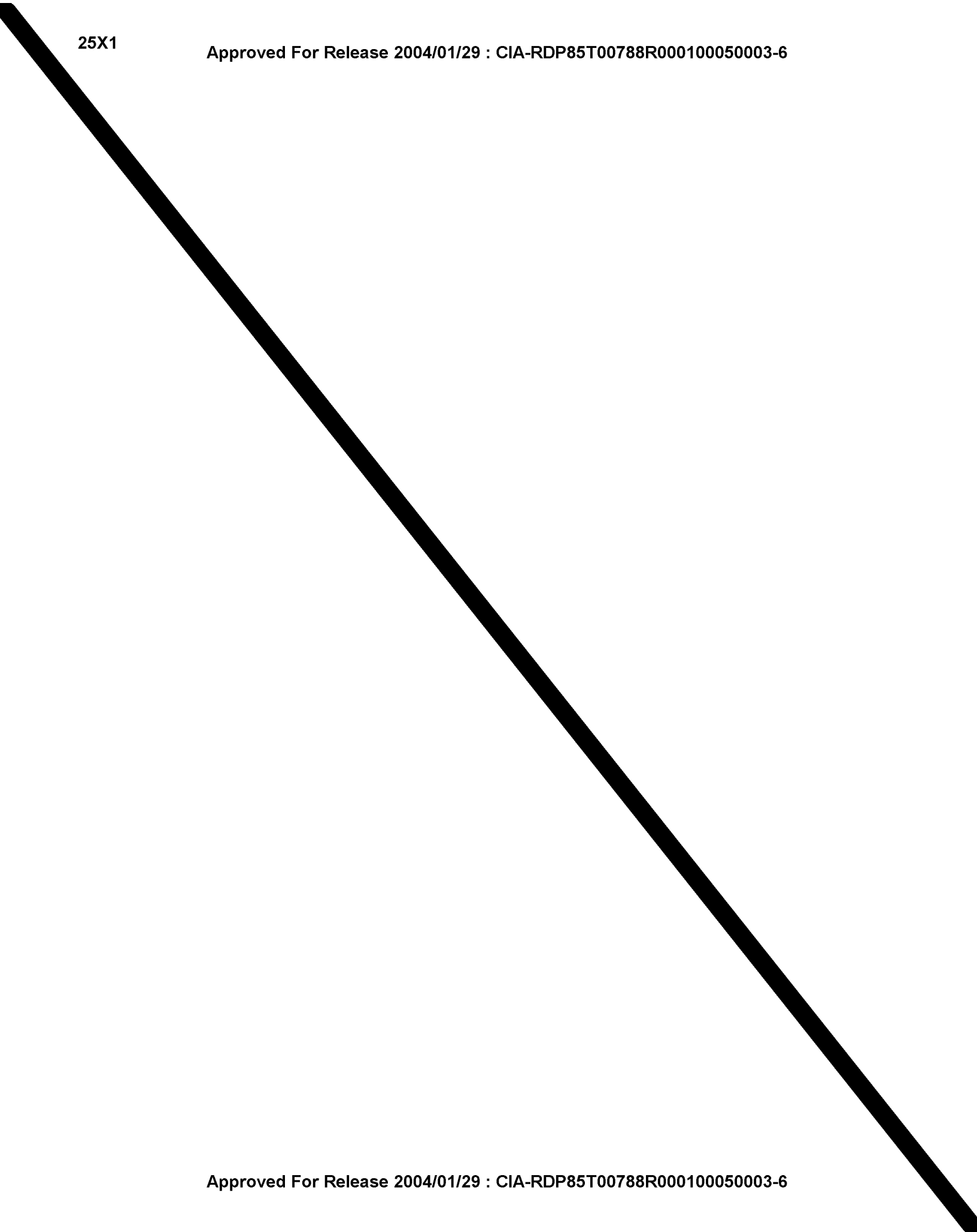
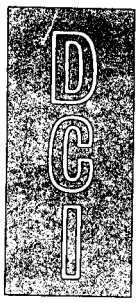


