Approved For Release 2002/08/21 : CIA-RDP80B01676R000800070019-9 61-8759

NOV 1961

MEMORANDUM FOR: The President's Foreign Intelligence Advisory Board

SUBJECT : Safeguarding Intelligence and Intelligence Sources and Methods (Recommendation No. 20 of the October 4, 1961 Report to the President by the President's Foreign Intelligence Advisory Board)

REFERENCE : Memorandum from The Special Assistant to the President dated 11 October 1961 subject as above.

In accordance with the recommendation of the President's Foreign Intelligence Advisory Board which was approved by the President, I am submitting this report on actions taken to implement Section 102 (d) (3) of the National Security Act and Section 5 of the National Security Council Directive No. 1 relating to the protection of intelligence and intelligence sources and methods.

The information requested is set forth in four sections, namely:

a. Legal Authority of the Director of Central Intelligence for Protection of Intelligence and Intelligence Sources and Methods.

b. Actions and Programs of CIA for Protection of Intelligence and Intelligence Sources and Methods.

c. Actions and Programs of USIB for Protection of Intelligence and Intelligence Sources and Methods.

d. Actions and Programs of the Clandestine Services for the Protection of Intelligence and Intelligence Sources and Methods.

Approved For Release 2002/08/21 : CIA-RDP80B01676R000800070019-9

ER

Approved For Release 2002/08/21 : CIA-RDP80B01676R000800070019-9

Legal Authority of the Director of Central Intelligence for Protection of Intelligence and Intelligence Sources and Methods.

The first formal assignment of responsibility for protecting intelligence sources and methods is contained in paragraph 10 of the Presidential Directive of January 22, 1946 which established the National Intelligence Authority and the Central Intelligence Group. This sentence reads, "In the conduct of their activities the National Intelligence Authority and the Director of Central Intelligence shall be responsible for fully protecting intelligence sources and methods." This provision was the result of discussions during the drafting of this directive in which the military intelligence agencies expressed concern because their intelligence material would be acquired and retained by the new Central Intelligence Group. Recognizing that the controls they had established within their agencies would not be binding on the Central Intelligence Group, they wished to assure that the Group (and the National Intelligence Authority) would be responsible for protecting their sources and methods. The Directive as worded, embraces all aspects of intelligence sources and methods including the military intelligence agencies.

In the National Security Act of 1947, the third proviso of 102 (d) (3) reads, "... That the Director of Central Intelligence shall be responsible for protecting intelligence sources and methods from unauthorized disclosure." There is no record of any congressional debate of this proviso or of any legislative history, and there is, therefore, no qualification of this broad assignment of responsibility. The addition of the words "from unauthorized disclosure" carries an implication which is even broader than the wording of the Presidential Directive. It should be noted, however, that the first proviso of the same section of the National Security Act provides, "... That the Agency shall have no police, subpoena, law-enforcement powers, or internal-security functions" and the Presidential Directive had similar language. It would appear, therefore, that in carrying out this responsibility the Director is limited to the development of policies and procedures designed to afford the required protection and to such investigations into the procedures and their administration as fall short of police or actual internal-security functions. Within the Agency, the Director has his administrative authorities to enforce his controls, but he has no such direct authority throughout the rest ofthe intelligence community or over other recipients of the intelligence product.

Approved For Release 2002/08/21 : CIA-RDP80B01676R000800070019-9

SECRET
Approved For Release 2002/08/21 : CIA-RDP80B01676R000800070019-9

Actions and Programs of CIA for Protection of Intelligence and Intelligence Sources and Methods.

1. Information Controls.

It is the general policy of the Central Intelligence Agency to disseminate CIA produced intelligence and intelligence information only to those departments and agencies of the U. S. Government which, in the interests of national security, have a need for such information. Those departments and agencies in turn are expected to disseminate such information only to those employees within their jurisdiction who have a "need to know" and who are appropriately cleared.

Within CIA the dissemination of both CIA produced intelligence and that intelligence received from other departments and agencies is carefully controlled to ensure that only those officials and employees who require the information in the performance of their duties are authorized access. The dissemination of intelligence is under constant review by originators, supervisors and dissemination control points to ensure that the principle of "need to know" is properly exercised in the protection of intelligence sources and methods.

