Service Cryptologic Organizations.

Service Cryptologic Organizations (SCO): See Service Cryptologic Elements.

Sensor: (1) A technical device designed to detect and respond to one or more particular stimulae and which may record and/or transmit a resultant impulse for interpretation or measurement; often called a technical sensor. (2) Special sensor: An unclassified term used as a matter of convenience to refer to a highly classified or controlled technical sensor.

Side-looking airborne radar (SLAR): An airborne radar, viewing at right angles to the axis of the vehicle, which produces a presentation of terrain or targets.

SIGINT activity: Any activity conducted for the purpose of producing signals intelligence. (Also see SIGINT-related activity.)

SIGINT Committee: See Director of Central Intelligence Committee. (Also see DCID 6/1.)

SIGINT-related activity: Any activity primarily intended for a purpose(s) other than signals intelligence (SIGINT), but which can be used to produce SIGINT, or which produces SIGINT as a by-product of its principal function(s). (Also see SIGINT activity.)

SIGINT technical information: Information concerning or derived from intercepted foreign transmissions or radiations which is composed of technical information (as opposed to intelligence) and which is required in the further collection or analysis of signals intelligence.

*See Appendix B, Alternate Definitions.

Signal*: Anything intentionally transmitted by visual and other electromagnetic, nuclear, or acoustical methods for either communications or non-communications purposes.

Signals intelligence* (SIGINT): Inteligence information comprising either individually or in combination all communications intelligence, electronics intelligence, and foreign instrumentation signals intelligence, however transmitted.

Signals security (SIGSEC): A term which includes communications security and electronics security and which encompasses measures intended to deny or counter hostile exploitation of electronic emissions.

Signals security acquisition and analysis: The acquisition of electronic emissions and subsequent anlysis to determine empirically the susceptibility of the emission to interception and exploitation by hostile intelligence services; it includes cataloging the transmission spectrum and taking signal parametric measurements as required, but does not include acquisition of information carried on the system; it is one of the techniques of signals security surveillance. (Also see signals security surveillance.)

Signals security surveillance: The systematic examination of electronic emissions to determine the adequacy of signals security measures, to identify signals security deficiencies, to provide data from which to predict the effectiveness of proposed signals security measures, and to confirm the adequacy of such measures after implementation.

Source*: A person, device, system, or activity from which intelligence information is obtained. (Also see human source and sensitive intelligence sources and methods.)

Special activities: As defined in Executive Order No. 12036, activities conducted abroad in support of national foreign policy objectives which are designed to further official United States programs and policies abroad and which are planned and executed so that the role of the United States Government is not apparent or acknowledged publicly, and functions in support of such activities, but not including diplomatic activity or the collection and production of intelligence or related support functions; also known as covert action. (Also see covert action.)

Special Activities Office(r) (SAO): A control point for certain categories of compartmented information. (The acronym is often used to refer to the compartmented information itself.)

Special Coordination Committee (SCC): A committee established under the National Security Council which deals inter alia with the oversight of sensitive intelligence activities, such as covert actions, which are undertaken on Presidential authority.

Special intelligence (SI): An unclassified term used to designate a category of sensitive compartmented information (SCI). (Also see sensitive compartmented information.)

Special intelligence communications* (SPINTCOMM): A communications network for the handling of all special intelligence and consisting of those facilities under the operational and technical control of the chief of intelligence of each of the military departments, under the management of the Defense Intelligence Agency, and under the

*See Appendix B, Alternate Definitions.

technical and security specification criteria established and monitored by the National Security Agency.

Special National Intelligence Estimate (SNIE): National Intelligence Estimates (NIEs) which are relevant to specific policy problems that need to be addressed in the immediate future. SNIEs are generally unscheduled, shorter, and prepared more quickly than NIEs and are coordinated within the Intelligence Community to the extent that time permits. (Also see National Intelligence Estimate.)

Special Security Office(r) (SSO): A control point for security procedures within any activity authorized access to sensitive compartmented information.

Special sensor*: See sensor.

Strategic intelligence: Intelligence which is required for the formulation of policy and military plans at national and international levels; it differs primarily from tactical intelligence in level of use, but may also vary in scope and detail.

Strategic warning: Intelligence information or intelligence regarding the threat of the initiation of hostilities against the U.S. or in which U.S. forces may become involved; it may be received at any time prior to the initiation of hostilities.

Support for the Analysts' File Environment (SAFE): A joint CIA/DIA project to develop a new computer/microfilm m system to support production analysts in reading, filing, and routing cable traffic; building and searching private and central files; and writing, editing, and routing intelligence memoranda and reports.

Surveillance: The systematic observation or monitoring of places, persons, or things by visual, aural, electronic, photographic, or other means.

Tactical intelligence* (TACINTEL): Foreign intelligence produced under the aegis of the Secretary of Defense and intended primarily to be responsive to the needs of military commanders in the field to maintain the readiness of operating forces for combat operations and to support the planning and conduct of combat operations. (Also see combat intelligence.)

Tactical intelligence asset: An intelligence asset funded in Department of Defense programs, the primary purpose of which is the collection or processing of intelligence information or the production of tactical intelligence. (Also see tactical intelligence and intelligence asset.)

Target: A country, area, installation, organization, weapon system, military force, situation (political or economic), signal, person, or other entity against which intelligence operations are conducted.

Target intelligence: Intelligence which portrays and locates the components of a target or target complex and indicates its identification, vulnerability, and relative importance.

Tasking: The assignment or direction of an individual or activity to perform in a specified way to achieve an objective or goal.

Technical intelligence (TI): Intelligence on the characteristics and performance of foreign weapons and equipment; a part of scientific and technical intelligence and distinct from order of battle.

Technical sensor: See sensor.

*See Appendix B, Alternate Definitions.

Technical SIGINT: Intelligence information which provides a detailed knowledge of the technical characteristics of a given emitter and thus permits estimates to be made about its primary function, capabilities, modes of operation (including malfunctions), and state-of-the-art, as well as its specific role within a complex weapon system or defense network; it is a contributor to technical intelligence.

Telecommunications: Any transmission, emission, or reception of signs, signals, writing, images, and sounds or information of any nature by wire, radio, visual, or other electromagnetic systems.

Telemetry intelligence (TELINT): Technical and intelligence information derived from intercept, processing, and analysis of foreign telemetry; a subcategory of foreign instrumentation signals intelligence.

Teleprocessing: The overall function of an information transmission system which combines telecommunications, automatic data processing, and man-machine interface equipment and their interaction as an integrated whole.

TEMPEST: An unclassified term referring to technical investigations for compromising emanations from electrically operated, information processing equipment; they are conducted in support of emanations and emission security.

Terrorist organization: A group that engages in terrorist activities. (Also see international terrorist activity.)

Traffic analysis (TA): The cryptologic discipline which develops information from communications about the composition and operation of communications structures and the organizations they serve. The process involves the study of traffic and related materials, and the reconstruction of communication plans, to produce signals intelligence.

Transmission security (TRANSEC): The component of communications security which results from all measures designed to protect transmissions from interception and from exploitation by means other than cryptanalysis.

Unauthorized disclosure: See compromise.

Uni-level security: (For automatic data processing systems) Provision for the safeguarding of all material within a single information handling system in accordance with the highest level of classification and most restrictive dissemination caveats assigned to any material contained therein, as distinguished from multilevel security. (Also see multi-level security.)