Approved For Release 2004/01/29 : CIA-RDP85T00788R000100050003-6

Confidential



DIRECTOR
OF
CENTRAL
INTELLIGENCE

DRAFT

A Security Manual for Industry

The APEX Special Access Control System

Confidential

May 1979

Copy
113

National Security Information

Unauthorized Disclosure
Subject to Criminal Sanctions

Contents

	Page
I. Introduction	1
II. Organizational Structure	1
III. Description of System	2
a. General	2
b. Access to APEX Security Control System	2
c. Revalidation of Access	3
d. Termination of Access	3
e. Termination Secrecy Agreements	3
f. Access Approvals	3
IV. Responsibilities of Contractor APEX Control and Security Officers	4
a. Duties of Contractor APEX Control Officers	4
b. Duties of Contractor APEX Security Officers	4
V. Security Standards for Access Approval	5
a. Need-to-Know Policy	5
b. Personnel Security Standards	5
c. Investigative Requirements	6
d. Reinvestigations	9
e. Changes in Personal Status	9
f. Contacts or Associations With and Marriages to Foreign Nationals	10
g. Travel Restrictions	10
VI. Factors Governing Contractor Access	12
a. General Guidelines	12
b. Factors Considered in Selection of Contractor Firms	12
c. Restrictions on Access	12
d. Types of Access	12
VII. Physical Security	14
a. Construction and Protection Standards	14
b. Accreditation of CACFs	14
c. Inspections	15
d. Colocation Within Facilities	15
e. Emergency Destruction and Evacuation Planning	15
f. Personnel Access Controls	15
g. Two-Person Rule	15

VIII. Technical Security	16
a. Technical Security Countermeasures Inspections	16
b. Computer Security	16
c. Compromising Emanations Control (TEMPEST Security)	16
IX. Access Approval Certifications	16
a. General Guidelines	16
b. Visits to/by Contractors	16
c. Central Assess Approval Registry	17
d. Information Updates	17
X. Security Classification and Control Guidelines	17
a. Basic Guidance	17
b. Decompartmentation/Sanitization	17
c. Challenges to Classification Levels and Control Restrictions	17
XI. Control Standards and Procedures	18
a. Classification Levels	18
b. Classification Guides	18
c. Labeling	18
d. Pouching and Transmittal Requirements	19
e. Electrical Transmission	20
f. Cover Sheets	20
g. Destruction	21
h. Reproduction	21
i. Accountability	21
XII. Procedures for Control of Specialized Hard-Copy Documents	22
a. Automatic Data Processing	22
b. Film/Photographic Materials	22
c. Microfiche	22
d. Microfilm	22
XIII. Security Violations/Compromises	23
a. Responsibility	23
b. Investigative Responsibility	23
c. Corrective Action	24

XIV. Security Education		24
	a. General	24
	b. Initial Indoctrination	24
	c. Periodic Reindoctrination	25
	d. Termination of Access	25
Glossary of Terms		

Appendixes

A.	DCI List of Communist-Controlled Countries
B.	USIB Policy Statement Establishing Physical Security Standards for Sensitive Compartmented Information Facilities, 30 April 1973

The APEX Special Access Control System

I. Introduction

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

This manual will serve as the authoritative guide for the security and control of APEX material. Existing directives and regulations governing the protection and control of Sensitive Compartmented Information (SCI) will be superseded or revised, if necessary, to be in accordance with this manual. The manual is not, however, intended to intrude on the activity of Senior Intelligence Officers (SIOs) of the Intelligence Community, who will continue to prescribe basic direction and classification guidance.

Certain terms used in this system are unclassified when standing alone or not connected to the intelligence activities or intelligence information they designate. The terms are: APEX; the APEX Security Control System; the codewords which identify the categories of intelligence product within the sytem (that is, COMINT, HUMINT, IMAGERY, and TECHNICAL); and the especially sensitive material designators in the [redacted] 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. The nature of individual contracts, however, may require that the connection of a contractor to APEX activity be treated as classified by virtue of the association. 25X

II. Organizational Structure

Senior Intelligence Officers of the Intelligence Community, government contracting officers, and industrial contractors authorized access to APEX materials are responsible for enforcing the policy and implementing the procedures outlined in this manual.

To fulfill their responsibilities, government officials may provide, as necessary, additional implementing guidance to contractors under their cognizance as long as such guidance does not conflict with the provisions of this manual.

