15 OCT 1979

PTOS did not make any new comments - had commented previously as stated in our memo. Package was discussed with [redacted] STAT provided numerous documents which were reviewed by he and [redacted] before STAT preparing our final answer. Nothing in writing from PTOS.

Pink sheets from PSI are attached.

[redacted] STAT

BASIC

ROUTING AND RECORD SHEET

SUBJECT: (Optional)

STAT The APEX Special Access Control System

DS REGISTRY
*FILE Security 18

FROM:
[redacted]
C/PPG
4E70 Hqs

EXTENSION

NO.

DATE
4 Oct 79

STAT

TO: (Officer designation, room number, and building)	DATE RECEIVED	DATE FORWARDED	OFFICER'S INITIALS	COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.)
C/OPS/PSI				
1. DD/PSI 4E58 Hqs	12 OCT 1979	10/12		For review and comment by 12 Oct 1979.
2.				
3. C/CO — for action + return to DD/PSI with appropriate Comment By Debra	10/11/79			
4.				
5.				[redacted] and I have reviewed the draft and we have no pertinent comments. C/CO 10/11/79
6. C/OPS/PSI	10/11	10/11		
7. DD/PSI — FYI	10/12			
8. C/PPG — for action				
9.				
10.				NO PSI OBJECTIONS — WOULD LIKE TO RETAIN COPY FOR REFERENCE PURPOSES.
11.				
12.				
13.				[redacted] C/OPS/PSI 10/11/79
14.				
15.				

FORM 1-79 610 USE PREVIOUS EDITIONS

OS REGISTRY

FILE Security 1-18

REFERENCE

ROUTING AND RECORD SHEET

SUBJECT: (Optional) Draft - The APEX Special Acess Control System

FROM: STAT
Acting Executive Officer/DDA

EXTENSION

NO. DD/A 79-3178

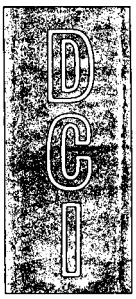
DATE 4 OCT 79

TO: (Officer designation, room number, and building)	DATE RECEIVED	DATE FORWARDED	OFFICER'S INITIALS	COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.)
1. Director of Security				Forwarded herewith are draft copies of manuals for industry and government under the proposed APEX special access control system. Would you review these drafts and foward any suggestions you may have regarding corrections, additions or deletions to [redacted] RES/NFAC, STAT Rm 3E58 by 10 October. This may be the last shot we will get to the modifications of these proposals so it is important that we look at them carefully. It is my understanding that the Office of Security has already been provided an additional 5 sets of these drafts. [redacted] STAT A-EO/DDA cc: D/OS D/OC D/OL C/RMD w/Atts
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				

OS-9-2481

FORM 1-79 610 USE PREVIOUS EDITIONS

Confidential



DIRECTOR
OF
CENTRAL
INTELLIGENCE

DRAFT

A Security Manual for Government

The APEX Special Access Control System

Confidential

May 1979

Copy 114

National Security Information Unauthorized Disclosure Subject to Criminal Sanctions

25X1

Approved For Release 2005/07/12 : CIA-RDP85T00788R000100050002-7

Contents

Appendixes

The APEX Special Access Control System

I. Introduction

This manual describes the Special Access Security Control System known as APEX. This system was established to control Special Access Programs within the category of national security information called National Foreign Intelligence.

Certain terms used in this system are unclassified when standing alone or not connected to the intelligence activities or intelligence information they designate. These terms are: APEX; the APEX Security Control System; the codewords which identify the categories of intelligence product within the system (that is, COMINT, HUMINT, IMAGERY, and TECHNICAL) and the especially sensitive material designators in the ROYAL category. The codewords which identify highly sensitive collection projects may be used outside the APEX control system but must be protected by the standard classification level of CONFIDENTIAL.

Existing directives and regulations governing the protection and control of Sensitive Compartmented Information (SCI) will be either superseded or revised, if necessary, to be in accordance with this manual. The manual is not, however, intended to intrude on the activity of Executive Agents or other operational program directors who have been delegated specific authority for dissemination of intelligence to foreign governments. They will continue to prescribe basic operational direction and classification guidance.

II. Authority

The authority for the DCI to establish the security policy as set forth in this manual is provided in Section 102(d) of the National Security Act of 1947, which states that the DCI is responsible for protecting intelligence sources and methods from unauthorized disclosure; and in Executive Order 12036, Section 1-6, which requires the DCI to ensure the establishment by the Intelligence Community of common security and access standards for managing and handling foreign intelligence systems, information, and products. Section 4-201 of EO 12065 recognizes the need to establish Special Access Programs to control access, distribution, and protection of particularly sensitive classified information and declares that only the DCI may create such programs for matters pertaining to intelligence sources and methods.

III. Purpose

The purpose of this manual is to provide standard procedures for the protection and control over all sensitive intelligence collection programs or derived intelligence which have been determined by the DCI to fall in the category of a Special Access Program as defined in Section 4-2 of EO 12065.

IV. Organizational Structure

The APEX Security Control System provides uniform procedures and policy guidance to protect designated collection programs and other sensitive sources and the processing, production, analysis, and dissemination of sensitive intelligence derived from them.

The Chairman of the DCI Security Committee* is responsible to the DCI for the development of security policy and for exercising the DCI's management responsibilities for the APEX Security Control System.

Senior Intelligence Officers (SIOs) of the Intelligence Community and heads of non-NFIB departments and agencies designated as recipients of APEX information are responsible for enforcing the policy and implementing the procedures outlined in this manual within their organizations. This responsibility may be delegated if the DCI is notified in writing of such delegation within 30 days of the effective date of such action.

To fulfill their responsibilities, SIOs may provide additional implementing guidance as long as such guidance is coordinated with the DCI Security Committee.

Although SIOs of the Intelligence Community must have the overall responsibility for policy compliance and implementation of pertinent procedures, adherence to the security procedures outlined in this manual is also the personal responsibility of each person indoctrinated into the APEX Security Control System.

To assist in carrying out the precepts dictated by the APEX Security Control System, SIOs will appoint or cause to be appointed APEX Control Officers (ACOs), ROYAL Control Officers (RCOs), and APEX Security Officers (ASOs), with alternates, to administer the system within their organizations or jurisdictions. ACOs and ASOs will be appointed within each organization at whatever levels may be appropriate to administer the system effectively. It is their responsibility to ensure full compliance with the provisions of this manual and any supplemental APEX directives that may be issued on behalf of the DCI.

It is preferable that the ACO and ASO positions not be held by the same individual unless management, operational, and organizational considerations clearly dictate otherwise. In that case, the ACO may also be appointed to serve as the ASO.

SIOs of the Intelligence Community are responsible for establishing APEX Control Facilities (ACFs) for the control, storage, and use of APEX materials. Each organization will have a central registry for materials coming from or being sent to other agencies and departments. Subregistries may be created.

The DCI will appoint an APEX Control Officer and an APEX Security Officer who will be responsible to him for overseeing the APEX system. The ACO/DCI and ASO/DCI may deal directly with officials of the Intelligence Community or their

* This will change when the new organization responsible for APEX is established.

designated ACOs and ASOs in matters related to policy interpretation and administration of the system. The ACO/DCI and ASO/DCI will be responsible for overseeing APEX system matters in all organizations outside the Intelligence Community and with foreign participants dealing with APEX material, excepting those APEX materials for which ACO/NSA and ASO/NSA will exercise authority in the area of foreign liaison on behalf of the DCI.

All APEX information will be transmitted and maintained within the APEX Security Control System. Compartmentation within the system will be denoted by the use of terms identifying categories of information (that is, COMINT, IMAGERY, HUMINT, and TECHNICAL), by project codewords which refer to collection activities, or by use of a special designator to indicate a requirement for exceptional access controls (for example, ROYAL). Approved projects and categories of information within the system may be added or removed from the APEX system only with the written approval of the DCI.