A principal factor in the protection of information is the establishment of compartmentation of both information and activities. This is accomplished by organizational structure, special channels and criteria for the handling and dissemination of information and creation of covert project mechanisms for the collection and exploitation of sensitive intelligence. The information flowing through these systems is subject to extra controls by markings, control points, custody and storage, clearance of personnel having access and continuous monitoring and frequent review to ensure the adequacy of the protective measures.

In the field of intelligence operations elaborate measures are taken to ensure the protection of the identity of covert personnel, projects and activities in any form of communication concerning these operations. Pseudonyms, cryptonyms, aliases and other concealing devices are utilized to protect intelligence sources and methods and to render any communication that may fall into unauthorized hands relatively meaningless.

Approved For Release 2002/08/21 : CIA-RDP80B01676R000800070019-9

Approved For Release 2002/08/21 : CIA-RDP80B01676R000800070019-9

A key factor in the protection of intelligence and intelligence sources and methods is the physical security program employed to protect CIA buildings and installations both in the United States and overseas. The provisions of Executive Order 10501 are carefully followed and supplemented to meet the special security protective requirements deemed necessary for Agency interests. CIA buildings are under 24 hour guard. Employees are admitted on presentation of photographic identification badges. Visitors are admitted only on official business and always under escort. All classified material is strictly controlled, is stored in safes, vaults or secure areas and is never left unattended. There are continuous security inspections to ensure that the protection of classified intelligence is properly maintained and that there are no inadequacies in our physical security program. Any security violation is promptly dealt with, and our regulations establish disciplinary action to be taken.

The Agency is seriously concerned with the possible technical penetration of Agency facilities which might result in a compromise of intelligence and Agency activities. An active program of audio countermeasure inspections and capabilities has been developed to nullify this threat.

In regard to the above measures designed to protect Agency information and activities, there is the fullest degree of cooperation between all components of the Agency and the Security Office. Any incident or information that indicates there is a possible penetration, an unauthorized disclosure, a loss or theft of property or intelligence documents results in an immediate investigation. The full assets of the Security Office and the Agency are employed to resolve the issue. Frequently, the indication of a possible compromise of information concerns intelligence which has been disseminated to other departments and agencies. Through security liaison channels the investigation is often extended to the other departments concerned and the other services respond with the fullest cooperation. This frequently results in a joint investigative effort. In this manner the Agency exercises its constant concern over the protection of intelligence and vigorously pursues any indication of a weakness in its protective system.

Approved For Release 2002/08/21 : CIA-RDP80B01676R000800070019-9

Approved For Release 2002/08/21 : CIA-RDP80B01676R000800070019-9

2. Personnel Security.

a. Policy: From its inception the Agency has recognized that a primary factor in the protection of intelligence is the security reliability of intelligence personnel having access to intelligence information. To this end, the Agency has established its policy to accept for employment only those individuals who are of excellent character, unquestioned loyalty, integrity, discretion and trustworthiness. Employment of individuals must be clearly consistent with the interests of the national security. All positions occupied by staff employees are designated as "sensitive" under Executive Order 10450.

b. Clearance Procedures: Security investigation of an applicant is conducted by CIA. Such investigation encompasses a verification of the applicant's claimed employment, education, references and residences. In addition, a check of appropriate Federal, state and local records is conducted. The investigation conducted exceeds the minimum standards for Federal employment as set forth in Executive Order 10450. The results of each security investigation are evaluated by professional security personnel and a determination is made as to the suitability or non-suitability of individuals for employment. In those cases where a person is determined not suitable, such cases are personally reviewed by the Director of Security who makes a final determination.

As part of the security investigation, applicants, upon entrance on duty, are accorded a polygraph interview in order to verify pertinent security factors developed during investigation and to establish the applicants' acceptability under Agency criteria.

In addition, in order to determine the suitability of an applicant for employment, each applicant is required to undergo a medical and psychiatric examination.

c. Security Review: Whenever personnel actions are taken which effect a change of an employee's status, a security review is conducted. This would include cases of assignment overseas, change in marital status, marriage to aliens and similar happenings. The Director of Central Intelligence is briefed by the Director of Security on any problem cases so that he will be apprised continually on the status of the Agency's security program.