United States Signals Intelligence System (USSS): An entity that is compromised of the National Security Agency (including assigned military personnel); those elements of the military departments and the Central Intelligence Agency performing signals intelligence activities; and those elements of any other department or agency which may from time to time be authorized by the National Security Council to perform signals intelligence activities during the time when such elements are so authorized; it is governed by the United States Signals Intelligence Directives (USSID) system.

Upgrade: To determine that certain classified information requires, in the interest of national security, a higher degree of protection against unauthorized disclosure than currently provided, coupled with

*See Appendix B, Alternate Definitions.

a changing of the classification designation to reflect such higher degree. (Also see classification.)

User: See customer.

Validation: A process normally associated with the collection of intelligence information which provides official status to an identified requirement and confirms that the requirement is appropriate for a given collector and has not previously been satisfied. (Also see collection requirement.)

Walk-in: A person who on his own initiative makes contact with a representative of a foreign country and who volunteers intelligence information and/or requests political asylum. (Also see disaffected person.)

Weapon and Space Systems Intelligence Committee (WSSIC): See Director of Central Intelligence Committee. (Also see DCID 3/4.)

APPENDIX A—ACRONYMS AND ABBREVIATIONS

ACINT—Acoustical Intelligence (Naval acronym; see definition.)
ACOUSTINT—Acoustical Intelligence.
ASCI—Assistant Chief of Staff/Intelligence (Army or Air Force).
CA—Cryptanalysis.
CAMS—COMIREX Automated Management System.
CCF—Collection Coordination Facility.
CCP—Consolidated Cryptologic Program.
CCPC—Critical Collection Problems Committee.
CI—Counterintelligence.
CIA—Central Intelligence Agency.
CIAP—Central Intelligence Agency Program.
CIFAX—Enciphered Facsimile.
CIPHONY—Enciphered Telephone.
CIRIS—Consolidated Intelligence Resources Information System.
CIVISION—Enciphered Television.
COINS—Community On-Line Intelligence System.
COMEX—Committee on Exchanges.
COMINT—Communications Intelligence.
COMIREX—Committee on Imagery Requirements and Exploitation.
COMSEC—Communications Security.
CONTEXT—Conferencing and Text Manipulation System.
CRITIC—Critical Intelligence Message.
CRITICOMM—Critical Intelligence Communications System.
CRYPTO—CRYPTO. (See definition.)
DAO—Defense Attache Office.
DCI—Director of Central Intelligence.
DCID—Director of Central Intelligence Directive.
DEA—Drug Enforcement Administration.
DEFSMAC—Defense Special Missile and Astronautic Center.
DF—Direction Finding.
DIA—Defense Intelligence Agency.
DNI—Director of Naval Intelligence.
ECCM—Electronic Counter-Countermeasures.
ECM—Electronic Countermeasures.
EEI—Essential Elements of Information.
E & E—Evasion and Escape.

EIC—Economic Intelligence Committee.
ELECTRO-OPTINT—Electro-optical Intelligence.
ELINT—Electronic Intelligence.
ELSEC—Electronic Security.
EMSEC—Emanations Security.
EOB—Electronic Order of Battle.
ESM—Electronic Warfare Support Measures.
EW—Electronic Warfare.
FBI—Federal Bureau of Investigation.
FBIS—Foreign Broadcast Information Service.
FCI—Foreign Counterintelligence.
FI—Foreign Intelligence.
FIS—Foreign Instrumentation Signals.
FISINT—Foreign Instrumentation Signals Intelligence.
FLIR—Forward-looking infrared.
FORMAT—Foreign Materiel.
GDIP—General Defense Intelligence Program.
GMI—General Medical Intelligence.
HPSCI—House Permanent Select Committee on Intelligence.
HRC—Human Resources Committee.
HUMINT—Human Intelligence.
IC—Intelligence Community.
ICRS—Imagery Collection Requirements Subcommittee (COMIREX).
IDC—Interagency Defector Committee.
IHC—Intelligence Information Handling Committee.
II—Imagery Interpretation.
IIM—Interagency Intelligence Memorandum.
ILC—International Lines of Communications.
IMINT—Imagery Intelligence.
INR—Bureau of Intelligence and Research, Department of State.
IOB—Intelligence Oversight Board.
IRA—Intelligence-Related Activities.
IR&DC—Intelligence Research & Development Council.
I&W—Indications and Warning.
JAEIC—Joint Atomic Energy Intelligence Committee.
JINTACCS—Joint Interoperability Tactical Command and Control System.
LASINT—Laser Intelligence.
MASINT—Measurement and Signature Intelligence.
MEDINT—Medical Intelligence.
MI—Military Intelligence.
NFAC—National Foreign Assessment Center.
NFIB—National Foreign Intelligence Board.
NFIP—National Foreign Intelligence Program.
NIE—National Intelligence Estimate.
NIO—National Intelligence Officer.
NITC—National Intelligence Tasking Center.
NMIC—National Military Intelligence Center
NOIWON—National Operations and Intelligence Watch Officers Network.
NPHR—National Foreign Intelligence Plan for Human Resources.

NPIC—National Photographic Interpretation Center.
NSA—National Security Agency.
NSCID—National Security Council Intelligence Directive.
NSOC—National SIGINT Operations Center.
NSRL—National SIGINT Requirements List.
NTPC—National Telemetry Processing Center.
NUCINT—Nuclear Intelligence.
OB—Order of Battle.
OPCON—Operational Control.
OPINTEL—Operational Intelligence.
OPSEC—Operations Security.
OPTINT—Optical Intelligence.
PARPRO—Peacetime Airborne Reconnaissance Program.
PHOTINT—Photographic Intelligence.
PI—Photographic Interpretation or Photographic Interpreter.
PRC(I)—Policy Review Committee (Intelligence).
RADINT—Radar Intelligence.
RECCE or RECON—Reconnaissance.
RINT—Radiation Intelligence.
S&T—Scientific and Technical.
SA—Signals Analysis.
SAFE—Support for the Analysts' File Environment.
SAO—Special Activities Office.
SCA—Service Cryptologic Agencies.
SCC—Special Coordination Committee.
SCI—Sensitive Compartmented Information or Source Code Indicator.
SCO—Service Cryptologic Organizations.
SECOM—Security Committee.
SI—Special Intelligence.
SIGINT—Signals Intelligence.
SIGINT Committee—Signals Intelligence Committee.
SIGSEC—Signals Security.
SIRVES—SIGINT Requirements Validation and Evaluation Subcommittee (of SIGINT Committee).
SLAR—Side-Looking Airborne Radar.
SNIE—Special National Intelligence Estimate.
SOSUS—Sound Surveillance System.
SOTA—SIGINT Operational Tasking Authority.
SPINTCOMM—Special Intelligence Communications.
SSCI—Senate Select Committee on Intelligence.
SSO—Special Security Officer.
STIC—Scientific and Technical Intelligence Committee.
TA—Traffic Analysis.
TACINTEL—Tactical Intelligence.
TI—Technical Intelligence.
TELINT—Telemetry Intelligence.
TRANSEC—Transmission Security.
USSID—United States Signals Intelligence Directive.
USSS—United States Signals Intelligence System.
WSSIC—Weapon and Space Systems Intelligence Committee.
WWMCCS—Worldwide Military Command and Control Systems.