V. Description of System

a. General

As noted, the APEX apparatus provides a single system for controlling access to, and distribution and protection of, selected intelligence information and collection programs requiring exceptional security measures. Within this unified system there are distinct means of controlling access to several categories of information: operational data; the product of generic sources of intelligence information; and, by means of a special dissemination system, particularly sensitive intelligence.

b. Access to APEX Security Control System

There are three basic requirements for individual access to the APEX Security Control System:

1. Certification by the SIO of a need-to-know for specific aspects of the system. In the case of access to operational projects, a nominee's need-to-know must be validated by the SIO and have the approval of the operational Program Manager or Director.

2. Favorable adjudication that the nominee meets uniform personnel security criteria and investigative requirements set forth in this manual.

3. Security indoctrination and execution of a nondisclosure agreement as a condition of access to APEX material. The security indoctrination will provide the individual with prescribed information so that he or she will know what is to be protected, his or her responsibilities in doing so, and general information about the APEX system. Only one APEX nondisclosure agreement will be required and will be executed at the time of original access to APEX material. Subsequent access to additional

compartments within the APEX system will be accompanied by security indoctrinations that will include a reminder of the original agreement and its obligations. Upon indoctrination for any access to APEX material, the individual's name and all approvals held will be recorded in the Central APEX Access Registry maintained by the DCI Security Committee.

c. Revalidation of Access

It is the responsibility of each SIO to maintain a continuous review of access approvals to ensure that only those personnel with documented need-to-know have access at any time. In addition, in January of each year, SIOs and the DCI will review all extant approvals under their cognizance and revalidate the need-to-know requirement. Those no longer required will be debriefed at the earliest possible date.

d. Termination of Access

When it has been determined that certain accesses are no longer required, each individual concerned will be notified that his/her access to specific types of information is being terminated. Concurrently, the Central APEX Access Registry will be notified to delete the appropriate names and approvals.

e. Termination Secrecy Agreements

At the time access is no longer required, the individual will be required to account for and surrender all APEX documents under his/her cognizance and control, execute a certification that he/she retains no material or documents in the APEX system, and be reminded of the continuing obligation not to discuss or otherwise reveal APEX-controlled information.

f. Reentry Into APEX System

Personnel formerly accessed for APEX approvals who once again require one or more APEX approvals are to be treated the same as personnel gaining initial access and will be processed as in paragraph b, above.

g. Control of Access Approval Authorizations

Access to APEX information will be stringently controlled and application of the need-to-know requirement rigidly enforced. The DCI, in consultation with the SIOs of the Intelligence Community, will approve initial APEX access requirements. These requirements will be revalidated annually, at which time SIOs will be asked to estimate changes in their requirements. Requests for increases in access approvals during the periods between revalidation will be forwarded to the APEX Community organization for information and central recordkeeping. In the case of requests involving operational compartments and subcompartments, the originating SIO must seek the agreement of the SIO responsible for the operational compartment or subcompartment involved. If agreement cannot be reached on the granting of a requested access, the matter will be referred to the APEX Community organization to be processed on behalf of the DCI.

h. Administrative Access Approval

Personnel who do not require access to individual APEX compartments and the substantive information protected by them but who are in close proximity to APEX materials or programs will be provided with an administrative approval called APEX-GENERAL. The APEX-GENERAL access may be given in two phases:

1. ***Phase I*** accommodates those personnel who must be aware of or who handle APEX materials but do not have physical access to them. These would include guards, couriers, and technical personnel such as switching center technicians, computer technicians, and communications personnel.

2. ***Phase II*** accommodates those personnel who do not need APEX-protected materials for the performance of their duties but are in positions which would enable them to have access to the substantive materials protected by the system. These would include registry personnel, document control personnel, file clerks, secretaries, and the like.

Personnel receiving these administrative approvals must meet the basic personnel security requirements for access to APEX. They will be briefed only on the overall concept of the APEX system and the generic types of activities or information that it protects, the security responsibilities which are demanded by the APEX system, and their responsibilities to maintain need-to-know.

i. APEX Special Access Approvals

The President, the Vice President, and Cabinet Officers will have access to APEX materials. The DCI will ensure appropriate security indoctrination. The DCI may grant access to such other persons who will require APEX information necessary to the performance of their duties, subsequent to appropriate security indoctrination briefing.

VI. ROYAL

a. Purpose

The ROYAL caveat is used to designate TOP SECRET material that must be afforded extraordinary handling procedures to provide maximum protection for information of the highest sensitivity.

1. ***Description of Material.*** ROYAL material consists of unique substantive intelligence information considered sensitive enough to require dissemination restrictions beyond those provided for the generic product compartments of the APEX security control system. NFIB agencies may nominate to the DCI the information or projects they wish to be handled and controlled under ROYAL procedures.

2. ***Selection Process.*** The following items should always be considered before nominating material for ROYAL control:

(a) *Sensitivity.* This primary determinant could be related to time, method, content, event, or other pertinent factor which could compromise the source of the information.

(b) *Damage Potential.* The compromise of ROYAL material, because of its extreme sensitivity, could reasonably be expected to cause exceptionally grave damage to the United States.

b. Access Procedures

The highly sensitive and critical nature of the material included in ROYAL dictates that its distribution be severely limited, distinctly selective, and tightly controlled. Departments and agencies originating ROYAL materials will disseminate such material only to specific individuals by name. Personnel authorized to receive ROYAL material will be determined by NFIB principals or their designated representatives. All personnel authorized ROYAL access will be given a ROYAL indoctrination and must sign an APEX security agreement. The strictest must-know criteria will govern access to ROYAL. ROYAL access authorization does not imply automatic receipt of all ROYAL material. All approved ROYAL categories and authorized recipients will be recorded in the Central APEX Access Registry. The number of personnel certified for ROYAL will be limited to an absolute minimum.

c. ROYAL Control

Material designated as ROYAL will be distributed within the APEX security control system in sealed envelopes, on a "by name" basis, to personnel who have been officially designated as ROYAL Control Officers by NFIB principals.

1. ***Hard-Copy Dissemination.*** Hard-copy dissemination of ROYAL material will normally be limited to the National Capital Region (NCR). It will be dispatched only by the RCO of the originating NFIB agency and disseminated, as necessary, to the RCOs of receiving agencies. Internal dissemination within receiving agencies or departments will be made only to ROYAL-indoctrinated individuals. Exceptions to this policy must be authorized by an NFIB principal, who must inform the originator of any exceptions which have been made. The notation "TO BE OPENED BY THE ROYAL CONTROL OFFICER" will be conspicuously displayed above the pouch address of the receiving APEX Control Facility on both the inner and outer containers. Hard-copy dissemination outside the NCR may be negotiated between the originator of ROYAL products and the SIO of those consumers with a validated need-to-know.

2. ***Electrical Transmission.*** Generally, electrical transmission of ROYAL material is not authorized. In those cases when a need for electrical transmission can be justified, the reasons will be outlined in the request nominating the project for acceptance in the ROYAL system.

3. ***Removal of ROYAL Protection.*** Subject to the approval of the originator, information may be removed from the ROYAL control system when dissemination of the information is required on an immediate and urgent basis in support of current or impending US operational activities; or when the intelligence is critical for strategic, tactical, analytical, or exploitation purposes by a broader base of consumers than the limited ROYAL audience permits.

4. ***Administrative Handling.*** All administrative handling requirements of this APEX manual apply to ROYAL materials with the following exceptions:

(a) *Reproduction.* The reproduction of ROYAL documents is expressly forbidden. Requests for additional copies will be addressed to the originator.

(b) *Storage.* ROYAL material will be segregated from other APEX material in the ACF. A separate drawer or file container, which must be locked when not under the supervision and surveillance of appropriately cleared personnel, will be used. Strict accountability, with mandatory semiannual inventories, of all ROYAL material will be maintained, and documents will be returned to the originator as soon as they serve their purpose. No formal accreditation for ROYAL storage is required, provided the ROYAL material is stored within the ACF and the ROYAL storage area identified to the Central Registry of Facilities.