Approved For Release 2002/08/21 : CIA-RDP80B01676R000800070019-9

Approved For Release 2002/08/21 : CIA-RDP80B01676R000800070019-9

d. Reinvestigation: In order to ensure that employees continue to meet the suitability criteria for employment, a security reinvestigation program is conducted on a five year cycle. As part of this reinvestigation each employee may be afforded a polygraph examination to ensure that classified information has not been divulged to unauthorized persons.

e. Employee Outside Activities: To ensure that Agency personnel do not jeopardize their official assignment or inadvertently disclose classified Agency material, there are limitations placed on the outside activities of Agency personnel. For example, all writings for publication or speeches whether they involve intelligence or not require prior security approval; private employment and memberships in organizations must be approved in advance by security, and advance security approval is required for all private foreign travel for which complete itineraries must be submitted and appropriate security briefings given.

3. Security Officers Assignment.

Professional career Security Officers are assigned to stations and bases overseas and domestic projects, installations and components in every case where professional security support is indicated as necessary. The Security Officer is under the direction of the Chief of Station or Base and is responsible for ensuring the security protection of personnel and physical assets of the Agency. To this end, Security Officers are thoroughly trained in all phases of security and are capable of acting with a minimum of guidance from Headquarters.

4. Briefing of Persons Assigned Overseas.

Personnel prior to overseas assignments are security briefed as to the nature and extent of the local hostile threat which may exist against U. S. installations and personnel, and actions they must take if they feel they are a target of the opposition. Personnel are also thoroughly briefed as to hostile penetration and surveillance techniques, risk of capture possibilities and resistance techniques to hostile interrogations. Also included are counteraudio demonstrations and protective measures to be employed. Upon arrival at the overseas station or base, the employee is given additional briefings on local security, cover, operations and personal conduct factors.

Approved For Release 2002/08/21 : CIA-RDP80B01676R000800070019-9

Approved For Release 2002/08/21 : CIA-RDP80B01676R000800070019-9

5. Security Coordination.

In regard to our constant concern over the possible penetration of the Agency, every incident, report, suspicion or other element which indicates a possible penetration is the subject of an immediate and specialized investigation. In such instances our full resources are employed to resolve the problem. The Director of Central Intelligence is kept fully informed by the Security officials of incidents of this nature and the Director of Central Intelligence follows them to their ultimate conclusion. The flow of security information pertaining to our employees is enhanced by the closest coordination of our Security Office with other security components of the Government. Within the Agency there is full coordination between the Security and Counterintelligence components for the fullest development of any indication of possible penetration. This extends to the joint working relationships with friendly foreign intelligence and security services for the mutual development of security information and the exploitation of investigative leads. The Director of Central Intelligence feels that only through the full coordination of professional personnel in these fields can the threat to intelligence sources and methods be properly contained.

Actions and Programs of USIB for Protection of Intelligence and Intelligence Sources and Methods.

Security Committee of USIB

1. Established.

The Security Committee was established on March 24, 1959, as a standing Committee of the USIB for the purpose of advising, assisting and making recommendations to the Board for the development and review of security standards as they relate to the protection of intelligence and of intelligence sources and methods from unauthorized disclosure. Further, the Committee is to advise and assist the DCI in the exercise of his responsibilities to investigate unauthorized disclosures of intelligence and of intelligence sources and methods.

2. Investigation of Unauthorized Disclosures.

The Committee has investigated seven reported unauthorized disclosures of classified intelligence. In each instance, the Committee has initiated a review of classified intelligence documents to determine upon which classified report the information was based. Concurrently, as a part of the investigative action, the Committee initiated a review of previously published overt publications to determine whether or not the information may have appeared previously in the overt press.

Approved For Release 2002/08/21 : CIA-RDP80B01676R000800070019-9

Approved For Release 2002/08/21 : CIA-RDP80B01676R000800070019-9

In one instance, an ad hoc investigative working group comprised of investigative representatives from the USIB agencies and departments conducted for more than a year an extensive investigation of an unauthorized disclosure of highly classified intelligence information. The ad hoc investigative working group exchanged investigative leads and utilized other techniques to avoid duplicative investigation and to ensure thorough coverage.

