ROUTING AND RECORD SHEET

SUBJECT: (Optional)
25X1 APEX Industrial Security Manual

FROM:
25X1

EXTENSION | NO.

DATE: 21 March 1979

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. 25X1 C/PPG/OS 4E70 HDQS	22 MAR 1979	22 Mar		
2.	23 MAR 1979			
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				

21 March 1979

MEMORANDUM FOR: Deputy Director of Security (PSI)
Chief, Security Staff, OD&E
Chief, Security Staff, OL
Chief, Technical Security Division, OS
Chief, Information Review Group, OS
Chief, Special Security Center, OS
Chief, Information Systems Security Group, OS
Associate General Counsel, OL
Chief, Policy and Plans Group, OS
Chief, Communications Security Staff, OC
Chief, Industrial Security Branch, OS

25X1 FROM: [redacted]
CIA Member, Industrial Security
Manual Working Group [redacted] 25X

SUBJECT: APEX Industrial Security Manual [redacted] 25X

1. Attached for your review and comment is a draft industrial security manual prepared by the Community Security Group, DCI Security Committee, which describes the proposed Special Access Program system, known as APEX, and which provides "standard procedures and guidance" to contractors for the control and protection of Sensitive Compartmented Information (SCI). The industrial security manual represents the follow up to an APEX Control System Manual governing the control of SCI within government. [redacted] 25X

2. Addressees will probably note that the attached draft lacks the procedural details spelled out in the recently coordinated "Standard Security Procedures for Contractors" governing Agency collateral classified contracting activities and that in many areas the two manuals lack uniformity. You may want to bear this in mind during your review, and comment
25X1 as you deem appropriate. [redacted]

3. In addition to a substantive review, you are requested to consider whether or not the manual should be 25

[redacted]

classified (and if so, at what level). You will note that for the present time the current draft is classified CONFIDENTIAL. Please explain your rationale in either case. [redacted] X1

4. Please submit your responses to me by the close of business 30 March 1979. All responses will be reviewed, consolidated and presented as the Agency position before the Manual Preparation Working Group. Should you have questions, you can reach me on [redacted] 25X

[redacted] 25X

Attachment

I. INTRODUCTION

This Manual describes the Special Access Program system known as APEX, which is herewith established under authority of the National Security Act of 1947, Executive Order 12036, and Executive Order 12065 to provide standard procedures and guidance to contractors on the control and protection of Sensitive Compartmented Information (SCI) defined as 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 Sensitive Compartmented Information. This Manual is not, however, intended to intrude on the authority of government Program Managers, who will continue to prescribe basic operational direction, classification guidance and policy on dissemination for programs under their cognizance.

The term APEX, APEX Security Control System, its project codewords and product categories are all unclassified when standing alone or not connected to their intelligence activities or intelligence information. However, by nature of individual contracts, the connection of a contractor to APEX activity may require that such connection be treated as "association classified".

II. ORGANIZATIONAL STRUCTURE

Senior Intelligence Officers (SIO's) of the U.S. Government Departments and Agencies represented on the National Foreign Intelligence Board (NFIB), Directors of designated sensitive collection programs, Government Contracting Officers and industrial contractors engaged in Special Access Programs are responsible for enforcing the policy and implementing the procedures outlined in this Manual.

To fulfill their responsibilities government officials may provide additional implementing guidance to contractors under their cognizance as necessary, as long as such guidance is in consonance with this Manual.

Although the above-named government and industrial officia 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 designated responsible officials will appoint or cause to be appointed APEX Control Officers (ACO's), and APEX Security Officers (ASO's), with alternates, to administer the system within contracting firms. ACO's and ASO's 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 as may be issued.

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.

SIO's and Program Managers/Directors are responsible for the establishment of APEX Control Facilities (ACF's) within industry for the control, storage and use of APEX materials. These facilities will be centralized 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 or product information and by project words which refer to collection activities.