APPENDIX B—ALTERNATE DEFINITIONS

Acoustial intelligence: The technical and intelligence information derived from foreign sources which generate waves. (Dictionary of Military and Associated Terms, Dept. of Defense (U), the Joint Chiefs of Staff, 3 Sep 74 (U)).

Agent: (1) An individual who acts under the direction of an intelligence agency or security service to obtain, or assist in obtaining, information for intelligence or counterintelligence purposes. (Final Report, Senate Select Committee on Intelligence, 26 April 1976). (2) In intelligence usage, one who is authorized or instructed to obtain or to assist in obtaining information for intelligence or counterintelligence purposes. (Dictionary of Military and Associated Terms, Dept. of Defense (U), the Joint Chiefs of Staff, 3 Sep 74. (U)).

Agent of influence: An individual who can be used to influence covertly foreign officials, opinion molders, organizations, or pressure groups in a way which will generally advance United States Government objectives, or to undertake specific action in support of United States Government objectives. (Final Report, Senate Select Committee on Intelligence, 26 April 1976).

Analysis: In electronic warfare, a study of electromagnetic radiations to determine their technical characteristics and their tactical or strategic use. (Glossary of Communications-Electronics Terms (U), JCS, Dec 74).

Assessment: Judgment of the motives, qualifications, and characteristics of present or prospective employees or "Agents." (Dictionary of Military and Associated Terms, Dept. of Defense (U), the Joint Chiefs of Staff, 3 Sep 74. (U)).

Asset: Any resource—a person, group, relationship, instrument, installation, or supply—at the disposition of an intelligence agency for use in an operational or support role. The term is normally applied to a person who is contributing to a CIA clandestine mission, but is not a fully controlled agent of CIA. (Final Report, Senate Select Committee on Intelligence, 26 April 1976.)

Basic intelligence: (1) General reference material for use in planning concerning other countries which pertains to capabilities, resources or potential theaters of operations. See also—intelligence—. (Dictionary of Military and Associated Terms, Dept. of Defense (U), the Joint Chiefs of Staff, 3 Sep 74. (U)). (2) Factual, fundamental, and generally permanent information about all aspects of a nation—physical, social, economic, political, biographical, and cultural—which is used as a base for intelligence products in support of planning, policymaking, and military operations. (Final Report, Senate Select Committee on Intelligence, 26 April 1976). (3) "Fundamental intelligence concerning the general situation, resources, capabilities and vulnerabilities of foreign countries or areas which may be used as reference material in the planning of operations at any level and in evaluating subsequent information relating to the same subject." (Recommended Changes to JCS Pub 1, 25 July 1977).

Case officer: A staff employee of the CIA who is responsible for handling agents. (Final Report, Senate Select Committee on Intelligence, 26 April 1976).

Cipher: Any cryptographic system in which arbitrary symbols or groups of symbols represent units of plain text. (Final Report, Senate Select Committee on Intelligence, 26 April 1976).

Clandestine operations: (1) Intelligence, counterintelligence, or other information collection activities and covert political, economic, propaganda and paramilitary activities, conducted so as to assure the secrecy of the operation. (Final Report, Senate Select Committee on Intelligence, 26 April 1976). (2) Activities to accomplish intelligence, counterintelligence, and other similar activities sponsored or conducted by Governmental departments or agencies, in such a way as to assure secrecy or concealment. (It differs from covert operations in that emphasis is placed on concealment of the operation rather than on concealment of identity of sponsor.) (Dictionary of Military and Associated Terms, Dept. of Defense (U), the Joint Chiefs of Staff, 3 Sep 74. (U)).

Classified information: "Classified information" means information or material (hereinafter collectively termed "information") that is owned by, produced for or being in the possession of or under the control of the United States Government that has been determined by proper authority to require protection against unauthorized disclosure in the interest of national security and is so designated. Classification and Declassification of National Security Information and Material; (Executive Order No. 11652 as amended, Nov 1977).

Code: A system of communication in which arbitrary groups of symbols represent units of plain text. Codes may be used for brevity or for security. (Final Report, Senate Select Committee on Intelligence, 26 April 1976).

Code word: (1) A word which has been assigned a classification and a classified meaning to safeguard intentions and information regarding a planned operation. (Final Report, Senate Select Committee on Intelligence, 26 April 1976). (2) A word which has been assigned a classification and a classified meaning to safeguard intentions and information regarding a classified plan or operation. (Communications-Electronics Terminology (U), U.S. Dept. of the Air Force, 15 Nov 73, (U)). (3) A word which conveys a meaning other than its conventional one. Prearranged by the correspondents. Its aim is to increase security. (Glossary of Communications-Electronics Terms (U), PCS, Dec 74).

CODEWORD: (1) A cryptonym used to identify sensitive intelligence data. (Glossary of Communications-Electronics Terms (U), JCS, Dec 74). (2) A single word selected from those listed in joint Army, Navy, Air Force publication (JANAP) 299 and subsequent volumes, and assigned a classified meaning by appropriate authority to insure proper security concerning intentions, and to safeguard information pertaining to actual, real world military plans or operations classified as Confidential or higher. (Modern Data Communications Concepts, Language and Media (U), Willaim P. Davenport, Hayden Book Co., Inc., 1971, (U)).

Collection: (1) Any one or more of the gathering, analysis dissemination or storage of non-publicly available information without the informed express consent of the subject of the information. (USSID 18, Limitations and Procedures in Signals Intelligence Operations of

the USSS (U), NSA, 26 May 76). (2) The act of employing instruments and/or equipment to obtain qualitative or quantitative data from the test or operation of foreign systems. (Defense Intelligence Collection Requirements Manual (C), DIA, 27 Jan 75). (3) Used ELINT to mean the gathering or collection of the unevaluated and uninterpreted information about the enemy or potential enemy. Specifically the collection of data from noncommunications radiators such as radars, navigation aids or countermeasures equipments. (Basic Manual (U), ELINT Collection Analysis Guide (U), National Cryptologic School, 1965, (S)).

Communications intelligence (COMINT): (1) Technical and intelligence information derived from foreign communications by other than the intended recipients. COMINT is produced by the collection and processing of foreign communications passed by electromagnetic means, with specific exceptions stated below, and by the processing of foreign encrypted communications. However transmitted, COMINT shall not include:

1. Intercept and processing of unencrypted written communications, except the processing of written plain text versions of communications which have been encrypted or are intended for subsequent encryption.

2. Intercept and processing of press, propaganda and other public broadcasts, except for processing encryted or "hidden meaning" passages in such broadcasts.

3. Oral and wire interceptions conducted under DoD Directive 5200.24.

4. Censorship. (Signals Intelligence (SIGINT) (U), DOD, 25 Jan. 73).

(2) Technical and intelligence information derived from foreign communications by other than the intended recipients:

A. Foreign Communications are all communications except: (1) Those of the governments of the U.S. and the British Commonwealth, (2) Those exchanged among private organizations and nationals, acting in a private capacity of the U.S. and the British Commonwealth, (3) Those of nationals of the U.S. and British Commonwealth appointed or detailed by their governments to serve in the international organizations.

B. COMINT activities are those which produce COMINT by collecting and processing foreign communications passed by radio, wire, or other electromagnetic means, and by the processing of foreign encrypted communications. However transmitted, collection comprises search, intercept, and direction finding. Processing comprises range estimation, transmitter/operator identification, signal analysis, traffic analysis, cryptanalysis, decryption, study of the plaintext, the fusion of these processes, and the reporting of results.