3. President's Directive on "Disclosure of Classified Intelligence" of 23 May 1960.

The Presidential Directive was recommended by the Security Committee as a result of extensive inquiries into reported unauthorized disclosures. The Directive called for a review of existing procedures for the control of classified intelligence and for corrective action to be taken where there is undue reliance upon routine administrative methods for control or where other inadequacies are found. The responsibility of the intelligence chief was established to assess the risk to intelligence sources and methods in each instance where classified information was proposed for release outside of authorized channels.

An Agreed Guidance paper for implementing the Presidential Directive was approved by the Board on 29 June 1960. This guidance set forth as appropriate uniform practices and procedures for the control of classified intelligence with special references to sensitive intelligence. At this time, a new marking "WARNING NOTICE - SENSITIVE SOURCES AND METHODS INVOLVED" was introduced which would clearly identify such information as sensitive and requiring special controls and a severely limited distribution. Each department and agency within the intelligence community caused a review to be made of its existing practices and procedures. In certain instances, this resulted in the revision of existing departmental regulations to ensure the better protection of sensitive intelligence.

A report of the action taken by the departments and agencies to implement the President's Directive was forwarded to the Special Assistant to the President on 4 November 1960.

4. Personnel Security Procedures as of 1 July 1960 for Intelligence Personnel of USIB Member Agencies and Recommendation to Improve Standards of Personnel Security.

As a result of the defection of the two NSA employees and at the request of high authority, the Director of Central Intelligence on 7 September 1960

Approved For Release 2002/08/21 : CIA-RDP80B01676R000800070019-9

Approved For Release 2002/08/21 : CIA-RDP80B01676R000800070019-9

directed the Security Committee to outline personnel security procedures implementing Executive Order 10450 as of 1 July 1960 for those personnel engaged in or having access to classified foreign intelligence information and materials. The Director of Central Intelligence also directed the Security Committee to consider and submit recommendations as to new or improved measures to effect overall improvement of the standards of personnel security.

The Committee reviewed existing personnel security procedures and its report dated 14 September 1960 was noted by the Board on 27 September 1960. The Committee in a separate report recommended to the Board proposed legislation as follows: (a) establish injunctive authority to enjoin acts which constitute an unauthorized disclosure; (b) establish an Official Secrets Act designed to overcome certain limitations in present espionage statutes; and (c) grant to those departments and agencies desiring it, similar statutory discretionary authority as given the Director of Central Intelligence to dismiss employees. The Committee also recommended that consideration be given to expand the number of positions designated as sensitive under Executive Order 10450.

The Board appointed an ad hoc group of legal and security representatives to review existing legislation and to recommend proposals in accordance with the Committee's recommendations. The Legislative Drafting Group of this ad hoc subcommittee completed its work on 2 November and the full committee will meet to prepare its final report and recommendations within the next two weeks.

5. <u>Revision of DCID 11/2, "Control of Dissemination and Use of Intelligence and Intelligence Information."</u>

The revision of DCID 11/2 is before the USIB to achieve uniformity and mutual understanding for the control of dissemination and use of intelligence and intelligence information. The Committee initiated an extensive and detailed review of existing practices within the community for the control of dissemination and use of intelligence and intelligence information. The Committee also considered in detail dissemination practices of intelligence both within the intelligence community and to other agencies and departments.

The paramount consideration in the revision of DCID 11/2 was the protection of intelligence sources and methods. The Committee introduced a new technique of dissemination and use of intelligence whereby sensitive intelligence would be adequately protected and whereby intelligence of a nonsensitive nature could be utilized to the fullest extent practicable without reference to originating agencies.

Approved For Release 2002/08/21 : CIA-RDP80B01676R000800070019-9

25X1

Approved For Release 2002/08/21 : CIA-RDP80B01676R000800070019-9

Next 1 Page(s) In Document Exempt

Approved For Release 2002/08/21 : CIA-RDP80B01676R000800070019-9

Approved For Release 2002/08/21 : CIA-RDP80B01676R000800070019-9

DISTRIBUTION:
Orig. and 1 - Addressee
1 - Spec. Ass't. to the President
1 - DCI
1 - DDCI
1 - Exec. Reg. ✓ (~~[illegible]~~)
2 - DDS
1 - DDI
1 - DDP
1 - IG
1 - AC/DCI
1 - Exec. Sec. USIB
1 - OGC
1 - OS w/basic

25X1 OS/D/[redacted] 30 Oct 61)

Approved For Release 2002/08/21 : CIA-RDP80B01676R000800070019-9