III. DESCRIPTION OF SYSTEM

a. General: The APEX Security Control System provides a single system for controlling access to selected intelligence information and programs requiring extra amounts of protection. Within this unified system there are distinct means of controlling access to operational data, as well as access to the product of generic sources of intelligence information and finished product by the establishment of disciplibalanced threshold criteria that allow only sensitive data to be placed inside compartmented access control.

b. Access to APEX Security Control System: Three steps are necessary for access to the APEX Security Control System:

1. Certification by the SIO, or Government Project Manager or contracting officer of need to know ~~to~~ specific aspects of the APEX Security Control System (operational projects, operational subcompartments, generic products).

In the case of access to operational projects, nominees need-to-know will be jointly certified by the SIO and the individual Agency's Program Manager/Director.

CONFIDENTIAL

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 Non-Disclosure Agreement as a condition of access to APEX material.

The security indoctrination will provide the individual with sufficient specific information so that he will know what he is to protect, his responsibilities in doing so, and general information about the APEX Security Control System so that he will know how the system is to be used in carrying out this responsibility. If additional access approvals are required the processing steps enumerated above will be repeated.

Upon indoctrination for any access to APEX material, the individual's name and all approvals held will be recorded in the Central Access Approval Registry.

c. Revalidation of Access: In January of each year, SIO's and Program Managers/Directors in both Government and industry, will review all extant approvals under their cognizance and revalidate all required accesses. Those no longer required will be formally terminated.

In addition to this formal, annual review program, it is the responsibility of each of the above responsible offic to maintain a continuous review of access approvals to ensure that only those personnel with documented "need-to-know" have access at any time.

d. Termination of Access: When it has been determined by the appropriate responsible official that individual accesse are no longer required, the individual concerned will be notifi that his/her access to specific types of information is no long justified and that access privileges are being terminated. The cognizant government Agency will be notified of all termination and, in turn, will notify the Central Access Approval Registry.

Personnel may, within need-to-know requirements, be authorized to transfer internally within their industrial firms and retain required access approvals. However, when leaving one firm to join another, all approvals will automatically be cancelled and need-to-know established by the new employer. Following approval by the cognizant Agency, those accesses deemed necessary for the completion of assigned duties with the new employer will be granted or reinstated ~~but~~ and a new secrecy agreement will be required.

e. Termination Secrecy Agreements: At the time access is no longer required, the individual will be required to accoun for and surrender all APEX documents under his cognizance and control, execute a certification that he 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. Access Ceilings: In order to control access to information within the APEX Security Control System, SIO's and Government Program Managers will provide access ceilings for each contract activity involving APEX material.

IV. RESPONSIBILITIES OF APEX CONTROL AND SECURITY OFFICERS

a. Duties of APEX Control Officers:

1. With the appropriately cleared officials, ensure that APEX materials are accounted for, controlled, transmitted, destroyed, packaged and otherwise safeguarded in accordance with provisions of this Manual.

2. Act as the exclusive control point within an 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 valid need-to-know.

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

6. Work closely with the APEX Security Officer to maintain the integrity of the APEX Security Control System.

b. Duties of APEX Security Officers:

1. Coordinate and receive prior approval through appropriate channels, as reflected in VII.b for accreditation and establishment of APEX Control Facilities.

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

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

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

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

6. Conduct annual security inspections of APEX Control Centers under his jurisdiction and submit a copy, with any recommendations for corrective action, to the accrediting official. Conduct follow-up action on recommended corrective measures.

7. Establish security procedures for transmitting and receiving APEX materials.

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

9. Notify cognizant agencies 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 to perform official duties on behalf of the United States Government. Need-to-know will be strictly applied and access will not be given solely by virtue of rank or status within an industrial firm. Need-to-know approval rests with responsible government officials.

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 or her immediate family

shall be U.S. citizens. 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 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 by unconstitutional means.

In exceptional cases, a responsible government official 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 shall be made at once, and should include a personal interview by traine security or counterintelligence personnel. Access in such case shall be strictly controlled, and the fully prescribed investigation and final evaluation shall be completed at the earliest practicable moment.