Although the government and industrial officials specified above must have the overall responsibility for policy compliance and implementation of pertinent procedures, adherence to the security and control 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, the cognizant government security official will appoint or cause to be appointed Contractor APEX Control Officers (CACOs) and Contractor APEX Security Officers (CASOs), with alternates, to administer the system within contracting firms. CACOs and CASOs shall be appointed within each firm at whatever levels may be appropriate. Their responsibility is to actively administer the APEX system within their firms and to ensure full compliance with the provisions of this manual and any subsequent supplemental APEX directives that may be issued.

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

SIOs are responsible for the establishment of Contractor APEX Control Facilities (CACFs) within industry for the control, storage, and use of APEX materials. These facilities will be consolidated or decentralized within industrial firms, depending on joint security-management concerns.

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 product information and by project codewords which refer to collection activities.

III. Description of System

a. General

The APEX apparatus provides a single system for controlling access to, and distribution and protection of, selected intelligence information and collection programs requiring extra security measures. Within this unified system there are distinct means of controlling access to operational data, as well as access to generic sources of intelligence information and to finished product, by the establishment of disciplined, balanced threshold criteria that allow only sensitive data to be placed inside compartmented access control.

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 by the SIO 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. If additional access approvals are required, the processing steps enumerated above will be repeated. Upon indoctrination for any access to APEX material, the completed indoctrination agreement will be forwarded to the SIO.

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 need-to-know requirements. Those accesses no longer required will be formally terminated.

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. The responsible SIO will be notified of all terminations of access.

Personnel may, within need-to-know requirements, be authorized by responsible SIOs to retain access approvals when they transfer internally within their industrial firms. However, when an individual leaves one firm to join another, all his/her approvals will automatically be canceled until a need-to-know is established by the responsible SIO. Following approval by an SIO, those accesses deemed necessary for the completion of assigned duties with the new employer will be granted or reinstated and a new secrecy agreement will be signed.

e. Termination Secrecy Agreement

At the time access is no longer required, the individuals concerned will be required to account for and surrender all APEX documents under their cognizance and control, and to execute a Termination Secrecy Agreement certifying that they retain no material or documents in the APEX system and are aware of the continuing obligation not to discuss or otherwise reveal APEX-controlled information.

f. Access Approvals

To control access to information within the APEX Security Control System, SIOs will provide only those access approvals required to fulfill the needs of the contract(s).

IV. Responsibilities of Contractor APEX Control and Security Officers

a. Duties of Contractor APEX Control Officers

Contractor APEX Control Officers will:

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

2. Act as the control point within a Contractor APEX Control Facility 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. Provide advice and guidance on the proper classification levels, codewords, and caveats within the APEX Security Control System.

b. Duties of Contractor APEX Security Officers

Contractor APEX Security Officers will:

1. Coordinate and receive prior approval for accreditation and establishment of APEX control facilities.

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

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

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

5. Conduct reindoctrinations on a periodic basis, not to exceed two-year intervals.

6. Ensure periodic security inspections of Contractor APEX Control Facilities under their jurisdiction; submit a report of this inspection, with any recommendations for corrective action, to the accrediting official, and conduct followup action on recommended corrective measures.

7. Ensure investigation 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. These reports will be forwarded as soon as feasible to the responsible SIO.

8. Notify responsible SIOs of all additions and deletions of access approvals within the APEX system on a timely basis.

V. 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. Need-to-know approval rests with the responsible SIO.

b. 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 or 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 responsible SIO or his/her 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 responsible 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.

c. 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 the age of 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 b2(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 on members of the spouse's immediate family to the extent necessary to permit a determination by the adjudicating agency that the provisions in paragraph b, 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.

d. 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 that 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.

e. Changes in Personal Status

The responsible SIO 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 SIO.

f. Contacts or Associations 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 cognizant SIO through the Contractor APEX Security Officers:

1. All nonofficial contacts with citizens or representatives of Communist-controlled countries, no matter how brief or apparently trivial the contacts may be.

2. Close and continuing or any regular, frequent nonofficial 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 cognizant SIO through the Contractor 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 by the cognizant SIO before there is any determination that a waiver of standards might be made to continue the approved person in APEX-indoctrinated status.

g. Travel 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 Contractor APEX Security Officer to risks associated with unofficial visits to, or travel through, certain designated countries (appendix A). The Contractor APEX Security Officer concerned should advise that unofficial travel in those countries without cognizant SIO official approval may result in the withdrawal of approval for continued access to APEX information for persons with specific and extensive knowledge of any of the following

categories of extremely sensitive information on foreign intelligence sources and methods:

(a) Technological structure, function, and technique 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.