(c) *Sensitivity Revalidation Procedures.* The need for materials to retain ROYAL protection will be reviewed semiannually by the originator and submitted to the DCI.

d. ROYAL Control Officers

RCOs will perform the following functions:

1. Administer all required ROYAL indoctrinations and debriefings.

2. Serve as the exclusive control point for all ROYAL materials originated or received by the agency represented.

3. Maintain complete and current lists of authorized recipients within each category of ROYAL information.

4. Ensure that ROYAL material is read in the RCO area and retain the material within the ACF. When ROYAL material is removed from an RCO area, the RCO is responsible for its safekeeping and return to the ACF.

5. Serve as the focal point for all ROYAL-related correspondence and ensure that all DCI-directed actions concerning ROYAL access are immediately and accurately accomplished.

6. Establish and supervise the necessary administrative procedures and controls necessary to ensure compliance with ROYAL procedures.

7. Be responsible for all reporting requirements of the ROYAL control system and file reports of security violations or compromises as required by this manual or by the RCO's parent organization or department.

VII. Responsibilities of APEX Control and Security Officers

a. Duties of APEX Control Officers

1. Ensure that APEX materials are accounted for, controlled, transmitted, destroyed, packaged, and safeguarded in accordance with provisions of this manual.

2. Act as the exclusive control point for receiving and dispatching APEX materials via electrical, courier, or other means approved for the transmission of APEX materials.

3. Complete and return to the sender receipts attached to APEX documents received. Ensure that all outgoing materials have properly prepared receipts and send tracers as required for receipts not returned.

4. Ensure that APEX materials are disseminated only to those persons properly indoctrinated and with a need-to-know.

5. Process all APEX access approval requests for personnel within their jurisdiction.

6. Provide advice and guidance on the proper classification levels, codewords, and caveats within the APEX Security Control System.

b. Duties of APEX Security Officers

1. Coordinate and receive prior approval through appropriate channels for accreditation and establishment of APEX Control Facilities.

2. Maintain current listings of all APEX-accessed individuals within their jurisdiction.

3. Conduct required security indoctrinations and debriefings of personnel approved for APEX access and obtain signed Nondisclosure and Termination Secrecy Agreements as necessary.

4. Conduct reindoctrination on a periodic basis, not to exceed two-year intervals.

5. Ensure periodic security inspections of APEX Control Facilities under their jurisdiction, make recommendations for corrective action, and conduct followup action on recommended corrective measures.

6. Approve secure procedures for transmitting and receiving APEX materials.

7. Ensure investigations of any possible security infractions involving APEX information under their jurisdiction to determine if a compromise has occurred, make appropriate recommendations, and prepare required reports.

8. Notify the APEX control organization of all additions and deletions of access approvals and facility accreditations within the APEX system on a timely basis.

VIII. Security Standards for Access Approval

a. Need-To-Know Policy

Access to the APEX Security Control System is governed by the need-to-know policy in conjunction with approval criteria established in this manual. The need-to-know policy is defined as that determination made by competent authority which attests to the bona fide need for access in order to perform official duties on behalf of the US Government.

b. Approval Authority

Authority to approve access to data within the APEX Security Control System rests with the DCI and the SIOs of the Intelligence Community. This authority presupposes determination that the individual to be approved meets prescribed personnel security criteria enunciated below and has a legitimate, official need for access.

Within NFIB agencies access to operational compartments and subcompartments will be requested by the appropriate SIO and approved by the responsible program director. If agreement cannot be reached on the granting of access, the matter will be referred to the APEX control organization to be processed on behalf of the DCI. In the case of non-NFIB agencies, this coordination will be the responsibility of the APEX control organization. In cases where agreement cannot be reached the matter will be referred to the DCI for resolution.

c. Personnel Security Standards

Criteria for security approval of an individual on a need-to-know basis for access to the APEX Security Control System are as follows:

1. The individual shall be stable, of excellent character and discretion, and of unquestioned loyalty to the United States.

2. Except where there is a compelling need and a determination has been made by competent authority as described below that every reasonable assurance has been obtained that under the circumstances the security risk is negligible:

(a) Both the individual and the members of his/her immediate family shall be citizens of the United States. For these purposes, "immediate family" is defined as including the individual's spouse, parents, brothers, sisters, and children.

(b) The members of the individual's immediate family and persons to whom he/she is bound by affection or obligation should neither be subject to physical, mental or other forms of duress by a foreign power, nor advocate the use of force of violence to overthrow the Government of the United States or the alteration of the form of Government of the United States by unconstitutional means.

In exceptional cases, the SIO of the Intelligence Community organization, or his formally appointed designee, may determine that it is necessary or advisable in the national interest to authorize access to APEX prior to completion of the fully prescribed investigation. In this situation, such investigative checks as are immediately possible will be made at once, and should include a personal interview by trained security or counterintelligence personnel. Access in such cases will be strictly controlled, and the fully prescribed investigation and final evaluation will be completed at the earliest practicable moment.

Exceptions to 2(a)(b) above may be granted only by the SIO or his/her designee. All exceptions granted will be common sense determinations based on all available information and will be recorded by the agency making the exception. In those cases in which the individual has lived outside the United States for a substantial period of his/her life, a thorough assessment of the adequacy of the investigation in terms of fulfillment of the minimum investigative requirements and judicious review of the information therein must be made before an exception is considered.

d. Investigative Requirements

The investigation conducted on an individual under consideration for access to the APEX Security Control System will be thorough and will be designed to develop information as to whether the individual clearly meets the personnel security standards specified above.

The investigation will be accomplished through record checks and personal interviews of various sources by trained investigative personnel in order to establish affirmatively to the adjudicating agency complete continuity of identity, to include birth, residences, education, places of employment, and military service. Where the circumstances of a case indicate, the investigation will exceed the basic requirements set out below to ensure that those responsible for adjudicating access eligibility have in their possession all the relevant facts available.

The individual will furnish a signed personal history statement, fingerprints of a quality acceptable to the Federal Bureau of Investigation, and a signed release, as necessary, authorizing custodians of police, credit, educational and medical records to provide information to the investigative agency. Photographs of the individual will also be obtained where additional corroboration of identity is required.

Minimum standards for the investigation are as follows:

1. Verification of date and place of birth and citizenship.

2. Check of the subversive and criminal files of the Federal Bureau of Investigation, including submission of fingerprint charts, and of such other national agencies as are appropriate to the individual's background. An additional check of Immigration and Naturalization Service records will be conducted on those members of the individual's immediate family who are US citizens by reason other than birth or who are resident aliens.

3. A check of appropriate police records covering all areas where the individual has resided in the United States during the previous 15 years or since age 18, whichever is the shorter period.

4. Verification of the individual's financial status and credit habits through checks of appropriate credit institutions and interviews with knowledgeable sources covering the previous five years.

5. Interviews with neighbors in the vicinity of all the individual's residences for periods of more than six months during the previous five-year period. This coverage will be expanded where the investigation suggests the existence of some questionable behavioral pattern.

6. Confirmation of all employment during the previous 15 years or since age 18, whichever is the shorter period, but in any event the previous two years. This will include personal interviews with supervisors and coworkers at places of employment over the previous 10 years if appropriate.

7. Verification of attendance at institutes of higher learning in all instances and at the last secondary school attended within the previous 15 years. Attendance at secondary schools may be verified through qualified collateral sources. If attendance at educational institutions occurred within the previous five years, investigators will seek personal interviews with faculty members or other persons acquainted with the individual during his/her attendance.

8. Review of appropriate military records.

9. Interviews with a sufficient number (a minimum of three) of knowledgeable acquaintances to provide a continuity, to the extent practicable, of the individual's activities and behavioral patterns over the previous 15 years, with particular emphasis on the most recent five.