Exceptions to 2(a)(b) above may be granted only by a government SIO or his designee. All exceptions granted will be common sense determinations based on all available information and shall be recorded by the agency making the exception. In

those cases in which the individual has lived outside of the United States for a substantial period of his 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 shall be designed to develop information as to whether the individual clearly meets the above Personnel Security Standards.

The investigation shall 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, employments and military service. Where the circumstances of a case indicate, the investigation shall 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 shall 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, education and medical records, to provide record information to the investigative agency. Photographs of the individual shall 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 such other National agencies as are appropriate to the individual's background. An additional check of Immigration and Naturalization Service records shall be conducted on those members of the individual's immediate family who are United States citizens other than by birth or who are resident aliens.

3. A check of appropriate police records covering all areas where the individual has resided in the U.S. throughout the most recent fifteen (15) years or since the age of eighteen, 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 most recent five (5) years.

5. Interviews with neighbors in the vicinity of all the individual's residences in excess of six (6) months throughout the most recent five (5) year period. This coverage shall be expanded where the investigation suggests the existence of some questionable behavioral pattern.

6. Confirmation of all employment during the past fifteen (15) years or since age eighteen, whichever is the shorter period but in any event the most recent two years. Personal interviews with supervisors and co-workers at places of employment covering the past ten (10) years shall be accomplished.

7. Verification of attendance at institutes of higher learning in all instances and at the last secondary school attended within the past fifteen (15) years. Attendance at secondary schools may be verified through qualified collateral sources. If attendance at

CONFIDENTIAL

educational institutions occurred within the most recent five (5) years, personal interviews with the faculty members or other persons who were acquainted with the individual during his attendance shall be accomplished.

8. Review of appropriate military records.

9. Interviews with a sufficient number of knowledgeable acquaintances (a minimum of three developed during the course of the investigation) as necessary to provide a continuity to the extent practicabl of the individual's activities and behavioral patterns over the past fifteen years with particular emphasis on the most recent five years.

10. When employment, education or residence has occurred overseas (except for period of less than five (5) years for personnel on US Government assignment and less than ninety days for other purposes) during the past fifteen years or since age eighteen, a check of the records will be made at the Department of State and other appropriate agencies. Efforts shall 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 of the U.S. continuously for over five years, the investigation will be expanded to cover fully this period in his life through the use of such investigative assets and checks of record sources as may be available to the US Government in the foreign country(ies) in which the individual resided.

11. In those instances in which the individual has immediate family members or other persons with whom he is bound by affection or obligation in any of the situations described in subparagraph c2.(b) above, 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 shall, at a minimum, be checked through the subversive files of the Federal Bureau of Investigation and other National agencies as appropriate. When conditions

indicate, additional investigation shall be conducted on the spouse of the individual and members of the immediate family to the extent necessary to permit a determination by the adjudicating agency that the provisions of Personnel Security Standards, above, 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.

Where a previous investigation has been conducted within the past five years which substantially meets the above minimum standards, 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 shall 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. Should new information be developed during the current investigation which bears unfavorably upon the individual's

activities covered by the previous investigation, the curre inquiries shall be expanded as necessary to develop full details of this new information.

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

When all other information developed on an individu is favorable, a minor investigative requirement which has n been met should not preclude favorable adjudication. In al evaluations, the protection of the national interest is para mount. Any doubt concerning personnel having access to APE information shall be resolved in favor of the national secu The ultimate determination of whether the granting of access is clearly consistent with the interests of national securit shall be an overall common sense determination based on all available information.

d. Reinvestigations: Programs shall be instituted requ the periodic reinvestigation of personnel provided access to APEX information. These reinvestigations will be conducted on a normal five year recurrent basis, but on a more frequen basis where the individual has shown some questionable behav pattern, his activities are otherwise suspect, or when deeme necessary by the SIO concerned.