All persons having access to APEX information who plan unofficial travel to or through designated countries must:

(a) Give advance notice of such planned travel to the CASO.

(b) Obtain a defensive security briefing from a Contractor 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 upon return from travel, to the cognizant SIO through their Contractor APEX Security Officer, any incidents of potential security concern that occurred during the trip.

2. ***Official Assignment/Travel.*** No contractor 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.

3. ***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.

VI. Factors Governing Contractor Access

a. General Guidelines

Contractors and consultants dealing with participating government agencies or departments will be furnished only that information which is essential to the fulfillment of contractual obligations. This manual will serve as the principal operating directive for the conduct of APEX activities within industry.

b. Factors Considered in Selection of Contractor Firms

The past record of a contractor or consultant in properly safeguarding material will be taken into account when making contractor selections for work on APEX-related activities. In this regard, when an APEX facility is established in industry, the responsible government APEX Security Officer will closely monitor its activities to ensure that APEX procedures are followed completely and that APEX materials are properly segregated from other classified or unclassified materials of the contractor.

c. Restrictions on Access

Contractor companies under foreign ownership, control, or influence will generally be ineligible for access to APEX activities and information. However, a waiver of this provision may be granted, after review by the responsible SIO, if the following conditions apply: the foreign ownership, control, or influence does not involve a Communist-controlled country; 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. Before a waiver is granted, provision must be made to ensure that security safeguards exist 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, a review of the contractor's eligibility for continued access will be made.

d. Types of Access

Within the APEX Security Control System, there are various types of access in industry. These types of access are identified as: APEX-GENERAL; APEX (Operational); APEX-ALPHA (Operational Subcompartment); and APEX (Product).

The Security criteria for indoctrination are the same for all categories in that all must be in accord with the APEX security access standards of this manual and must withstand strict need-to-know tests.

The extent of indoctrination for the various categories is as follows:

APEX-GENERAL. This category is intended for guard, protective, administrative, and other support personnel who need only to know generally that the APEX system exists and must be protected because of national security concerns. The APEX-GENERAL access may be given in two phases:

Phase I accommodates persons who do not need physical access to the substance of APEX materials. These might include external guards, some switching center personnel, computer technicians, communications personnel, and couriers of sealed pouches.

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 might include: some couriers, registry personnel, document control personnel, file clerks, secretaries, internal guards, and some switching center, communications, and computer technicians.

Persons indoctrinated for APEX-GENERAL access will be instructed that their industrial firm has a contract or contracts with US Government entities but may not necessarily be told of the specific departments or agencies. They will not be briefed on details of operational programs. They will be instructed in the rules for protecting classified materials, in its proper storage, transport, and destruction, and in the need for it to be disseminated only to appropriately indoctrinated individuals.

The Phase I and Phase II briefings will be identical, except that those briefed for Phase II will be advised of the specific codeword relating to the particular project in which they and their firm participate.

APEX (Operational Codeword) - Phase I. This level of access is intended for industrial contractors whose personnel need to know about specific operational parameters but have no need to know all aspects of the activity. Included within the Phase I briefing would be the general purpose of the activity, those technical details which are necessary to accomplish that portion of the engineering design, development, fabrication, or installation that is directly within the individual's area of assignment. Reference will not be made to the particular governmental sponsor unless such identity is obvious from the nature of the contract. This category of access should be considered for machinists, engineers not directly involved in total program planning, and others not requiring full knowledge of the activity.

APEX (Operational Codeword) - Phase II. This level of operational access is reserved for those in industry who, by virtue of contractual necessity or other duties, are required to have full knowledge of a particular operational activity. The Phase II level of access will permit knowledge of all data released to the Phase I accessed individuals and will allow detailed knowledge of the activity mission, sponsor, financial arrangements, geographic operational bases, system vulnerabilities, and so forth, as may be necessary. A need-to-know policy still exists despite approval for Phase II access, and it should not be assumed that all details will be given to all Phase II accessed individuals.

APEX (Operational Subcompartment) - ALPHA. In addition to the above-cited phases of access, it is envisiond that under analytical contracts in industry and academic circles, certain facts about operational compartments will be required by industrial intelligence processors/analysts. To provide relevant operational details to such personnel, a separate operational subcategory, designated by the collection project codeword plus the term ALPHA, is to be used. The intent of this subcompartment is to avoid disclosure of full operational details not considered relevant to the contract. Generally this subcompartment will not allow access to financial or funding details, information pertaining to international agreements, details about governmental sponsorship, interagency arrangements, vulnerability data, and such other operational parameters deemed nonreleasable by the operational program manager or his designee.