C. Exceptions to COMINT and COMINT activities. COMINT and COMINT activities as defined here do not include: (1) Intercept and processing of unencrypted written communications, except written plaintext versions of communications which have been encrypted or are intended for subsequent encryption. (2) Intercept and processing of press, propaganda and other public broadcasts, except for encrypted or "hidden meaning" passages in such

broadcast. (3) Operations conducted by U.S., U.K. or Commonwealth security authorities. (4) Censorship. (5) The interception and study of non-communications transmissions (ELINT). (USSID 3, SIGINT Security (U), NSA, 24 Aug. 72).

(3) Technical and intelligence information derived from foreign communications by someone other than the intended recipient. It does not include foreign press, propaganda, or public broadcasts. The term is sometimes used interchangeably with SIGINT. (Final Report, Senate Select Committee on Intelligence, 26 April 1976).

Communications security (COMSEC): (1) Protective measures taken to deny unauthorized persons information derived from telecommunications of the United States Government related to national security and to ensure the authenticity of such telecommunications. (U.S. Intelligence Activities, Executive Order No. 12036, January 1978.) (2) The protection of United States telecommunications and other communications from exploitation by foreign intelligence services and from unauthorized disclosure. COMSEC is one of the mission responsibilities of NSA. It includes cryptosecurity, transmission security, emission security, and physical security of classified equipment, material, and documents. (Final Report, Senate Select Committee on Intelligence, April 26, 1976). (3) The protection resulting from the application of cryptosecurity, transmission security, and emission security measures to telecommunications and from application of physical security measures to COMSEC information. These measures are taken to deny unauthorized persons information of value which might be derived from the possession and study of such telecommunications or to insure the authenticity of such telecommunications. (Glossary of Communications Security and Emanations Security Terms (U), U.S. Communications Security Board, Oct. 74). (4) The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. Also called COMSEC. Communications security includes: A. Cryptosecurity: B. Transmission Security: C. Emission Security: and D. Physical Security of Communications Security materials and information:

A. Cryptosecurity—The component of communications security which results from the provision of technically sound cryptosystems and their proper use.

B. Transmission Security—The component of communications security which results from all measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis.

C. Emission Security—The component of communications security which results from all measures taken to deny unauthorized persons information of value which might be derived from intercept and analysis of compromising emanations from cryptoequipment and telecommunications systems.

D. Physical Security—The component of communications security which results from all physical measures necessary to safeguard classified equipment, material, and documents from access thereto or observation thereof by unauthorized persons. (Dictionary of Military and Associated Terms, Dept. of Defense (U), the Joint Chiefs of Staff, 3 Sep. 74. (U)).

Compartmentation: (1) The practice of establishing special channels for handling sensitive intelligence information. The channels are limited to individuals with a specific need for such information and who are therefore given special security clearances in order to have access to it. (Final Report, Senate Select Committee on Intelligence, 26 April 1976). (2) 1. In SIGINT, special protection given to the production and distribution of SIGINT material of especially sensitive nature because of its source, method of processing, or content. 2. In COMSEC, restricting the use of specific primary cryptovariables to specific operational units grouped together on the basis of their geographical area or their common participation in a mission or operation for the purpose of limiting the information protected by these cryptovariables and thus limiting the adverse impact of a compromise of these variables. (Basic Cryptologic Glossary (U), NSA, 1971. (3) 1. Establishment and management of an intelligence organization so that information about the personnel, organization, or activities of one component is made available to any other component only to the extent required for the performance of assigned duties. (Dictionary of Military and Associated Terms, Dept. of Defense (U), the Joint Chiefs of Staff, 3 Sep 74 (U)).

Compromise: (1) The loss of control over any COMINT or information related to COMINT or COMINT activities resulting in a reasonable assumption that it could have, or confirmation of the fact that it has, come to the knowledge of an unauthorized person. (USSID 3, SIGINT Support to Military Commanders (U), NSA, 1 Jul 74). (2) The known or suspected exposure of classified information or material in whole or in part to unauthorized persons through loss, theft, capture, recovery by salvage, defection of individuals, unauthorized viewing, or any other means. (Basic Cryptologic Glossary (U), NSA, 1971).

Computer security: The protection resulting from all measures designed to prevent either deliberate or inadvertent unauthorized disclosure, acquisition, manipulation, or modification of classified information in a computer system. (Basic Cryptologic Glossary (U), NSA, 1971).

Consumer: An obsolete term for customer. (Basic Cryptologic Glossary (U), NSA, 1971).

Counterintelligence: (1) Information gathered and activities conducted to protect against espionage and other clandestine intelligence activities, sabotage, international terrorist activities or assassinations conducted for or on behalf of foreign powers, organizations or persons, but not including personnel, physical, document, or communications security programs. (U.S. Intelligence Activities, Executive Order No. 12036, Jan 1978.) (2) Information concerning the protection of foreign intelligence or of national security information and its collection from detection or disclosure. (USSID 18, Limitations and Procedures in Signals Intelligence Operations of the USSS (U), NSA, 26 May 76). (3) That phase of intelligence covering all activity devoted to destroying the effectiveness of inimical foreign intelligence activities and to the protection of information against espionage, personnel against subversion, and installations or material against sabotage. See also counterespionage, countersabotage, countersubversion. (Dictionary of Military and Associated Terms, Dept. of Defense (U), the Joint

Chiefs of Staff, 3 Sep 74). (4) That aspect of intelligence activity which is devoted to destroying the effectiveness of inimical foreign intelligence activities and to the protection of information against espionage, individuals against subversion, and installations or material against sabotage. See also counterespionage, countersabotage, countersubversion. (Dictionary of Military and Associated Terms, Dept. of Defense (U), the Joint Chiefs of Staff, 3 Sep 74 (U)).

Critical intelligence: Intelligence which is critical and requires the immediate attention of the commander. It is required to enable the commander to make decisions which will provide a timely and appropriate response to actions by the potential/actual enemy. It includes but it is not limited to the following:

A. Strong indications of the imminent outbreak of hostilities of any type (warning of attack):

B. Aggression of any nature against a friendly country:

C. Indications or use of nuclear-biological chemical weapons (targets): and

D. Significant events within potential enemy countries that may lead to modification of nuclear strike plans. (Dictionary of Military and Associated Terms, Dept. of Defense (U), the Joint Chiefs of Staff, 3 Sep 74. (U)).

Critical intelligence message (CRITIC): A message containing information indicating a situation or pertaining to a situation which affects the security or interests of the United States or its allies to such an extent that it may require the immediate attention of the President. (Defense Special Security Communications System (DSSCS) Operating Instructions System Procedures (U), NSA, 6 Feb 73).

Cryptography: The enciphering of plain text so that it will be unintelligible to an unauthorized recipient. (Final Report, Senate Select Committee on Intelligence, 26 April 1976).

Cryptomaterial: All COMSEC material bearing the marking CRYTO or otherwise designated as incorporating cryptographic information. Classified cryptoequipments, their classified subdivisions and keying material are considered cryptomaterial even though they do not bear the CRYPTO marking. (Communications-Electronics Terminology (U), U.S. Dept. of the Air Force, 15 Nov. 73).

Current intelligence: Summaries and analyses of recent events. (Final Report, Senate Select Committee on Intelligence, 26 April 1976).