The scope of reinvestigations shall be determined by the SIO concerned 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 continually evaluate factors related to the individual's suitability for continued access. In all cases, the reinvestigation shall include, as a minimum, appropriate National agency checks, local agency checks (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 upon an individual's security status, appropriate investigations shall be conducted on a timely basis. The investigation shall be of sufficient scope necessary 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 is clearly consistent with the interests of the national security.

e. Contacts or Assoociation with Foreign Nationals and Alien Marriages: Close, continuing personal associations with foreign nationals ~~is a matter~~ are of APEX Security concern if they become characterized by ties of kinship, affection or obligation. APEX-cleared 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 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 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, etc., then the contact must be promptly reported. Whenever any doubt exists 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 non-U.S. citizen must report such plans to their APEX Security Officer along with, at a minimum, details about the intended spouse's name, date and place of birth, country of origin and current citizenship, identity of immediate family members, current residence, present occupation and any present or former employment on behalf of any foreign government. Investigation of the prospective spouse will be undertaken prior to a determination being made that a waiver of standards might be made to continue the approved person in cleared status.

f. 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 APEX Security Officer to risks associated with unofficial visits to, or travel through certain designated countries. The APEX Security Officer 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 and extensive knowledge 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) Collection or exploitation system/method capabilities and vulnerabilities.

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.

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

(c) Contact immediately the nearest U.S. 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 their APEX Security Officer any incidents of potential security concern which befell them.

2. 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 operating directive for the conduct of APEX activities within industry.

b. Factors Considered in Selection of Contractor Firms: A contractor or consultant's past record 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 APEX Security Officer 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.

c. Restrictions on Access: Contractor companies which are under foreign ownership, control or influence shall generally be ineligible for access to APEX activities and

information. However, if that ownership, control or influence is not from a Communist-controlled country and the foreign interests own less than five 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 after cognizant Agency review. Prior to the granting of a waiver, provisions must be made to ensure that security safeguards exist to prevent disclosure of APEX-controlled information to any non-U.S. owners and managing officials. Should foreign ownership increase beyond five 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 (Operationa with Phases I, II, and III; and APEX (Product).

The security criteria for indoctrination are the same for all categories in that all must meet investigative requirements of this Manual and must satisfy strict need-to-know tests.

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

APEX GENERAL - This category is intended for guards, protective, administrative and other support personnel who need only to know generally that a system such as APEX exists because their industrial firm has such contracts, and that it involves operational programs which generate product materials. Briefings of APEX GEN approved individual will include reference to US Government contractual control but will not specify interested Departments or Agencies. They will not be briefed on details of operational activity; will not be told the number of operational programs being conducted; will not be given the codeword names. They will be instructed in the rules for protecting APEX material, for its proper storage, transport and destruction, and for its dissemination only to appropriately cleared individuals.

APEX (_____) - Phase I

Operational Codeword

This level of access is intended primarily for industrial contractors personnel who resemble those in the APEX GEN category above (i.e., admin, protective, etc.). The criteria for access is identical with the only exception being that the specific operational program codeword will be divulged to the Phase I approved person. This category is intended for those support type personnel who do not need to know more than that a system such as APEX exists, that it must be protected, that National Security interests are involved and that the particular Project in which they and their firm participate has been given a specific code name which they will be told.

APEX (_____) - Phase II

Operational Codeword

This level of access is intended also for industrial contractors whose personnel need-to-know more about specific operational parameters than Phase I personnel but have no need-to-know all aspects of the Program. Included within

the Phase II briefing would be the general purpose of the Program, those technical details which are necessary to accomplish that portion of the engineering design, development, fabrication or installation which is directly within the individual's area of assignment. Reference will not be made to the particular governmental sponsor unless its 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 program knowledge.

APEX (_____) - Phase III

Operational Codeword

This level of operational access is reserved for those in industry and in government who, by virtue of contractual necessity or official duties, are required to have full knowledge of a particular operational Program. The Phase III level of access will permit knowledge of all data released to the Phase I and II individuals plus it will allow detailed knowledge of the Program mission, sponsor, financial

arrangements, geographic operational bases, system vulnerabilities, etc., as may be necessary. A need-to-know policy still exists despite approval for Phase III access and it should not be assumed that all details will be given to all Phase III accessed individuals.