APEX (Generic Product). The product resulting from operational collection projects will be identified within the APEX Security Control System by its generic term. Access to each of these generic products is not controlled by phases of access. The APEX Product accesses will be reserved for personnel engaged in analytical and research projects that produce finished intelligence and for those engaged in developmental research projects requiring access to intelligence product.

VII. Physical Security

a. Construction and Protection Standards

All materials within the APEX Security Control System must be stored in accredited Contractor APEX Control Facilities. These standards for construction and protection of C[illegible]CFs will be as prescribed in appendix B (Physical Security Standards for Se[illegible]ve Compartmented Information Facilities, dated 30 April 1973) or other such guidelines that may supersede it.

b. Accreditation of CACFs

Before an industrial facility is authorized to handle APEX material, it must be accredited as having met the aforementioned construction and protection standards.

c. Inspections

Periodic inspection of CACFs is mandatory and must be done at least annually. Inspections are to be performed by designated government APEX security representatives experienced in conducting security inspections for the control and storage of APEX materials and will assure that procedures and safeguards comply with standards prescribed by this manual. Reports of inspection will note all irregularities and will be forwarded to accrediting officials for review and necessary corrective action. Inspections will include at least a spot inventory of sensitive documents. Failure to locate any such documents will be reported on a priority basis.

d. Colocation Within Facilities

When it is deemed economically desirable to colocate different APEX activities within a single industrial CACF, a determination must first be made that such sharing will not have an adverse effect on any of the compartmented activities involved. When security considerations permit, a "Memorandum of Agreement To Share Facilities" will be executed between the industrial contractor and the government agencies sponsoring each separate APEX activity. The agreement will delineate the spaces to be used, storage procedures, access limitations, security responsibilities, and any other provisions considered germane to sharing the facility.

e. Emergency Destruction And Evacuation Planning

Each CACF must maintain an emergency plan approved by the responsible government APEX security representative. This plan will normally be part of an overall facility or corporate plan. It will, however, be separately stated for the CACF and will include provisions for the protection of APEX data as well as protection of assigned personnel. Plans shall include provisions for the emergency destruction of APEX materials as well as action to be taken in the event of fire or other natural disaster. Emergency planning should ensure that adequate protection and firefighting equipment is available, especially in vault areas, and that escape and emergency exit plans are provided for and published. Updates of emergency plans will be made annually and training provided to familiarize assigned personnel with the plans.

f. Personnel Access Controls

Positive controls for personnel access must be established over all areas where APEX information is handled. In areas where only small groups of personnel are involved, this control may be by means of personal identification. Where larger numbers are involved, a system of identification badges may be required for assigned personnel and cleared visitors. The industrial contractor will implement whichever procedure is deemed appropriate by the cognizant APEX security representative. Access to CACFs by uncleared visitors must be approved in advance by the cognizant SIO except in those emergency situations where maintenance, fire, or medical personnel may require access. Uncleared visitors will be escorted at all times while in APEX areas.

g. Two-Person Rule

To provide proper security and safety protection to APEX materials, all CACFs 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 the responsible SIO.

VIII. Technical Security*

a. Technical Security Countermeasures Inspections

Technical Security Countermeasures Inspections will be conducted as part of the accreditation process before the opening of a CACF and within six months following major physical renovations. Reinspections are to be conducted every 18 months. Such inspections will be scheduled by the cognizant SIO, who will also ensure that personnel assigned to CACFs are briefed concerning the threat of technical penetration.

b. Computer Security

All automatic data-processing equipment used in CACFs will be operated in compliance with standard requirements provided by the responsible SIO. No APEX or APEX-related information is to be processed before approval by the responsible SIO.

c. Compromising Emanations Control (TEMPEST Security)

Before electronic processing of any APEX or APEX-related information, the equipment to be used, including ADP equipment, must be certified from the standpoint of controlling compromising emanations. Proper RED/BLACK engineering measures must be taken to ensure that any such emanations are contained within boundaries determined to be satisfactory by the cognizant SIO.