10. When employment, education, or residence has occurred overseas (except for a period of less than five years for personnel on US Government assignment and less than 90 days for other purposes) during the previous 15 years or since age 18, a check will be made of records at the Department of State and other appropriate agencies. Efforts will be made to develop sources, generally in the United States, who knew the individual overseas in order to cover significant employment, education, or residence and to attempt to determine if any lasting foreign contacts or connections were established during this period. However, in all cases where an individual has worked or lived outside the United States continuously for more than five years, the investigation will be expanded to cover fully this period in his/her life through the use of such investigative assets and checks of record sources as may be available to the US Government in the country or countries in which the individual resided.

11. In those instances in which any of the situations described in subparagraph C2(b), above, apply to the immediate family of an individual under investigation or to a person to whom he/she is bound by affection or obligation, the investigation will include an interview of the individual by trained security, investigative, or counterintelligence personnel to ascertain the facts as they may relate to the individual's access eligibility.

12. In all cases, the individual's spouse will, at a minimum, be checked through the subversives files of the Federal Bureau of Investigation and other national agencies as appropriate. When conditions indicate, additional investigation will be conducted on the spouse of the individual and members of the spouse's immediate family to the extent necessary to permit a determination by the adjudicating agency that the provisions in paragraph C, above, concerning personnel security standards are met.

13. A personal interview of the individual will be conducted by trained security, investigative, or counterintelligence personnel when necessary to resolve any significant adverse information and/or inconsistencies developed during the investigation.

If an earlier investigation conducted within the previous five years substantially meets the minimum standards specified above, it may serve as a basis for granting access approvals, provided a review of the personnel and security files does not reveal substantive changes in the individual's security eligibility. If a previous

investigation does not substantially meet the minimum standards, or if it is more than five years old, a current investigation will be required but may be limited to that necessary to bring the individual's file up to date in accordance with the investigative requirements set forth above. If new information developed during the current investigation should bear unfavorably on activities of the individual that were covered by the previous investigation, the current inquiries will be expanded as necessary to develop full details of the new information.

The evaluation of the information developed by investigation of an individual's loyalty and suitability will be accomplished under the cognizance of the SIO concerned by analysts of broad knowledge, good judgment, and wide experience in personnel security and/or counterintelligence.

When all other information developed on an individual is favorable, a minor investigative requirement which has not been met should not preclude favorable adjudication. In all evaluations, the protection of the national interest is paramount. Any doubt concerning personnel having access to APEX information will be resolved in favor of protecting the national security. The ultimate determination that national security is or is not endangered will be an overall common sense decision based on all available information.

e. Reinvestigations

Programs will be instituted requiring the periodic reinvestigation of personnel provided access to APEX information. These reinvestigations will be conducted on a five-year recurrent basis under normal circumstances, but on a more frequent basis where the individual has shown some questionable behavioral pattern, where his/her activities are otherwise suspect, or when deemed necessary by the SIO concerned.

The scope of reinvestigations will be determined by the SIO concerned. His /her decision will be based on such considerations as the potential damage that might result from the individual's defection or willful compromise of APEX information and the availability and probable effectiveness of other means to evaluate continually the factors related to the individual's suitability for continued access. In all cases, the reinvestigation will include, at a minimum, appropriate checks of national or local agencies (including overseas checks where appropriate), credit checks, and a personal discussion with the individual by trained investigative, security, or counterintelligence personnel when necessary to resolve significant adverse information or inconsistencies.

Whenever adverse or derogatory information is discovered or inconsistencies arise which could impact on an individual's security status, appropriate investigations will be conducted on a timely basis. The investigation will be of sufficient scope to resolve the specific adverse or derogatory information or inconsistency in question so a determination can be made as to whether the individual's continued utilization in activities requiring APEX access is clearly consistent with the interests of the national security.

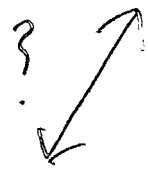
f. Changes in Personal Status

Responsible officials must take into consideration any change in personal status that may have a bearing on the continuing eligibility of individuals approved for access to APEX material. Name changes (resulting from marriage, divorce, or court decree) must be reported to the Central APEX Access Registry.

g. Contacts or Association With and Marriages to Foreign Nationals

A close, continuing personal association with a foreign national is a matter of APEX security concern if it is characterized by ties of kinship, affection, or obligation. APEX-indoctrinated personnel must protect themselves against cultivation and possible exploitation by foreign nationals who are or may be working for foreign intelligence services and to whom they might even unwittingly provide APEX classified information.

The following types of relationships must be reported to the APEX Security Officer:



1. All nonofficial contacts with citizens or representatives of Communist-controlled countries listed by the DCI (appendix A), no matter how brief or apparently trivial the contacts may be.

2. Close and continuing nonofficial or any regular, frequent contact with any other foreign national.

Casual, inadvertent, or irregular contacts which arise from normal living and working in a community need not be reported. However, if the person with whom the casual contact occurs shows undue interest in employment, assignment, and so forth, then the contact must be promptly reported. Whenever any doubt exists about whether a situation should be reported or made a matter of record, the individual should promptly make a report to the APEX Security Officer. Failure to report such contact may result in denial or withdrawal of access to APEX material.

APEX-approved individuals who contemplate marriage to a foreign national must report such plans to their APEX Security Officer along with, at a minimum, basic biographic details about the intended spouse and his/her immediate family (name, date and place of birth, country of origin and current citizenship, current residence, present occupation, and any present or former employment on behalf of any foreign government). A security evaluation will be undertaken before there is any determination that a waiver of standards might be made to continue the approved person in APEX-indoctrinated status.

h. Travel and Duty Assignment Restrictions

1. ***Unofficial Travel.*** Persons granted authorization for access to certain categories of extremely sensitive information on foreign intelligence sources and methods protected by the APEX Security Control System incur a special security obligation and are to be alerted by their SIO to risks associated with unofficial visits to, or travel through, countries identified by the DCI (appendix A). The SIO concerned should advise that unofficial travel in those countries without official approval may result in the withdrawal of approval for

continued access to APEX information for persons with specific extensive knowledge of any of the following categories of extremely sensitive information on foreign intelligence sources and methods:

(a) Technological structure, function, and techniques of sensitive intelligence collection or exploitation systems/methods.

(b) Designated system targets or sources.

(c) Method and purpose of target selection.

(d) Degree of success of collection or exploitation system/method.

(e) Capabilities and vulnerabilities of collection or exploitation system/method.

2. All persons having access to APEX information who plan unofficial travel to or through countries listed by the DCI must:

(a) Give advance notice of such planned travel.

(b) Obtain a defensive security briefing from an APEX Security Officer before traveling to such countries.

(c) Contact immediately the nearest US consular, attache, or embassy official if they are detained or subjected to significant harassment or provocation while traveling.

(d) Report to their SIO upon their return from travel any incidents of potential security concern that occurred during the trip.

3. ***Official Assignment/Travel.*** No person with access to APEX information will be assigned to or directed to participate in hazardous activities until he/she has been afforded a defensive security briefing and/or risk-of-capture briefing as applicable. Due consideration will be given to the relative protection enjoyed by US officials having diplomatic status.

4. ***Individuals With Previous Access.*** Persons whose access to APEX information is being terminated will be officially reminded of the risks associated with hazardous activities as defined herein and of their obligation to ensure protection of APEX.

5. ***Responsibilities.***

(a) The DCI will cause to be prepared and disseminated to the SIOs a list of countries identified as posing a security risk bearing on this policy. The DCI Security Committee will coordinate required support, including source material concerning these risks.

(b) SIOs will ensure:

(1) Preparation and provision of defensive security briefings or risk-of-capture briefings to personnel of their departments or agencies.

(2) Institution of positive programs for the collection of information reported under the provisions of paragraph h 2(d), above.

(3) That new information obtained by their departments or agencies on harassments or provocations, or on risk-of-capture situations, is provided to the DCI and to other interested NFIB agencies.

