22 April 1975

MEMORANDUM FOR [redacted]

SUBJECT: DCID 1/11, Security Committee,Effective 28 AUgust 1974

1. Hank Knoche reports that the Rockefeller Commission has expressed some concern about the wording of DCID 1/11 on the ground that it is so worded that it might constitute a "hunting license" to conduct investigations.

2. Will you ~~please~~ please provide me, for Mr. Knoche, a copy of DCID 1/11 ~~and~~ and a memorandum which he can use as a talking paper to respond to the concern expressed by the Commission.

3. I have no indication as to any specifics of this concern, but if you feel there are any sentences or paragraphs which might be tightened to improve the DCID you might include that in your memorandum.

4, The Commission's role as you know, is focused entirely on domestic aspects of the operation of the Intelligence Community.

[redacted]

(b)(3)

[redacted]

DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE NO. 1/11[1]

SECURITY COMMITTEE

(Effective 23 August 1974)

In support of the DCI's statutory responsibilities and of his efforts to improve the Intelligence Community's product and to achieve more efficient use of intelligence resources, the community's security policies and procedures must be effective and consistent for the protection of intelligence and of intelligence sources and methods,[2] and must ensure timeliness and economy in the handling of compartmented information. Therefore, pursuant to provisions of Subsection 102 (d) of the National Security Act of 1947, as amended, to provisions of NSCID 1 and to paragraph 2.b of NSAM 317, a new standing Committee of the USIB is hereby established.

1. *Name of the Committee*

The committee will be known as the Security Committee.

2. *Mission*

The mission of the committee is to provide the means by which the Director of Central Intelligence, with the advice of United States Intelligence Board principals, can:

a. Ensure establishment of security policies and procedures including recommendations for legislation for the protection of intelligence and intelligence sources and methods from unauthorized disclosure.

b. Review and formulate personnel, physical and document security policies, standards and practices and dissemination procedures applicable to all government departments and agencies as such policies, standards, practices and procedures relate to the protection of intelligence

[1] Supersedes DCID 1/11, effective 23 April 1965 and DCID 1/12 effective 23 December 1964.

[2] The term intelligence as used in this document applies only to information covered by statute, Executive Order, or other authority consonant with the DCI's statutory responsibility for foreign intelligence and for the protection of intelligence and intelligence sources and methods from unauthorized disclosure.

~~SECRET~~
CONTROLLED DISSEM

Copy No. 291

of these investigations to the Director of Central Intelligence, through the United States Intelligence Board. Such reports will (1) assess the disclosure's impact on the U.S. intelligence process, and its implications for national security and foreign relations, (2) describe corrective measures taken or needed to prevent such disclosures in the future or to minimize the adverse effects of the case at hand, and (3) recommend any appropriate additional actions.

d. The functions of the committee as they relate to technical surveillance countermeasures, computer security and special security compartmentation are set forth in attachments 1, 2, and 3.

4. *Community Responsibilities*

a. Upon request of the committee chairman, USIB departments and agencies shall furnish to the committee within established security safeguards particular information needed by the committee and pertinent to its functions. Temporary material and ad hoc personnel support will be provided to the committee as needed and as mutually agreed upon by the departments and agencies represented on the committee.

b. Each USIB principal is responsible for investigation of any unauthorized disclosure or compromise of intelligence or intelligence sources and methods occurring within his department or agency. When investigation determines that the possibility of compromise cannot be discounted, and the interests of the USIB or another USIB principal are involved or affected, the results of investigation will be forwarded to the Security Committee for review and possible remedial action as determined appropriate by the committee.

5. *Composition and Organization*

a. The committee will consist of a full-time chairman designated by the DCI, representatives of the chiefs of departments and agencies who are members of the USIB, and the representatives of the Departments of the Army, Navy, and Air Force. The chairman may invite a representative of the chief of any other department or agency having functions related to matters being considered by the committee to sit with the committee whenever matters within the purview of that department or agency are to be discussed.

b. The committee will be supported by permanent subcommittees for technical surveillance countermeasures, for special security compartmentation, and for computer security, and by other subcommittees as needed and as approved by the DCI and by ad hoc working groups as approved by the chairman. The chairman of subcommittees will be designated by the committee chairman with the concurrence of the DCI. Membership on the subcommittees and ad hoc working groups need not be limited to member agencies of the committee, but may be

Copy No 291

DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE NO. 1/11

(Attachment 1)

Technical Surveillance Countermeasures

The functions of the Security Committee include:

A. With respect to general technical surveillance countermeasures:

(1) To facilitate the formulation, development and application of effective countermeasures equipment and techniques based on assessments by the Central Intelligence Agency and other knowledgeable member agencies of USIB of (a) the state of the art of audio surveillance equipment, and (b) the known and estimated technical surveillance capabilities of foreign governments.