Defector: A person who, for political or other reasons, has repudiated his country and may be in possession of information of interest to the United States Government. (Final Report, Senate Select Committee on Intelligence, 26 April 1976).

Defense Intelligence Community: The Defense Intelligence Agency, National Security Agency, and the intelligence components of the unified and specified command. (IDHS Glossary of Common Acronyms, Codes, Abbreviations, and Terms Used in Dept. of Defense Intelligence Data Handling Systems (IDHS) Documents (U), DIA, 1970).

Departmental intelligence: (1) Intelligence which any department or agency of the Federal Government requires to execute its own mission. (Dictionary of Military and Associated Terms, Dept. of Defense (U), the Joint Chiefs of Staff, 3 Sept. 74. (U)). (2) The intelligence

which Government departments and agencies generate in support of their own activities. (Final Report, Senate Select Committee on Intelligence, 26 April 1976).

Dissemination: The distribution of information intelligence products (in oral, written, or graphic form) to departmental and agency intelligence consumers. (Final Report, Senate Select Committee on Intelligence, 26 April 1976).

Double agent: Agent in contact with two opposing intelligence services only one of which is aware of the double agent contact or quasi-intelligence services. (Dictionary of Military and Associated Terms, Dept. of Defense (U), the Joint Chiefs of Staff, 3 Sept. 74. (U)).

Economic intelligence: Intelligence regarding foreign economic resources, activities, and policies. (Final Report, Senate Select Committee on Intelligence, 26 April 1976).

Electronic intelligence (ELINT): (1) That technical and intelligence information derived from foreign electromagnetic noncommunications transmissions by other than the intended recipients. (Glossary of Communications-Electronics Terms (U), JCS, Dec. 74). (2) The intelligence information product of activities engaged in the collection and processing for subsequent intelligence purposes of foreign noncommunications electromagnetic radiations emanating from other than nuclear detonations and radioactive sources. (Basic Cryptologic Glossary (U), NSA, 1971). (3) Technical and intelligence information derived from the collection (or interception) and processing of foreign electromagnetic radiations (noncommunications) emanating from sources such as radar. ELINT is part of the NSA/CSS Signals Intelligence Mission. (Final Report, Senate Select Committee on Intelligence, 26 April 1976).

Electronic order of battle (EOB): A document summarizing the deployment of enemy noncommunications and communications emitters in a given area. In addition to deployment, the EOB also contains data as to the function of each emitter. (Basic Manual (U), ELINT Collection Analysis Guide (U), National Cryptologi School, 1965).

Electronic security: The detection, identification, evaluation, and location of foreign electromagnetic radiations. (Final Report, Senate Select Committee on Intelligence, 26 April 1976).

Electronic surveillance: Surveillance conducted on a person, group, or other entity by electronic equipment which is often highly sophisticated and extremely sensitive. (Final Report, Senate Select Committee on Intelligence, 26 April 1976).

Encipher: To convert a plain text message into unintelligible form by the use of a cipher system. (Final Report, Senate Select Committee on Intelligence, 26 April 1976).

Encrypt: To convert a plain text message into unintelligible form by means of a cryptosystem; this term covers the meanings of encipher and encode. (Final Report, Senate Select Committee on Intelligence, 26 April 1976).

Espionage: Clandestine intelligence collection activity: This term is often interchanged with "clandestine collection." (Final Report, Senate Select Committee on Intelligence, 26 April 1976).

Evaluation: (1) Appraisal of an item of information in terms of credibility, reliability, pertinency, and accuracy. Appraisal is accomplished at several stages within the intelligence process with progres-

sively different contexts. Initial evalutions made by case officers and report officers are focused upon the reliability of the source and the accuracy of the information as judged by data available at or close to their operational levels. Later evaluations by intelligence analysts are primarily concerned with verifying accuracy of information and may, in effect, convert information into intelligence. Appraisal or evaluation of items of information or intelligence is indicated by a standard letter-number system. The evaluation of the reliability of sources is designated by a letter from A through F, and the accuracy of the information is designated by numeral 1 through 6. These are two entirely independent appraisals, and these separate appraisals are indicated in accordance with the system indicated below. Thus, information adjudged to be "probably true" received from a "usually reliable source" is designated "B–2" or "B2" while information of which the "truth cannot be judged" received from a "usually reliable source" is designated "B–6" or "B6":

Reliability of source: A—Completely reliable; B—Usually reliable; C—Fairly reliable; D—Not usually reliable; E—Unreliable; F—Reliability cannot be judged.

Accuracy of information: 1—Confirmed by other sources; 2—Probably true; 3—Possibly true; 4—Doubtful; 5—Improbable; 6—Truth cannot be judged. (Dictionary of Military and Associated Terms, Dept. of Defense (U), the Joint Chiefs of Staff, 3 Sep 74. (U)).

(2) In intelligence usage, appraisal of an item of information in terms of credibility, reliability, pertinency, and accuracy. Appraisal is accomplished at several stages within the intelligence cycle with progressively different contexts. (Recommended Change to JCS Pub 1, 25 July 1977).

Exploitation: In SIGINT, the production of information from messages that are encrypted in systems whose basic elements are known. Exploitation includes decryption, translation, and the solution of specific controls such as indicators and specific keys. (Basic Cryptologic Glossary (U), NSA, 1971).

Foreign intelligence: (1) Information relating to the capabilities, intentions and activities of foreign powers, organizations or persons, but not including counterintelligence except for information on international terrorist activities. (U.S. Intelligence Activities, Executive Order No. 12036, Jan. 1978.) (2) a. Information concerning the capabilities, intentions and activities of any foreign power, or of any non-United States person, whether within or outside the United States or concerning areas outside the United States. b. Information relating to the ability of the United States to protect itself against actual or potential attack or other hostile acts of a foreign power or its agents. c. Information with respect to foreign powers or non-United States persons which because of its importance is deemed essential to the security of the United States or to the conduct of its foreign affairs. d. Information relating to the ability of the United States to protect itself against the activities of foreign intelligence services. (USSID 18, Limitations and Procedures in Signals Intelligence Operations of the USSS (U), NSA, 26 May 76). (3) Intelligence concerning areas not under control of the power sponsoring the collection effort. (Dictionary of Military and Associated Terms, Dept. of Defense (U), the Joint Chiefs of Staff, 3 Sep 74. (U)).

Guidance: The general direction of an intelligence effort, particularly in the area of collection. (Final Report, Senate Select Committee on Intelligence, 26 April 1976).

Integration: In photography, a process by which the average radar picture seen on several scans of the time base may be obtained on a print, or, the process by which several photographic images are combined into a single image. (Dictionary of Military and Associated Terms, Dept. of Defense (U), the Joint Chiefs of Staff, 3 Sep 74. (U)).

Intelligence: (1) Foreign intelligence and counterintelligence. (U.S. Intelligence Activities, Executive Order No. 12036, Jan 78.) (2) The product resulting from the collection, collation, evaluation, analysis, integration, and interpretation of all collected information. (Final Report, Senate Select Committee on Intelligence, 26 April 1976). (3) The product resulting from the collecting and processing of information concerning actual and potential situations and conditions relating to foreign activities and to foreign or enemy-held areas. This processing includes the evaluation and collation of the information obtained from all available sources, and its analysis, synthesis, and interpretation. (Basic Cryptologic Glossary (U), NSA, 1971). (4) The product resulting from the collection, evaluation, analysis, integration, and interpretation of all available information which concerns one or more aspects of foreign nations or of areas of operation and which is immediately or potentially significant to military planning and operations. (Dictionary of Military and Associated Terms, Dept. of Defense (U) the Joint Chiefs of Staff, 3 Sep 74 (U)).