IX. Physical Security

a. Construction and Protection Standards

All materials within the APEX Security Control System must be stored within accredited APEX Control Facilities. Standards for construction and protection of ACFs will be as prescribed in USIB-D-9.1.20 (USIB Policy Statement Establishing Physical Security Standards for Sensitive Compartmented Information Facilities), 30 April 1973, or according to other guidelines that may supersede the USIB statement (appendix B).

b. Accreditation and Registration of Approved Facilities

Before a facility is authorized to handle APEX material, it must be accredited as having met the aforementioned construction and protection standards. Such accreditation will be made by SIOs of the Intelligence Community or by the CIA Office of Security for non-NFIB departments and agencies, the Legislative and Judicial Branches, and cooperating foreign countries.

All accredited ACFs and the categories of information they handle will be provided to the APEX control organization, which will maintain a Central Registry of Facilities. SIOs of the Intelligence Community will be provided periodic listings of the ACFs which they control for verification of accuracy or updating as necessary.

The DCI, through his ASO, reserves the right to review all files on accredited ACFs, to inspect the ACFs, and to make the final determination regarding the appropriateness of the security safeguards provided for any particular ACF.

c. Inspections

Periodic inspection of ACFs is mandatory and must be done at least annually. Inspections are to be performed by designated persons qualified in conducting security inspections for control and storage of APEX materials and will assure that procedures and safeguards comply with standards prescribed by this manual. Reports of inspection will be retained in the files of the accrediting officials. Where there are joint facilities or shared accommodations, notations to that effect will be made in inspection reports to indicate identities of all offices using the facilities as well as the projects being handled therein. Irregularities, and action taken to correct these irregularities, will be noted in inspection reports. Sensitive documents which cannot be accounted for will be given priority attention. All action taken to locate such documents will be made a part of all inspection reports.

d. Emergency Plans

Each APEX Control Facility will maintain an emergency plan approved by the appropriate accrediting official. Normally this plan will be included within an overall department, agency, or installation plan. Emergency plans must be made for all APEX-controlled data. In areas where political or criminal activity suggests the possibility that an ACF might be overrun by outsiders, emergency destruction of APEX materials must be considered and appropriate plans drawn for this eventuality. Emergency planning must also take account of fire, natural disasters, entrance of uncleared emergency personnel into an ACF, and the physical protection of those working in such areas. In addition to adequate protective equipment, firefighting equipment, and escape plans, consideration must be given to life-support equipment which might be required for personnel trapped in ACF vault areas. Updates on these plans will be made annually, and training provided to familiarize personnel with the plans.

e. Two-Person Rule

To provide proper security and safety protection to APEX materials, all ACFs will be staffed by at least two persons when in use. Persons selected to work in such areas will be chosen on the basis of proven reliability and maturity. Waivers to the two-person rule may be granted only by SIOs of the Intelligence Community.

X. Technical Security

a. Technical Security Countermeasures (TSCMs)

TSCMs will be conducted as soon as possible after the opening of an APEX facility and within six months following major physical renovations. ACFs are to be reinspected every 18 months. Briefings on the threat of technical penetrations will be provided to personnel manning all APEX Control Facilities.

b. Computer Security

All automatic data-processing equipment used in connection with programs or products developed under the APEX Security Control System will be operated in compliance with DCID 1/16 (Security of Foreign Intelligence in Automated Data-Processing Systems and Networks). (See appendix C.)

c. Compromising Emanations Control (TEMPEST Security)

All equipment used to transmit or process APEX information electronically, including communications, word-processing, and automatic data-processing systems and equipment, must satisfy the requirements of USCSB 4-11 (National Policy on Control of Compromising Emanations). (See appendix D.) All compromising emanations must be contained within boundaries specified by the TEMPEST accreditation authority.

XI. Central Registry of Access Approvals and Certifications

a. Central APEX Access Registry

A Central APEX Access Registry is established within the APEX control organization to serve as the official central data base for the APEX Security Control System. All approvals of access to the APEX system will be recorded in this data base.

b. Information Updates

A critical need of the APEX Security Control System is to maintain an accurate record of personnel currently cleared for various compartments of the system. To enable the system to function properly, all departments and agencies must provide timely information on approval status to the Central Registry. Updates will be provided to ensure that all briefing or debriefing actions are recorded within 30 days of the actual event. Personnel newly approved or recently debriefed can be verified as necessary through host agencies within the Intelligence Community or, outside the Community, by the sponsoring agency or program. However, this will not relieve sponsoring departments, agencies, and programs of the obligation for timely reporting of personnel briefed or debriefed.

The Central APEX Access Registry will provide, on a monthly basis to each controlling SIO, a listing of approved personnel within his/her organization and the accesses they hold. It is expected that, with provision of these lists, review will be made of active approvals and that those no longer needed will be canceled and reported to the Central Registry. This is a continuing requirement assigned to each ACO irrespective of the formal annual review by the DCI, SIOs, and Program Managers/Directors of personnel approved for access.

These same listings will be used to correct records in order to reflect personnel approved but not recorded in the Central Registry. DCI, SIO, or Program Manager/Director verification will be effected, as necessary, before adding personnel or approvals for already-approved personnel to the Central Registry.

c. Certification Requirements and Methods

Wherever possible, and within practicable limitations, departments and agencies will establish a common badging system to establish clear and valid evidence of approval status for various compartments within the product compartments of the APEX Security Control System. This system will be used, wherever possible, between participating components. When this system is not feasible, approval certification will be provided either by telephone, secure communications, or memorandum, as appropriate. It is the responsibility of each approving component to provide certification to those other components with which its personnel have a need-to-know requirement to do business.

XII. Security Classification and Control Guidelines

a. Basic Guidance

Security classification and document control are functions of management. Classification of information, therefore, will be accomplished only by individuals specifically authorized under EO 12065. Use of compartmentation caveats on National Foreign Intelligence will be solely to provide need-to-know or access protection where normal management and safeguarding procedures are not, as a protective measure, considered sufficient.

b. Decompartmentation

Decompartmentation is the official act of removing intelligence information or material from a compartment by deleting specific references to sources and methods in accordance with a definitive set of criteria for each generic source. Depending upon the criteria, decompartmentation can be accomplished by sanitization or by eliminating all evidence of special security control. To the extent possible, materials protected under the APEX Security Control System will be decompartmented. However, neither specific intelligence sources and methods nor data of special sensitivity are to be disclosed in this process. Decompartmentation is to be accomplished in accordance with guidelines established by the APEX control organization in APEX Control Facilities by indoctrinated APEX personnel, and will be reviewed by the ACO prior to release.

ACOs will notify recipient centers of decompartmentation actions so the items concerned may be removed from APEX control requirements.

c. Downgrading

Downgrading is the lowering of classification level. Intelligence and intelligence-related information may, with the passage of time, lose the sensitivity that justified its original classification. In such a case, action will be taken by the DCI, SIOs, Program Managers or Directors, or other appropriate authorities to assign a lower classification or to declassify the material.

The test for continuing or lowering a classification level will be the standards established for TOP SECRET, SECRET, and CONFIDENTIAL in EO 12065, Section 1-1.

To the extent practicable, ACOs are to notify known holders of affected documents of downgrading actions.

d. Sanitization

Sanitization is the process of removing intelligence information which may reveal sources and methods. Information may be removed from the APEX Security Control System in accordance with guidelines established by the APEX control organization by deleting all references to intelligence sources and methods. Prior to sanitization, a conclusion must be reached that there exists a possible alternate source for the information or that the information can be presented in such a way that complete protection is provided to the actual source. Normally, in reporting sanitized information, no source attribution will be made. If attribution is necessary, only a general statement—such as "a source of known reliability"—will be used.

e. Emergency Dissemination Authorization

Broader dissemination of APEX-derived products is authorized in emergency situations. In such emergencies, the Director, INR, and the Director, Defense Intelligence Agency, are authorized to decompartment, downgrade, declassify, and disseminate APEX-controlled or APEX-derived products. In military situations, this authority may be further delegated, as necessary, to the commanders of the unified and specified commands and their subordinates. Such decompartmentation/downgrading/declassification actions will be strictly limited to the products that are pertinent to the geographic areas and the types of operations in which US, allied, or friendly forces are, or likely to be, engaged. When such decompartmentation/downgrading/declassification actions have been initiated as a contingency measure in anticipation of hostile activity that does not subsequently materialize, actions will be taken within 48 hours after the threat subsides to recall the materials to the extent practicable and to put them back under the original security classification controls. A report will then be forwarded to the DCI assessing the extent of any compromise of the APEX-derived products.

or are likely

If APEX materials provided by other countries are involved, every effort should be made to consult officials of those countries prior to any emergency dissemination and use. At a minimum, those countries must be advised that such actions have occurred.