APEX (_____) - Generic Product

The product resulting from operational 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. Most generally the APEX Product accesses will be reserved for analytic and research projects to produce finished intelligence. There will also be requirements to grant this approval to personnel who must design certain processing equipment in support of intelligence production.

VII. PHYSICAL SECURITY

a. Construction and Protection Standards: All materials within the APEX Security Control System must be stored in accredited APEX areas. Standards for construction and protection of facilities that store or process APEX material or provide discussion/work areas for APEX information shall be as prescribed in the attached Physical Security Standards for Sensitive Compartmented Information Facilities, dated 30 April 1973 or other such guidelines as may subsequently supercede it. (Appendix A)

b. Accreditation of Facilities: Before an industrial facility is authorized to handle APEX material, it must be accredited by the cognizant Government APEX Security Representative as having met the aforementioned construction and protection standards.

c. Inspections: Periodic inspections of approved APEX industrial facilities are mandatory and must be accomplished at least annually. Inspections are to be performed by designated government APEX Security Representatives, who will be persons experienced in conducting security inspections for the control

and storage of Sensitive Compartmented Information 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 also include at least 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 APEX facility, a determination must first be made that such sharing will not have an adverse effect on either of the compartmented activities to be conducted. When security considerations permit, a "Memorandum of Agreement to Share Facilities" will be agreed to in writing by 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 APEX industrial facility must maintain an Emergency Plan which is approved by the cognizant 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 APEX facility 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 sensitive materials as well as action to be taken in the event of fire or other natural disaster. Emergency planning should ensure that adequate protective 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 these 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, possibly beginning with a figure of fifty, 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 Government Security Representative. Access to APEX areas by uncleared visitors must be approved in advance by sponsoring agencies 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 protection to APEX materials, SIO's, Government and Contractor Program Managers will designate sensitive facilities, such as ACF's, as requiring "two man coverage" at all times. Persons selected to work in such areas will be chosen on the basis of proven reliability and maturity.

VIII. TECHNICAL SECURITY

a. Technical Security Countermeasures: Technical Security Countermeasures inspections will be conducted as soon as possible after the opening of an APEX industrial facility and following major physical renovations. Reinspections are to be conducted every 18 months. Such inspections will be scheduled by the cognizant Government APEX Security Representative. The Government APEX Security Representative will also ensure that personnel assigned to APEX facilities are briefed concerning the threat of technical penetration.

b. Computer Security: All Automatic Data Processing equipment used in APEX industrial facilities will be operated in compliance with standard requirements provided by the cognizant Government APEX Security Representative. No APEX or APEX-related information is to be processed prior to approval by the Government Security Representative.

c. Emanations Control (TEMPEST Security): Prior to electrical processing of any APEX or APEX-related information, equipment to be used must be certified as satisfactory from

an emanations control standpoint and that proper RED/BLACK engineering measures have been taken to ensure that any compromising emanations are contained within areas determined to be satisfactory.

When new or modified equipments are brought into service in existing APEX areas, TEMPEST approval must be received. It is the responsibility of the cognizant Government APEX Security Representatives to arrange for all required TEMPEST inspections and schedule any required corrective measures.

NOTE: All requirements for technical security approvals are in addition to physical security approvals required in Section VIII.

IX. ACCESS APPROVAL CERTIFICATIONS

a. General Guidelines: The cognizant Government APEX contracting or security 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. Normally, certifications will be made on a one-time visit basis only. However, in unusual cases, when constant contact is required, term certifications for a period not exceeding one year may be authorized. Visit certifications are to be made in writing, either by letter or secure communication circuits, as required by circumstances; when time does not permit, such certifications may be made by telephone but should be confirmed subsequently in writing.

b. Visits by Contractors: No visits will be undertaken by the contractor without the approval of the cognizant Government APEX program contract manager.

c. Central Access Approval Registry: To record and serve as the official central data base for the APEX Security Control System, a Central Access Approval Registry is established

as a service of common concern. All approvals within the APEX System will be on record in this data base.

d. Information Updates: A critical feature of the APEX Security Control System is its ability to accurately reflect personnel currently cleared for various compartments of the system. To function properly, all contractors must provide timely information on changes in the status of their personnel. These updates will be provided to ensure that all briefing or debriefing actions are recorded as soon as possible.