Intelligence activities: Sec. 14. (a) As used in this resolution, the term "intelligence activities" includes (1) the collection, analysis, production, dissemination, or use of information which relates to any foreign country, or any government, political group, party, military force, movement, or other association in such foreign country, and which relates to the defense, foreign policy, national security, or related policies of the United States, and other activity which is in support of such activities; (2) activities taken to counter similar activities directed against the United States; (3) covert or clandestine activities affecting the relations of the United States with any foreign government, political group, party, military force, movement or other association; (4) the collection, analysis, production, dissemination, or use of information about activities of persons within the United States, its territories and possessions, or nationals of the United States abroad whose political and related activities pose, or may be considered by any department, agency, bureau, office, division, instrumentality, or employee of the United States to pose, a threat to the internal security of the United States, and covert or clandestine activities directed against such persons. Such term does not include tactical foreign military intelligence serving no national policymaking function. (Senate Resolution 400, June 1977.)

Intelligence cycle: (1) The steps by which information is assembled, converted to intelligence, and made available to users. These steps are in four phases:

A. Planning and direction: Determination of intelligence requirements, preparation of a collection plan, issuance of orders and requests to information collection agencies, and a continuous check on the productivity of collection agencies.

B. Collection: The exploitation of sources of information by collection agencies and the delivery of this information to the proper intelligence processing unit for use in the production of intelligence.

C. Processing: The step whereby information becomes intelligence through evaluation, analysis, integration, and interpretation.

D. Dissemination: The conveyance of intelligence in suitable form (oral, graphic, or written) to agencies needing it. (Dictionary of Military and Associated Terms, Dept. of Defense (U), the Joint Chiefs of Staff, 3 Sep. 74. (U)). (2) The steps by which information is assembled, converted into intelligence, and made available to consumers. The cycle is composed of four basic phases: (1) direction: the determination of intelligence requirements, preparation of a collection plan, tasking of collection agencies, and a continuous check on the productivity of these agencies; (2) collection: the exploitation of information sources and the delivery of the collected information to the proper intelligence processing unit for use in the production of intelligence; (3) processing: the steps whereby information becomes intelligence through evaluation, analysis, integration, and interpretation; and (4) dissemination: the distribution of information or intelligence products (in oral, written, or graphic form) to departmental and agency intelligence consumers. (Final Report, Senate Select Committee on Intelligence, April 26, 1976).

Intelligence estimate: An appraisal of the elements of intelligence relating to a specific situation or condition with a view to determining the courses of action open to the enemy or potential enemy and the probable order of their adoption. (Dictionary of Military and Associated Terms, Dept. of Defense (U), the Joint Chiefs of Staff, 3 Sep 74. (U)).

Intelligence information: (1) In SIGINT, information which is of intelligence use to customers whose primary mission does not include SIGINT operations of technical SIGINT information. (Basic Cryptologic Glossary (U), NSA (P1, 1971). (2) The unevaluated and uninterpreted information about the enemy or potential enemy. (Basic manual (U), ELINT Collection Analysis Guide (U), National Cryptologic School, 1965).

Intelligence report: A specific report of information, usually on a single item, made at any level of command in tactical operations and disseminated as rapidly as possible in keeping with the timeliness of the information. Also called INTREP. (Dictionary of Military and Associated Terms. Dept. of Defense (U), the Joint Chiefs of Staff, 3 Sep. 74. (U)).

Intelligence requirement: A consumer statement of information needed which is not already at hand. (Final Report, Senate Select Committee on Intelligence, 26 April 1976).

Interception: The act of searching for and listening to and/or recording communications and/or electronic transmissions for the purpose of obtaining intelligence. (Glossary of Communications-Electronics Terms (U), JCS, Dec. 1974).

International terrorist activities: Means any activity or activities which: (a) involves killing, causing serious bodily harm, kidnapping,

or violent destruction of property, or an attempt or credible threat to commit such acts; and (b) appears intended to endanger a protectee of the Secret Service or the Department of State or to further political, social, or economic goals by intimidating or coercing a civilian population or any segment thereof, influencing the policy of a government or international organization by intimidation or coercion, or obtaining widespread publicity for a group or its cause; and (c) transcends national boundaries in terms of the means by which it is accomplished, the civilian population, government, or international organization it appears intended to coerce or intimidate, or the locale in which its perpetrators operate or seek asylum. (U.S. Intelligence Activities, Executive Order No. 12036, 26 Jan. 1978.)

Measurement and signature intelligence (MASINT): MASINT is obtained by quantitative and qualitative analysis of data (metric, angle, spatial, wavelength, time dependent, modulation, plasma, and hydromagnetic) derived from sensing instruments other than those normally associated with human communications, electronics intelligence (HUMINT, COMINT, ELINT) or imagery collection. MASINT includes, but is not limited to, the following disciplines: Radar intelligence (RADINT): Nuclear intelligence (NUCINT): Unintentional Radiation intelligence (RINT): Acoustic intelligence (Non-Compressible fluids—ACINT: Compressible fluids—ACOUSTINT): Electro-Optic intelligence (Electro-OPTINT): Even-related dynamic measurements photography (OPTINT): and debris collection. Telemetry intelligence (TELINT) is a special category of signals intelligence (SIGINT) that provides measurement data on foreign instrumentation signals (FIS). Requirements for collection will be expressed as MASINT requirements. The term MASINT should be used when referring to the above categories of special sensor disciplines in aggregate. (Defense Intelligence Collection Requirements Manual (C), DIA, 27 Jan. 1975).

Medical intelligence: That category of intelligence which concerns itself with man as a living organism and those factors affecting his efficiency, capability, and well-being. (Dictionary of Military and Associated Terms, Dept. of Defense (U), the Joint Chiefs of Staff, 3 Sep 74. (U)).

National intelligence: (1) Integrated departmental intelligence that covers the broad aspects of national policy and national security, is of concern to more than one department or agency, and transcends the exclusive competence of a single department or agency. (Dictionary of Military and Associated Terms, Dept. of Defense (U), the Joint Chiefs of Staff, 3 Sep 74. (U)). (2) Intelligence produced by the CIA which bears on the broad aspects of United States national policy and national security. It is of concern to more than one department or agency. (Final Report, Senate Select Committee on Intelligence, 26 April 1976).

National Intelligence Estimate: A strategic estimate of capabilities, vulnerabilities, and probable courses of action of foreign nations which is produced at the national level as a composite of the views of the Intelligence Community. (Dictionary of Military and Associated Terms, Dept. of Defense (U), the Joint Chiefs of Staff, 3 Sep 74. (U)).

Operational intelligence: (1) Intelligence required for planning and executing all types of military operations. (2) Intelligence required to support the activities of intelligence agencies under the National Security Council. (Basic Cryptologic Glossary (U), NSA, 1971).