The DCI will be advised of all emergency disseminations as soon after the fact as possible.

f. Challenges to Classification Levels and Control Restrictions

Any person with access to APEX may challenge either the classification level or the need for compartmented control of any APEX material. The challenger should submit the challenge to the originating component for consideration. Items which are irreconcilable should be forwarded through APEX control channels to the APEX control organization for final review and resolution.

XIII. Control Standards and Procedures

a. Classification Levels

Documents in the APEX Security Control System will be classified according to potential damage to national security if the information in them is disclosed without authority. Classification levels will be ascribed in accordance with EO 12065, reserving CONFIDENTIAL for "identifiable damage," SECRET for "serious damage," and TOP SECRET for "exceptionally grave damage." No other classification levels are authorized.

b. Labeling

The following labeling requirements are established for all written or graphic materials that contain APEX information and are disseminated within the APEX Security Control System.

1. ***Classification.*** The overall classification of a document, whether or not permanently bound, or any copy or reproduction thereof, will be conspicuously marked or stamped at the top and bottom of the outside of the front cover (if any), on the title page (if any), on the first page, on the back page, and on the outside of the back cover (if any). Each interior page of a document will be conspicuously marked or stamped at the top and bottom with the highest classification of the document. Portions of documents, to include paragraphs, subparagraphs, and titles will be marked to reflect the level of classification, codewords, caveats, and other control markings or to state that the particular portion is unclassified. Major components of some documents are likely to be used separately. In such instances, each major component will be marked as a separate document. Examples include each annex, appendix, or similar component of a plan, program, or operations order; attachments and appendixes to a memorandum or letter; and each chapter of a report or document.

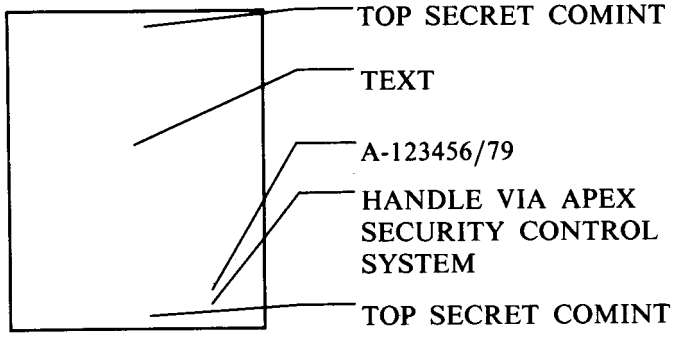
2. ***Control System Caveats.*** All documents controlled within the system will be marked "HANDLE VIA APEX SECURITY CONTROL SYSTEM" on the front cover (if any), title page (if any), back page, and first page of all documents. Each interior page that contains information containing APEX information will bear the same markings.

3. ***Codewords and Indicators.*** Codewords for operational projects, operational subcompartments, ROYAL material, and product indicators will be placed following the classification markings on the top and bottom of the title page (if any), first page, and each page which contains information requiring specific codeword/indicator protection.

4. ***Control Numbers.*** APEX document control numbers will be provided to Community SIOs by the APEX control organization. Originators will assign a control number to all APEX material for general distribution to other offices, agencies, or commands, when use of a number is considered a necessary adjunct to identification, control, or retrieval of the material. Control numbers will be placed immediately above the control system caveat on the front cover (if any), title page, and first page of each document. These numbers will be issued sequentially ("one up") and will consist of the letter A, a dash, a six-digit assigned number, a slant or

oblique stroke, and the last two digits of the current year (for example, A-123456/79). Copy numbers of individual documents will be reflected as Copy __ of __ on the cover and first page of the document.

SAMPLE PAGE



5. ***Control Markings for the Dissemination of Foreign Intelligence and Related Material.*** Restrictive and other markings prescribed in DCID 1/7 (appendix E) will be used on the title page, front cover, and other applicable pages or paragraphs when it is necessary to control the dissemination of foreign intelligence or related material which requires APEX protection.

6. ***Declassification Review Notice.*** Having satisfied threshold criteria demanding protection under the APEX Security Control System, APEX materials are classified for a period of 20 years (except for information from foreign governments, which will remain protected for 30 years). The following Declassification Review Notice will be used on the cover (if any), title page, or first page of typescript text, or inside cover of formal publications:

CLASSIFIED BY: (appropriate authority)

REVIEW ON : (indicate date 20 or 30 years from date of issuance)

REASON FOR EXTENDED CLASSIFICATION: APEX XIII, b.6 (for original classification decisions only)

The abbreviation "REVW (date 20 or 30 years)" may be substituted in electrically transmitted messages.

7. ***Abbreviations.*** Distinctive APEX markings will not be abbreviated where there is a likelihood that the abbreviation will be confusing or otherwise not understood by the recipient. A standard list of approved abbreviations will be provided by the APEX control organization.

8. ***Marking Files, Folders, or Groups of Documents.*** Files, folders, or groups of documents shall be conspicuously marked to assure the protection of all APEX material contained therein. Such material should be marked on the file folder tab or other prominent location, or the marking should be affixed to an appropriate APEX cover sheet.

c. Pouching and Transmittal Requirements

APEX material to be transmitted from one ACF to another must be carried either by two couriers approved for this purpose, by diplomatic pouch, or by the Armed Forces Courier Service (ARFCOS). Courier procedures will ensure that APEX materials are adequately protected against the possibility of hijacking, unauthorized viewing, loss, or other form of compromise during the transmission. Transmittal of APEX material via non-US-Government-operated or chartered aircraft is prohibited.* The responsible SIO must specifically approve all exceptions.

APEX couriers will be active-duty military or US Government civilian employees meeting APEX access standards and be specifically designated by the responsible SIO. Couriering of APEX material by contractors or consultants is prohibited except when specifically approved by the responsible SIO.

APEX materials will be enclosed for delivery in two opaque envelopes or otherwise be suitably double-wrapped using canvas bags, cartons, crates, leather pouches, and so forth. Containers will be secured with tape, lead seals, and tumbler padlocks, or by other means which would reasonably protect against surreptitious access.

The inner and outer container will be annotated to show the pouch address and package number of the sending APEX Control Facility. The notation "TO BE OPENED BY THE ACO" will be placed above the pouch address of the receiving APEX Control Facility on both containers. The proper security classification and the caveat "CONTAINS APEX-CONTROLLED MATERIAL" will be annotated on each side of the inner wrapper only. The inner container will contain the document receipt and should also reflect the name or office symbol of the person/activity for whom the material is intended.

APEX documents may be transported by a single officially designated courier within US Government or military installations. Within the Washington metropolitan area, an SIO of the Intelligence Community may authorize designated personnel to hand-carry APEX material. In all cases, APEX material will be in a securely locked briefcase or sealed pouch marked with the words "TO BE RETURNED UNOPENED TO (NAME OF APEX FACILITY)" and with other applicable information if required by operational necessity. No inner wrapper or container is required under these circumstances.

d. Electrical Transmissions

APEX material transmitted electrically will be controlled according to procedures prescribed below. Senders must assure that electronic transmissions are made only to authorized recipients, and receivers must provide procedures for the proper protection of APEX material received in this manner. These procedures will include the establishment of a recipient's need-to-know in circumstances where no hard copy or record copy of the material will result.

The transmission of APEX material will be restricted to means specifically approved and accredited by the DCI for this purpose.

*Does not apply to ARFCOS and the Diplomatic Courier Service.

Electrical transmission of APEX material will be limited to specifically accredited communications circuits secured by an NSA-approved crypto system, protected distribution system, and the effective edition of KAG-1 communications policy and procedures.