(2) To formulate and recommend to the DCI resource programming objectives for USIB departments and agencies in the field of technical surveillance countermeasures in consideration of current and foreseen threats and with regard for the effective and efficient use of resources.

(3) To coordinate all aspects of the U.S. Government effort in defense against technical surveillance penetration and to resolve conflicts that may arise in connection therewith.

(4) To facilitate the interchange of information in the field of technical surveillance countermeasures among USIB departments and agencies and others as appropriate, particularly by the preparation, publication and dissemination of appropriate reports, notices and guides.

(5) To recommend policies governing disclosures concerning technical surveillance devices (except as otherwise provided for under NSCID No. 5), or countermeasures thereto, to be made to foreign governments or international organizations in which the U.S. Government participates.

(6) To advise USIB department and agencies of technical surveillance countermeasures objectives and standards to be considered in connection with existing or new facilities abroad.

(7) To prepare damage assessments by furnishing reports of known or suspected hostile audio surveillance penetrations of U.S. facilities and recommending remedial or other actions as appropriate.

Copy No 291

DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE NO. 1/11

(Attachment 2)

Computer Security

The functions of the Security Committee include:

(1) To review, formulate and recommend to the DCI policies, standards, and procedures to protect intelligence data stored or processed by computer.

(2) To advise and assist the DCI, the Intelligence Community Staff, Committees of the United States Intelligence Board, USIB member agencies and departments, and other intelligence users with respect to all computer security issues and to resolve conflicts that may arise in connection therewith.

(3) To formulate and recommend to the DCI resource programming objectives for USIB departments and agencies in the field of computer security in consideration of current and foreseen vulnerabilities and threats and with regard for the effective and efficient use of resources; to foster and to monitor an aggressive program of computer security research and development in the Intelligence Community in order to avoid unwarranted duplication and to assure the pursuit of an effective effort at resolving technical problems associated with the protection of computer operations.

(4) To coordinate all aspects of Intelligence Community efforts in defense against hostile penetration of Community computer systems as feasible to support other Government and national efforts aimed at improving computer security technology; to foster a coordinated program of Intelligence Community computer security training and indoctrination.

(5) To facilitate within the Intelligence Community the exchange of information relating to computer security threats, vulnerabilities, and countermeasures by providing a focal point for the evaluation of foreign intentions and capabilities to exploit Community computer operations, for central notification of hostile exploitation attempts, for the preparation of damage assessments of incidents of foreign exploitation of intelligence computer operations, and for the formulation of Community policy on the release of computer security information to foreign governments and international organizations.

Copy No. 291

DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE NO. 1/11

(Attachment 3)

Compartmentation [1]

The functions of the Security Committee as they relate to compartmentation controls are: [2]

A. To develop and recommend to the DCI, with the advice of the United States Intelligence Board, technical guidance for the establishment, maintenance and improvement of coordinated compartmentation systems.

(1) Providing special protection to sensitive intelligence, intelligence information and intelligence sources and methods under the authority of Section 9 of Executive Order 11652.

(2) Ensuring the establishment and disestablishment of compartmentation of intelligence and intelligence information on the instructions of the DCI.

(3) Ensuring coherent control by the DCI of the processes for access approvals to compartmented intelligence and intelligence information and of the processes for dissemination, sanitization or release of such intelligence information.

(4) Ensuring the establishment and promulgation or appropriate criteria for security and need-to-know access approvals.

B. To formulate, coordinate, maintain and promulgate technical guidance for use in the administration of compartmentation controls at all echelons of department and agency domestic and overseas activity, including consultants and contractor support activity concerning:

(1) Access approval criteria and employment in hazardous duty areas.

(2) Physical Security.

---

[1] The term "compartmentation" as used in this directive refers to the system whereby special Intelligence Community controls indicating restricted handling within collection programs and their end products are applied to certain types of intelligence information and material. The term does not include Restricted Data as defined in Section 11, Atomic Energy Act of 1954, as amended.

[2] In the conduct of these functions, the Committee will recognize the special requirements of individual compartmented collection programs operated on an executive agent basis, particularly those which involve hazardous activities.

Copy No. 291