The Central Access Approval Registry will provide, on a quarterly basis, lists of personnel approved on behalf of individual contractors. It is expected that, with provision of these lists, review will be made of active approvals and that those no longer needing access will be cancelled and reported through cognizant agencies to the Central Registry. This is a continuing requirement assigned to each ACO irrespective of the formal annual review by Program Managers 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. Verification, through Program Managers,

CONFIDENTIAL

will be effected, as necessary, prior to adding personnel or approvals for already approved personnel to the Central Registry.

X. SECURITY CLASSIFICATION AND CONTROL GUIDELINES

a. Basic Guidance: Security classification and document control are a function of Management. Classification of information, therefore, will be accomplished only by individuals specifically authorized under E.O. 12065. This authority extends to contractors through Government contracting officers. Use of compartmentation caveats 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. Using compartmentation as a means of restricting access to sensitive data should be viewed as a meaningful exercise and not one which occurs by force of habit.

b. Decompartmentation/Sanitization: Contractors are not authorized to decompartment or sanitize any materials (documents, film, hardware, tape, et al) except as specifically approved by cognizant agencies. 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: 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 shall be forwarded through APEX control channels for final review and resolution.

XI. CONTROL STANDARDS AND PROCEDURES

a. Classification Levels: Documents in the APEX Security Control System will be classified according to damage accruing to National Security if disclosed without authority. Classification levels will be ascribed in accordance with E.O. 12065, reserving CONFIDENTIAL for "identifiable damage", SECRET for "serious damage", and TOP SECRET for "exceptionally grave damage". No other classification levels are authorized and none are to be adopted within the APEX Security Control System.

b. Classification Guides: Contractors will be furnished Classification Guides by Government Program Managers or contracting officers to assist in the classification of documents, hardware or other items originating in Contractor firms. These guides will be made as specific as possible and will be used as the means by which contractor firms assign classification categories. Cognizant Government agencies will provide individual guidance as required for situations not covered in the basic guides.

c. Labelling: The following labelling 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, shall 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 shall be conspicuously marked or stamped at the top and bottom with the highest classification of the document. The determination of national security classification shall be on the basis of the policies indicated in Executive Order 12065 on National Security Information. Portions of documents, to include paragraphs, subparagraphs, and titles shall be marked to reflect the level of classification and dissemination control markings or that the particular portion is unclassified.

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 which contains APEX information will also 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, first page and each page which contains information requiring specific codeword/indicator protection.

4. Control Numbering: APEX document control numbers,which will be provided by cognizant government agencies, will be placed immediately above the Control System Caveat on the front cover, title page and first page of each document. A "one up" six digit numbering system, to include year of creation, will be utilized (e.g., A-123456/79).

5. Declassification Review Notice: Having satisfied threshold criteria demanding protection under the APEX Security Control System due to sensitivity of the source, method or the information itself, APEX materials are classified for a period of 20 years excepting Foreign Government

Information which will remain protected for 30 years. The following Declassification Review Notice will be used on the cover, title page, or first page of typescript text, or inside of formal publications:

Classified By: (appropriate authority)

Review for Declassification On: (Indicate date, 20 or 30 years from date of issuance)

Reason for Extended Classification: APEX.XII.B.6

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

6. 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 to contractors.

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

CONFIDENTIAL

c. Pouching and Transmittal Requirements: APEX material to be transmitted from one facility 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 shall 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-U.S. Government operated or chartered aircraft is prohibited.* The cognizant SIO must specifically approve all exceptions.