Material transmitted by accredited communications circuits or other specialized means will be marked at the top and bottom with the assigned classification and portion marked in the manner prescribed above for documents. Applicable codewords, designators, caveats, and so forth, will be clearly shown, consistent with the design of the message form or format being used.

The first item in the text of a message will be the overall classification of the message, applicable codeword(s), the "HANDLE VIA APEX SECURITY CONTROL SYSTEM," and such other markings as may be required by DCID 1/7.

e. Cover Sheets

To preclude unauthorized disclosure, an unclassified cover sheet will be used when transmitting APEX materials outside of an ACF. Publications need not have a separate document cover sheet affixed if the publication cover includes all prescribed markings and is unclassified standing alone.

f. Destruction

As soon as possible after its purpose has been served, all APEX-controlled material will be destroyed in a manner that will preclude reconstruction in any intelligible form. Only those methods (these may include burning, pulping, pulverizing, melting, or chemical decomposition, depending on the type of materials to be destroyed) specifically authorized by the responsible SIO will be used. Destruction will be supervised and witnessed by at least two APEX indoctrinated individuals. Certification-of-destruction records shall be maintained for a period of three years. APEX material contained within computer or automated data-processing systems or other magnetic media will be erased by approved degaussing equipment or by other means designated by the DCI. (See "Intelligence Community Policy for the Release of Magnetic Storage Media," 13 March 1974, appendix F.)

g. Reproduction

Reproduction of APEX material will be kept to a minimum consistent with operational necessity. Copies of documents are subject to the same controls as the original. Adherence to stated prohibitions against reproduction is mandatory. Any equipment used for APEX reproduction must be thoroughly inspected and sanitized before removal of the equipment from the ACF.

Reproduction of hard-copy APEX TOP SECRET materials requires the prior consent of the originator. Materials classified SECRET or CONFIDENTIAL may be restricted from reproduction by the originator by application of the phrase "REPRODUCTION REQUIRES APPROVAL OF ORIGINATOR."

h. Accountability

All hard-copy APEX TOP SECRET documents will be inventoried at least annually or when there is a change of designated ACOs or authorized custodians of such material. SIOs of the Intelligence Community may authorize adjustments to this policy in the case of ACFs with limited manpower or with substantial holdings (such as libraries or order-of-battle files).

Accountability and inventory of ROYAL material will be in accordance with chapter VI of this manual.

Random audits will be conducted annually for all other APEX hard-copy documents to ensure that the holdings are properly accounted for and maintained according to this manual.

Should a random audit fail to locate a significant number of sampled documents, the responsible ASO will order a complete inventory of APEX documents received by the ACF.

All discrepancy reports will be provided to the responsible ASO, who will initiate search and investigation of all missing documents. Intelligence Community ASOs will provide the DCI/ASO an annual report of the results of their inventories or audits during October of each year.

Each ACF will keep a record of all APEX documents that are dispatched outside the facility. This dissemination record will identify the material and the specific organizations to which the documents were disseminated.

Dissemination records of incoming TOP SECRET and ROYAL hard-copy documents will be retained as long as the material is held by an ACF and for three years after destruction.

Dissemination records for other incoming APEX documents will be retained for as long as needed for administrative or accountability purposes, but in no case for less than six months. The dissemination record requirement for dispatched materials may be satisfied by keeping copies of the envelope/pouch/package receipt or other appropriate dissemination records maintained by the dispatching ACF. Such receipts should be retained for a minimum of two years.

Dissemination records are not required for raw intelligence data that are transmitted on a regular basis from a collection point or facility to a processing facility; nor are records required while such material is being processed into a form suitable for analytical use, provided it remains under the control of a single Intelligence Community agency, is transmitted only by means authorized herein for APEX materials, and is accessible only to personnel meeting standards for and granted access to the appropriate APEX program.

Working materials containing APEX-controlled information that are used and retained exclusively within an ACF for less than 120 days—such as preliminary drafts of reports or studies, film clips included in analysts' reference files, copies of incoming and outgoing electrical messages, and waste materials such as carbon sheets, carbon ribbons, reproduction plates, stencils, composition tapes, masters, stenographic notes, and worksheets—do not require an APEX dissemination record but must be safeguarded in accordance with the storage requirements for APEX-controlled materials.

XIV. Procedures for Control and Marking Of Specialized Hard-Copy Documents

a. Automatic Data Processing

All automatic processing of APEX-controlled information and material will be conducted in accordance with DCID 1/16, (Security of Foreign Intelligence in Automated Data-Processing Systems and Networks). (See appendix C.) To facilitate identification, accounting, and control of APEX-controlled data in magnetic form, each reel or cassette of tape and each magnetic card or disk pack that contains APEX-controlled data will be prominently labeled with security classifications, APEX Security Control System markings, and other required APEX caveat designators.

b. Film/Photographic Materials

Roll film, slides, or other forms of photographic negatives or positives must be labeled as to security classification and controlled under APEX control procedures.

Labels on roll film placed in metal containers will be located as follows:

1. One on end of spool flange.
2. One on side of spool container.
3. One on container cover.

Film in transparent containers needs only one label placed visibly on the spool flange. This procedure is intended to facilitate reuse of the containers.

The film itself will include all required APEX markings on the heading and tail identification.

c. Microfiche

Each microfiche will have a heading whose elements are readable without magnification. The heading elements will specify: the long and short titles of the document; security classification and codewords, which will not be abbreviated; and standard abbreviations or codes for handling caveats, dissemination control markings, and distribution restrictions. Individual microfiche are to be placed in separate envelopes that are color-coded to reflect the categories of APEX information contained within them.

d. Microfilm

Each roll of microfilm, whether mounted on an open reel or in a cartridge, will contain security information which is readable without magnification. For microfilm of an individual document, the information will be on a page target and contain the security classification and codewords, which will not be abbreviated, as well as standard abbreviations and codes for handling caveats, dissemination control markings, and distribution restrictions. This page target will immediately precede the first page of the document and will follow the last page of text preceding the "END - date filmed" target frame. For film produced by a Computer Output Microfilm (COM) recorder, the above-mentioned security information will be recorded in human-readable format, when feasible, on one length of film immediately preceding and on another immediately following the document text. The boxes containing processed film on open reels and the film cartridges will be labeled with the appropriate security information. In addition, the labeling will include the document's long and short titles. Microfilms containing documents with individual titles and APEX numbers too numerous to be included on the label may be identified by a generalized composite title and a new APEX number.

XV. Contractor/Consultant Access

a. General Guidelines

Contractors and consultants of Intelligence Community departments and agencies may be provided access to APEX information as required on a strict need-to-know basis under provisions of this manual, the APEX Industrial Security Manual, and DCID 1/7. Particular attention should be paid to the release, control, destruction, and return of APEX materials.

A contractor's or consultant's past record in properly safeguarding classified material will be taken into account when making decisions on selection of contractors or consultants.

When an APEX facility is established and accredited in industry, the ASO of the government component responsible for its security will closely monitor its activities to ensure that APEX procedures are followed completely and that APEX materials are properly segregated from any other classified or unclassified materials of the contractor.

b. Restrictions on Access

Contractor companies that are under foreign ownership, control, or influence will generally be ineligible for access to APEX activities and information. However, if that ownership, control, or influence does not involve a Communist-controlled country and the foreign interests own less than 5 percent of the contractor's voting stock and such minority holdings do not enable the foreign interest to control the appointment and tenure of the contractor's APEX-approved managing officials, a waiver of this provision may be granted by the DCI or SIOs of the Intelligence Community. Prior to the granting of a waiver, provision must be made for security safeguards to prevent disclosure of APEX-controlled information to any non-US owners and managing officials. Should foreign ownership increase beyond 5 percent during the course of a contract, the DCI or the appropriate SIO will review the contractor's eligibility for continued access.