Physical security: (1) The component of security which results from all physical measures necessary to safeguard classified equipment and material from access by unauthorized persons. (Basic Cryptologic Glossary (U), NSA, 1971). (2) The component of COMSEC which results from all physical measures necessary to safeguard COMSEC material and information from access thereto or observation thereof by unauthorized persons. (Glossary of Communications Security and Emanations Security Terms (U), U.S. Communiactions Security Board, Oct 74). (3) The element of communications security that results from all physical measures necessary for safeguarding classified equipment, material, and documents from access or observation by unauthorized persons. (Communications-Electronics Terminology (U), U.S. Dept. of the Air Force, 15 Nov 73). (4) That part of security concerned with physical measures designed to safeguard personnel to prevent unauthorized access to equipment, facilities, material, and documents, and to safeguard them against espionage, sabotage, damage, and theft. See also communications security. (Dictionary of Military and Associated Terms, Dept. of Defense (U), the Joint Chiefs of Staff, 3 Sep 74).

Plain text: Unencrypted communications; specifically, the original message of a cryptogram, expressed in ordinary language. (Final Report, Senate Select Committee on Intelligence, 26 April 1976).

Political intelligence: Intelligence concerning foreign and domestic policies of governments and the activities of political movements. (Dictionary of Military and Associated Terms, Dept. of Defense (U), the Joint Chiefs of Staff, 3 Sep 74).

Processing: (1) The manipulation of collected raw information to make it usable in analysis to prepare for data storage or retrieval. (Final Report, Senate Select Committee on Intelligence, 26 April 1976). (2) Treatment of copy in accordance with predetermined and generalized criteria so as to produce all or some of the information contained in it in a new medium or a new form. (The main types of processing are conversion, scanning, extraction, digestion and diarization). (Basic Cryptologic Glossary (U), 1971). (3) Further handling, manipulation, consolidation, compositing, etc., of information to convert it from one format to another or to reduce it to manageable and/or intelligible information. (Communications-Electronics Terminology (U), U.S. Dept. of the Air Force, 15 Nov 73). (4) In photography, the operations necessary to produce negatives, diapositives or prints from exposed films, plates or paper. (Dictionary of Military and Associated Terms, Dept. of Defense (U), the Joint Chiefs of Staff, 3 Sep 74).

Production: (1) Intelligence product means the estimates, memoranda and other reports produced from the analysis of available information. (Executive Order No. 12036, 26 Jan 1978). (2) The preparation of reports based on an analysis of information to meet the needs of intelligence users (consumers) within and outside the Intelligence Community. (Final Report, Senate Select Committee on Intelligence, 26 April 1976).

Radiation intelligence: Intelligence derived from the collection and analysis of non-information bearing elements extracted from the electromagnetic energy unintentionally emanated by foreign devices, equipments, and systems excluding those generated by the detonation of automatic/nuclear weapons. (Dictionary of Military and Associated Terms, Dept. of Defense (U), the Joint Chiefs of Staff, 3 Sep 74).

Requirement: A general or specific request for intelligence information made by a member of the Intelligence Community. (Final Report, Senate Select Committee on Intelligence, 26 April 1976).

Scientific and technical intelligence: The product resulting from collection, evaluation, analysis and interpretation of foreign scientific and technical information which covers: A. Foreign developments in basic and applied research and in applied engineering techniques; and B. Scientific and technical characteristics, capabilities, and limitations of all foreign military systems, weapons, weapon systems and material. The research and development related thereto, and the production methods employed for their manufacture. (USSID 40, ELINT Operating Policy (U), NSA, 24 Oct 75).

Sensitive: Something which requires special protection from disclosure, which could cause embarrassment, compromise, or threat to the security of the sponsoring power. (Final Report, Senate Select Committee on Intelligence, 26 April 1976).

Sensitive compartmented information: The term as used in this manual is identified with its use in DCID 1/14. It is intended to include all information and material bearing special Intelligence Community controls indicating restricted handling within Community intelligence collection programs and their end products for which Community systems of compartmentation are formally established. The term does not include restricted data as defined in section 11, Atomic Energy Act of 1954, as amended. (Security of Compartmented Computer Operations (U), DIA, 14 Jan. 75).

Signal: (1) In electronics, any transmitted electric impulse which is of interest in the particular context; and (2) Anything intentionally transmitted by visual, acoustical, or electrical methods, which is intended to convey a meaning to the recipient. (Basic Cryptologic Glossary (U), NSA, 1971). (3) A visual, audible, electrical, or other indication used to convey information; and (4) the message or effect to be conveyed over a communication system. (Glossary of Machine Processing Terms (U), NSA (Office of Machine Processing), 1964). (5) Event, phenomenon or electrical quality that conveys information from one point to another; and (6) Operationally, a type of message that is conveyed or transmitted by visual, acoustical, or electric means. The text consists of one or more letters, words, characters, signal flags, visual displays, or special sounds with prearranged meanings. (Communications-Electronic Terminology (U), U.S. Dept. of the Air Force, 15 Nov. 73).

Signals intelligence (SIGINT): (1) A generic term which includes both communications intelligence (COMINT) and electronic intelligence (ELINT). (Glossary of Communications-Electronics Terms (U), NSA, 1971. (3) A generic term which includes both communintelligence and electronic intelligence, abbr. SIGINT. (SIGINT refers to the combination of COMINT and ELINT or to either when one of them is not specifically identified). (Basic Cryptologic Glossary

(U), NSA, 1971. (3) A generic term which includes both communication intelligence and electronic intelligence. Also called SIGINT. See also intelligence. (Dictionary of Military and Associated Terms, Dept. of Defense (U), the Joint Chiefs of Staff, 3 Sept. 74. (U)). (4) A category of intelligence information comprising all communications intelligence (COMINT), electronics intelligence (ELINT), and telemetry intelligence (TELINT). (Signals Intelligence (SIGINT) (U), DOD, 25 Jan. 73).

Source: (1) A person, thing, or activity which provides intelligence information. In clandestine activities, the term applies to an agent or asset, normally a foreign national, being used in an intelligence activity for intelligence purposes. In interrogations, it refers to a person who furnishes intelligence information with or without knowledge that the information is being used for intelligence purposes. (2) In interrogation activities, any person who furnished intelligence that the information is being used for intelligence purposes. In this context, a controlled source is in the employment or under the control of the intelligence activity and knows that this information is to be used for intelligence purposes. An uncontrolled source is a voluntary contributor of information and may or may not know that the information is to be used for intelligence purposes. (Dictionary of Military and Associated Terms, Dept. of Defense (U), the Joint Chiefs of Staff, 3 Sept. 74. (U)).

Special intelligence communications, (SPINTCOMM): SPINTCOMM was established by Secretary of Defense Memorandum, dated 4 November 1964. It consists of those communications facilities under the operational and technical control of the chief of intelligence of each of the military departments and under the management of the Defense Intelligence Agency. (Defense Special Security Communications System (DSSCS) Operating Instructions System/Data Procedures (U), NSA, 8 Oct. 75).

Special sensor: Equipment on instrumented platforms and in installations designed to collect measurement and signature data that can be further processed into data usable by intelligence analysts. (Defense Intelligence Collection Requirements Manual DIA, 27 Jan. 75).

Tactical intelligence: Intelligence which is required for the planning and conduct of tactical operations. Essentially tactical intelligence and strategic intelligence differ only in scope, point of view and level of employment. (Dictionary of Military and Associated Terms, Dept. of Defense (U), the Joint Chiefs of Staff, 3 Sept. 74. (U)).

APPENDIX C—INDEX OF OTHER INTELLIGENCE GLOSSARIES

(Other publications, many of which contain classified information, also contain definitions of intelligence terms. An index of some of these publications appears below.)