When new or modified equipment is brought into service in existing CACFs, TEMPEST approval must be received. It is the responsibility of the responsible government SIO to arrange for all required TEMPEST inspections and instrumented tests and to schedule any required corrective measures.

IX. Access Approval Certifications

a. General Guidelines

The responsible government SIO or contracting representative is the sole authority empowered to certify APEX accesses held by a contractor to other government departments and agencies or to other government contractors or consultants. Such certification will be made only when need-to-know and the necessity of visit requirements have been established.

b. Visits to/by Contractors

APEX-related visits will not be undertaken to/by the contractor without the approval of the cognizant government APEX program contract manager. Normally, certification for a visit will be made on a one-time basis only. In unusual cases, however, when constant contact is required, term certifications for a period

*All requirements for technical security approvals are in addition to physical security approvals required in Section VII.

not exceeding one year may be authorized. Visit certifications are to be made in writing, either by letter or secure communications circuits, as required by circumstances; when time does not permit, such certifications may be made by telephone but should be confirmed subsequently in writing.

c. Central APEX Access Registry

A Central APEX Access Registry has been established, as a service of common concern, to serve as the official central data base for the APEX Security Control System. The names of all indoctrinated personnel within the APEX system will be recorded in this data base.

d. Information Updates

A critical need of the APEX Security Control System is to maintain an accurate record of personnel currently indoctrinated for various compartments of the system. To enable the system to function properly, all contractors must provide timely information on changes in the status of their personnel to the responsible government SIO. These updates will also ensure that all briefing or debriefing actions are recorded as soon as possible.

On a quarterly basis, the Central APEX Access Registry will provide lists of contractor personnel to the SIO who certified their need for access. These lists will be used to certify those access approvals which are still required and to identify those which are no longer needed.

X. Security Classification And Control Guidelines

a. Basic Guidance

Only those government officials specifically authorized under EO 12065 may decide security classifications. Compartmentation caveats will be used solely to provide need-to-know or access protection where normal management and safeguarding procedures are not, as protective measures, considered sufficient.

b. Decompartmentation/ Sanitization

Contractors are not authorized to decompartment or sanitize APEX materials except as specifically approved by cognizant SIOs. Authority to decompartment or sanitize must be received in writing and must be kept with program records for the duration of the contract. Secure electrically transmitted messages may function as the required written authority.

c. Challenges to Classification Levels and Control Restrictions

Contractors 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 through his CACO. Items which are irreconcilable will be forwarded through APEX control channels for final review and resolution by the cognizant SIO.

XI. Control Standards and Procedures

a. Classification Levels

Information in the APEX Security Control System will be classified according to potential damage to national security if the information is disclosed without authority. Classification levels will be set 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. Classification Guides

Contractors will be furnished classification guides by APEX government program managers or contracting officers to assist in the marking and control of information, hardware, or other items originating in contractor firms. These guides will be made as specific as possible and will be the means by which contractor firms assign classification categories. Responsible SIOs will provide individual guidance as required.

c. 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 dissemination 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 APEX information will bear the same markings.

3. ***Codewords and Indicators.*** Codewords for operational projects and product indicators will be placed following the classification marking 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, which will be provided by the responsible government agencies, will be placed immediately below the classification in the upper right-hand corner of the front cover (if any), title page (if any), and first page of each document. A sequential ("one up") series of six-digit numbers, together with the last two digits of the current year, will be utilized (for example, ACS-123456/79).

5. ***Declassification Review Notice.*** 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 (if any), or first page of typescript text, or inside cover of formal publications:

CLASSIFIED BY: (designated authority)

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

REASON FOR EXTENDED CLASSIFICATION: APEX XI, c.5.

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

6. ***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.

d. Pouching and Transmittal Requirements

APEX material to be transmitted from one CACF to another must be carried by two approved couriers, 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 approval standards of this manual and be specifically designated by the cognizant sponsoring agency. Couriering of APEX material by contractor employees is prohibited except when specifically approved by the responsible SIO.

* Does not apply to ARFCOS.

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, or 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 facility. The notation "TO BE OPENED BY THE CACO" shall be placed above the pouch address of the receiving APEX 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.

e. Electrical Transmissions

APEX material transmitted electrically will be controlled according to procedures prescribed below. Senders must assure that electrical transmissions are made only to authorized recipients, who 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 for this purpose.