XVI. Congressional Access

The Legislative Branch requires foreign intelligence information to carry out its responsibilities. As an underlying principle, access will be consistent with the protection of intelligence sources and methods. Normally, Congressional requirements for intelligence information can be satisfied at the collateral, noncodeword level, but there will sometimes be a need for access to APEX information. Where possible, sanitization of such information will be accomplished to eliminate the identification of intelligence sources and methods. Where APEX material must be furnished in unaltered form, the following guidelines will apply:

1. Members of Congress, by virtue of their elected positions, are eligible for access to APEX material without a formally established clearance.

2. Clearances for access to APEX information will ordinarily be limited to other persons within the Legislative Branch as follows:

(a) Staff personnel of Congressional committees and subcommittees.

(b) Employees of the General Accounting Office and the Library of Congress.

(c) Selected members of the staffs of the Leadership of the House and Senate as jointly agreed to by the DCI and the Leadership.

3. Requests for APEX clearances for persons other than those specified above will be referred to the Legislative Counsel of the DCI for approval.

Why not a C ?

4. The DCI Legislative Counsel will certify, on behalf of the DCI, the need of persons in the Legislative Branch other than elected officials for a clearance permitting access to APEX material. Such certification will be based on such persons' job responsibilities in the following areas:

(a) Direct involvement in authorization legislation pertaining to Intelligence Community agencies.

(b) Direct involvement in appropriations legislation for Intelligence Community agencies.

(c) Direct involvement in reviews authorized by law of activities of Intelligence Community agencies.

(d) Direct involvement in oversight responsibilities carried out by the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence.

(e) Direct involvement on other legislative matters which of necessity require direct access to compartmented intelligence.

5. A clearance for access to APEX material will ordinarily be granted to nonelected persons in the Legislative Branch who possess a TOP SECRET collateral clearance based on the investigative standards set forth in this manual. Requests for exceptions to this policy should ordinarily be referred to the DCI Legislative Counsel for resolution. ?

6. APEX information will ordinarily be made available to committee and subcommittee members only through the chairman of the Congressional committee or subcommittee concerned.

7. Any agency of the Intelligence Community that provides APEX materials to Congress will take appropriate measures to ensure that the handling and storage of such information conforms as closely as possible to the requirements set forth in this manual. Where adequate provisions cannot be made for the handling and storage of such information, no such information will be provided without the approval of the DCI.

8. Any agency of the Intelligence Community that provides testimony or briefings to persons in the Legislative Branch that involves APEX information will attempt to ensure that such testimony or briefings are provided in accordance with the following security measures:

(a) A thorough physical security and audio countermeasures inspection of the room where testimony or briefing will occur should be conducted immediately

before the presentation unless the premises are maintained in a secure status. Audio countermeasures surveillance of the premises should also be maintained during the presentation.

(b) All persons present, other than elected officials, including transcribers and other clerical personnel, should be certified for access to APEX materials. Arrangements should be made to monitor entrances to the room where the presentation will be given to exclude unauthorized persons.

(c) All transcriptions or notes that result from briefings or testimony should be handled and stored in accordance with the requirements set forth in this manual.

(d) The room in which the presentation occurred should be inspected after the presentation to ensure that all APEX material is properly secured.

Where, in the opinion of the agency concerned, adequate provision cannot be made for the security of APEX information, no such information will be provided without the approval of the DCI.

9. Any agency of the Intelligence Community which provides APEX information to a Congressional committee, other than a committee routinely involved in the oversight and appropriations processes of Intelligence Community agencies, should endeavor to provide such information through the appropriate oversight committee. Where possible, custody of such material should remain with the Intelligence Community agency concerned. Where such material must be physically transferred, efforts should be made beforehand, where feasible, to have APEX information screened by the appropriate Congressional oversight committee to eliminate or minimize the exposure of sensitive sources and methods.

XVII. Security Violations/Compromises

a. Responsibility To Report

Persons approved and briefed for APEX access are responsible for reporting any possible security violations or compromises of APEX information to their APEX Security Officer. Such reporting must be done immediately to keep damage to an absolute minimum.

b. Investigative Responsibility

ASOs are responsible for the investigation of all possible security violations and compromises of APEX materials within their jurisdiction. Investigations will attempt to develop full details of the violation or compromise and to determine

whether and how much information was exposed, the damage that resulted, and whether culpability was apparent in allowing the violation or compromise to occur. Administrative sanctions will be assessed in accordance with regulations. These sanctions will be recorded in security files of the Intelligence Community departments and agencies involved. Investigative reports concerning flagrant violations and compromises will be reported to the DCI.

If inadvertent disclosure has been made, the ASO will exercise his best judgment about whether to seek an inadvertent-disclosure statement. The matter will be reported in writing to the DCI Security Committee if inadvertent disclosure has been made to a foreigner.

If personnel to whom inadvertent disclosures have been made can reasonably be expected to maintain absolute secrecy over the APEX material to which they have been exposed and execute an inadvertent-exposure agreement, the ASO may make a finding that no compromise has occurred.

c. Corrective Action

In the course of investigating security violations and compromises, it may become clear that there are weaknesses in operating procedures in the affected components. It is the responsibility of each ASO, when identifying such basic flaws, to initiate corrective action. The corrective action recommended will be incorporated in the investigative report.

d. Central Repository

To maintain a complete record of APEX information known or believed to be compromised, a central repository for the recording of APEX Compromise Reports has been established in the APEX control organization.

XVIII. Security Education

a. General

Security education is a continuing process, which must be initiated at the time of indoctrination, periodically reinforced, and emphasized at the time of termination of access. ASOs as well as all indoctrinated personnel must continually maintain and increase security awareness through day-to-day vigilance and reinforcement of basic security principles.

b. Initial Indoctrination

Personnel are to be indoctrinated by an ASO. The indoctrination will cover:

1. The need for, purpose of, and structure of the APEX Security Control System and the adverse effects on the national security that could result from unauthorized disclosure of APEX information.

2. An explanation of the sensitivity of APEX information and its relationship to other intelligence information processed by the US Government.

3. The administrative, physical, and other procedural security requirements of the APEX Security Control System.

4. Individual classification management responsibilities of personnel in the APEX system, including classification/declassification, decompartmentation, and sanitization guidelines and marking requirements.

5. The criminal penalties for espionage and unauthorized disclosure.

6. The sanctions for violation or disregard of APEX security procedures.

7. The techniques employed by foreign intelligence organizations in attempting to obtain national security information.

8. The security responsibilities of the individual, who must be made aware of:

(a) The prohibition against disclosing any classified information over nonsecure telephones or in nonsecure places.

(b) The procedures to determine that prospective recipients are approved for access.

(c) Administrative reporting requirements involving such things as nonofficial foreign travel, contacts with foreign nationals, attempts by unauthorized persons to obtain APEX information, possible loss or compromise of APEX material, physical security deficiencies, and personnel security concerns that would probably have an adverse effect on APEX security.

9. Execution of a Nondisclosure Secrecy Agreement.

c. Periodic Re-indoctrination

At intervals of no less than two years, all APEX-indoctrinated personnel are to receive a formal reindoctrination. This reindoctrination should cover all the points enumerated in paragraph b, above. Such reindoctrinations should reinforce the individual's understanding of his/her responsibilities. This opportunity should be used, moreover, to encourage suggestions for better security within the system.

d. Termination of Access

When an individual no longer requires access to any type of APEX information, he/she should be debriefed and provided with final instructions and guidelines on the protection of APEX information and his/her personal responsibilities. This debriefing will include:

1. A reminder of the appropriate sections of Titles 18 and 50 of the US Code, their provisions, and criminal sanctions relative to espionage and unauthorized disclosures.

2. The continuing obligation never to divulge, publish, or otherwise reveal to any unauthorized person any APEX information without express permission of the appropriate responsible officials.

3. An acknowledgment of individual responsibility to report to appropriate US Government officials any attempt by an unauthorized person to solicit APEX information.

4. A declaration that the individual no longer has any APEX materials in his/her possession.

5. A reminder of the risks associated with hazardous activities, as defined in chapter VIII, and the need for a defensive security briefing.

6. Execution of a Termination Secrecy Agreement.

Confidential

Confidential