Acquisition and Storage of Information Converning Non-Affiliated Persons and Organizations. Army Regulation 380-13. September 1974.

ADP Security Manual, Techniques and Procedures for Implementing Deactivating, Testing, and Evaluating Secure Resource-Sharing ADP Systems. DoD. January 1973.

Basic Cryptologic Glossary. NSA. 1971.

Charter of DCI SIGINT Committee, DCID No. 6/1, May 1976.

Classification and Declassification of National Security Information and Material. Executive Order No. 11652. March 1972 and as amended.
Combat Intelligence. Army Field Manual 30–5. October 1973.
Communications-Electronics Terminology Handbook. Public Affairs Press. 1965.
Communications-Electronics Terminology, U.S. Dept. of the Air Force. November 1973.
Communications Glossary, Range Commanders Council, White Sands Missile Range. March 1966.
Communications Security. Army Regulation 530–2. March 1976.
Control of Compromising Emanations. Army Regulation 530–4. June 1971.
Coordination of U.S. Clandestine Foreign Intelligence and Activities Abroad, DCID No. 5/1. May 1976.
Coordination of U.S. Clandestine Foreign Intelligence and Counterintelligence Liaison, DCID No. 5/2. May 1976.
Counterintelligence Operations. Army Field Manual 30–17. January 1972.
Counterintelligence Special Operations. Army Field Manual 30–17A February 1973.
DCI Policy or Release of Foreign Intelligence to Contractors, DCID No. 1/7. May 1976.
DoD Human Resource Intelligence Collection Implementation Plan. 1966.
Data Standardization for the Intelligence Community, DCID No. 1/5. May 1976.
Defector Program, The, NSCID No. 4. February 1972.
Defector Program Abroad, The, DCID No. 4/2. May 1976.
Defense Intelligence Collection Requirements Manual, DIA. January 1975.
Defense Special Security Communications System (DSSCS) Operating Instructions System/Data Procedures. NSA. October 1975.
Definitions of Search and Analysis Terms, Appendix D to "Selected Electronic Emitters for Target Countries," June 1964.
Department of the Army Supplement to DoD 5200.1–R. Army Regulation 38–05. July 1974.
Dictionary of Military and Associated Terms. JCS Pub. 1. September 1974.
Dictionary of Telecommunications. 1970.
Dictionary of United States Army Terms. Army Regulation 310–25. June 1972.
Domestic Exploitation Program. Army Regulation 381–15. July 1974.
Electronic Security. Army Regulation 530–3. June 1971.
Electronic Warfare. Army Regulation 105–87. August 1976.
ELINT Operating Policy. USSID 40. October 1975.
ELINT Collection Analysis Guide, National Cryptologic School. 1965.
Enemy Prisoners of War, Civilian Internees, and Detained Persons. Army Field Manual 19–40. February 1976.
Engineer Intelligence. Army Field Manual 5–30. September 1967.
Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities, United States Senate,

Together with Additional Supplemental and Separate Views. April 1976.
Foreign Intelligence Production, NSCID No. 3. February 1972.
Glossary of Basic TA Terminology, National Cryptologic School. 1969.
Glossary of Communications-Electronics Terms. December 1974.
Glossary of Communications Security and Emanations Security Terms. U.S. Communications and Security Board. October 1974.
Glossary for Computer Systems Security, National Bureau of Standards. February 1976.
Glossary of Machine Processing Terms. September 1964.
Handling of Critical Information, DCID No. 7/1. May 1976.
House Resolution 658. (Establishes House Permanent Select Committee on Intelligence). November 1977.
IDHS Glossary of Common Acronyms, Codes, Abbreviations, and Terms Used in Dept. of Defense Intelligence Data Handling Systems (IDHS) Documents. 1970.
Information Security Regulation. DoD 5200.1–R.
Intelligence Collection Operations. Army Field Manual 30–18. November 1973.
Intelligence Cover and Operational Support Activities. Army Regulation 381–102. November 1973.
Intelligence Interrogation. Army Field Manual 30–15. June 1973.
Intelligence Support. Army Regulation 381–19. March 1977.
Limitations and Procedures in Signals Intelligence Operations of the USSS. USSID 18. May 1976.
List of Terminology Used in Foreign Counterintelligence and Counterespionage Investigations. December 1973.
Meteorological Support for the U.S. Army. Army Regulation 115–10. June 1970.
Military Geographic Intelligence (Terrain). Army Field Manual 30–10. March 1972.
Military Intelligence Officer Excepted Career Program. Army Regulation 614–115. January 1975.
Military Intelligence Organizations. Army Field Manual 30–9. October 1973.
Modern Data Communications Concepts, Language and Media. Wm. P. Davenport, Hayden Book Co., Inc. 1971.
National Foreign Intelligence Plan for Human Resources. NFIB D/27.7/5. 1977.
NATO Glossary of Terms and Definitions for Military Use (AAP–6).
National SIGINT Requirements System Handbook. December 1976.
Naval Intelligence System Architectural Management Plan for 1978 (NISAM–78) (Draft).
Offensive CI Operations (OFCO). Army Regulation 381–47. April 1976.
Operations. Army Field Manual 100–5. July 1976.
Operations Security. Army Regulation 530–1. May 1976.
Physical Security. Army Field Manual 19–30. November 1977.
Point Weather Warning Dissemination. Army Regulation 115–1. February 1975.
Security Committee, DCID No. 1/11. May 1976.

Security, Use and Dissemination of Communications Intelligence, The. Army Regulation 380–35. March 1973.
Security, Use and Dissemination of Communications Intelligence, The DoD Directive S–5200.17 (M–2).
Security, Use and Dissemination of Communications Intelligence, The. USAFINTEL 201–1.
Senate Resolution 400. (Establishes the Senate Select Committee on Intelligence). June 1977.
SIGINT Security, NSA. USSID 3. August 1972.
Signals Intelligence, NSCID No. 6. February 1972.
Signal Intelligence (SIGINT). Army Field Manual 30–21. August 1975.
Signals Intelligence. DoD Directive S–3115.7.
SIGSEC Techniques. Army Manual 32–6. February 1977.
Soviet Naval Threat Circa 2000, The. August 1976.
Special Security Officer System, The. Army Regulation 380–28. October 1971.
Statement of Intelligence Interest. DoD Document No. 05990.
Surveillance, Target Acquisition and Night Observation (STANO) Operations. Army Field Manual 31–100. May 1971.
Technical Intelligence. Army Fied Manual 30–16. August 1972.
Telemetry Terminology, Missile Intelligence Agency, Huntsville, Alabama. January 1975.
Threat Analysis. Army Regulation 381–11. August 1974.
Title Classified. DCID No. 6/2. May 1976.
Title Classified. DoD Directive TS–500.12 (M–1).
Title Classified (USAFINTEL 201–4).
United States Air Force Dictionary, Woodford Agee Heflin (Editor), Research-Studies Institute, Air University Press, Maxwell Air Force Base, Alabama 1956.
United States Intelligence Activities. Executive Order No. 12036. January 1978.
U.S. Air Force Glossary of Standardized Terms. (Air Force Manual 11–1).
U.S. Army Requirements for Weather Service Support. Army Regulation 115–12. August 1976.
U.S. Clandestine Foreign Intelligence and Counterintelligence Activities Abroad, NSCID No. 5. February 1972.