Electrical transmission of APEX material will be limited to specifically accredited communications circuits secured by a government-approved cryptographic and/or protected distribution system.

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 words "HANDLE VIA APEX CONTROL SYSTEM ONLY," and such other markings as may be required to note dissemination controls.

f. Cover Sheets

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

g. 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. However, only those items approved by the cognizant government agency may be destroyed, by only those methods of destruction specifically authorized by the responsible SIO. (These methods may include burning, pulping, pulverizing, melting, or chemical decomposition, depending on the type of materials to be destroyed.) All destruction shall be supervised and witnessed by at least two APEX-indoctrinated individuals. Destruction certificates will be completed for all items destroyed. APEX material contained within computer or automated data-processing systems or other magnetic media will be erased by approved degaussing equipment or destroyed by other approved means.

h. 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 from an APEX facility.

Reproduction of all hard-copy APEX materials within the APEX Security Control System requires the consent of the responsible SIO.

i. Accountability

All hard-copy APEX TOP SECRET documents will be inventoried at least annually or when there is a termination of contract, a change of designated CACO, or a change of authorized custodians of such material.

Random inventories will be conducted at least annually for all APEX materials classified SECRET or CONFIDENTIAL according to formulas provided by the responsible SIO.

Should the random inventory of APEX material fail to locate a number of the sampled documents, the CASO will order a complete inventory of all APEX documents received by a CACF.

Reports of discrepancies will be provided to the responsible SIO, who will initiate a search for an investigation of all missing documents.

CACOs will keep a record of all APEX-numbered materials that are received by or dispatched outside their CACFs. This dissemination record will include for each item a brief entry that identifies the nature of the APEX material and the specific organizations—outside or within the CACF—for whom the material is intended. Dissemination records of incoming APEX materials will be retained for as long as the materials are held by the CACF. The dissemination record requirement for dispatched materials may be satisfied by keeping copies of the envelope/package/pouch receipt or other appropriate dissemination record maintained by the dispatching CACF. Such receipts should be retained for a minimum of two years.

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

Contractors will not distribute APEX materials outside a CACF without the permission of the responsible SIO.

XII. Procedures for Control of Specialized Hard-Copy Documents

a. Automatic Data Processing:

All automatic processing of APEX-controlled information and material will be conducted in accordance with instructions provided by the responsible SIO. To facilitate identification, accounting, and control of APEX-controlled data in magnetic form, each reel or casette 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 APEX control system 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. The exact placement of the heading elements will be as prescribed by the cognizant SIO. Individual microfiche are also to be placed in separate envelopes that are color-coded to reflect the level of security protection to be accorded 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 in 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.

XIII. 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 CASO. Such reporting must be done immediately to keep damage to an absolute minimum. The cognizant government ASO is to be notified in a timely fashion of both the incident and the results of the investigation of it.

b. Investigative Responsibility

CASOs and ASOs of cognizant government agencies are jointly responsible for the investigation of all security violations and possible compromises of APEX materials within their jurisdiction. Investigations will attempt to develop full details of the violation or compromise, 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. Sanctions will be prescribed by the responsible SIO. These sanctions will be administered by the ASO and the action taken will be recorded in security files of the contractor and the cognizant government agency.

When it is determined that material has, in fact, been revealed inadvertently to an unauthorized person, the contractor will immediately advise the responsible government ASO of the incident and will secure an inadvertent-exposure agreement, unless otherwise directed.

In all cases of inadvertent exposure a written report will be provided by the CASO to the cognizant government ASO.

If personnel to whom inadvertent exposure has been made can be expected to maintain absolute secrecy of the APEX material to which they have been exposed and execute an inadvertent-exposure agreement, the cognizant government 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 CASO, when identifying such basic deficiencies, to initiate corrective action. The corrective action recommended will be incorporated in the investigative report to the ASO of the cognizant government agency.

XIV. Security Education

a. General

Security education is a continung process, which must be initiated at the time of indoctrination, periodically reinforced, and emphasized when access is terminated. 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 a designated 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 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) Procedures to determine that prospective recipients are approved for access.

(c) The 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 Reindoctrination

At intervals not to exceed 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 reindoctrination 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 it has been determined that 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 disclosure.

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 V, and the need for a defensive security briefing.

6. Execution of a Termination Secrecy Agreement.

Confidential

Confidential

Approved For Release 2004/01/29 : CIA-RDP85T00788R000100050003-6