APEX couriers shall be active duty military or U.S. Government civilian employees meeting investigative standards of this Manual and be specifically designated by the cognizant sponsoring agency. Couriering of APEX by contractor employees is prohibited except when specifically approved by a responsible government official.

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

*Does not apply to ARFCOS and the Diplomatic Courier Service

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

d. Electrical Transmissions: APEX material transmitted electronically will be controlled according to procedures prescribed below. Senders must assure that electronic transmissio are made only to authorized recipients and receivers must provi procedures for the proper protection of APEX material received in this manner. These procedures shall 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 shall be restricted to means specifically approved and accredited for this purpose.

Electrical transmission of APEX material shall be limited to specifically accredited communications circuits secured by a government approved crypto and protected distribution system.

CONFIDENTIAL

Operational procedures shall ensure that only properly indoctrinated personnel are provided access to clear text APEX materials.

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

The first item in the text of a message shall be the overall classification of the message, applicable codeword(s), Control System Designator, and such other markings as may be required to note dissemination controls.

e. Cover Sheets: To preclude unauthorized disclosure, an unclassified cover sheet shall be used when transmitting APEX materials outside 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 shall 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, and only those methods of destruction specifically authorized by the responsible government program manager shall be used. (These methods may

25X1

[redacted]

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 shall be erased by approved degaussing equipment or destroyed by other approved means.

g. Reproduction: Reproduction of APEX material shall 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 TOP SECRET materials within the APEX System requires consent of originating Agencies. Materials classified SECRET or CONFIDENTIAL may be restricted from reproduction by originating Agencies.

h. Accountability: All APEX TOP SECRET documents will be inventoried at least annually or when there is a termination of contract, a change of designated APEX Control Officers or authorized custodians of such material.

Random inventories will be conducted annually for all APEX materials classified SECRET or CONFIDENTIAL according to formulae provided by the cognizant government Agency ASO.

Should the random inventory of APEX material fail to locate a number of the sampled documents, the contractor ASO will order a complete inventory of all APEX documents received by an APEX Control Facility.

Reports of discrepancies will be provided to the cognizant agency who will initiate a search for and investigation of all missing documents.

APEX Control Facilities shall keep a record of all APEX numbered materials that are received by or dispatched outside the Control Facilities. This dissemination record shall include a brief entry which identifies the nature of the controlled material and the specific organizations - outside or within the Control Facility - for whom the material is intended. Dissemination records of incoming materials shall be retained. The dissemination record requirement for dispatched materials may be satisfied by

keeping copies of the envelop/package/pouch receipt or other appropriate dissemination record maintained by the dispatching Control Facility. Such receipts should be retained for a minimum of two years.

Working materials containing APEX-controlled data, that are used and retained exclusively within an ACF - such as preliminary drafts of reports, 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, work sheets, and similar items - do not require an APEX number or dissemination record but shall be safeguarded and marked as "WORKING PAPERS" in accordance with the storage requirements for APEX-controlled materials.

CONFIDENTIAL

XII. PROCEDURES FOR CONTROL OF OTHER HARD COPY DOCUMENTS

a. Automatic Data Processing: All automatic data processing of APEX controlled information and material will be conducted in accordance with instructions provided by the responsible Government official. To facilitate identification, accounting and control of APEX-controlled data in magnetic form, each reel or cassette of tape, each magnetic card or disk pack which contains APEX-controlled data will be prominently marked with labels indicating security classification, APEX Security Control System markings and other required APEX caveat designators Internal media identification must include a header and trailer block which contains security markings.

b. Film/Photographic Materials: Roll film, slides, or other forms of photographic negatives or positive items must be labelled as to security classification and control under APEX control procedures and document and copy number.

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, and
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.

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 shall not be abbreviated; 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 responsible government official. Microfiche may also be placed in envelopes which, through a specified color code, indicate the level of security protection to be accorded the microfiche.

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 source document microfilm, the information will be on a page target and contain the security classification and codewords, which shall not be abbreviated, 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 within equipment capability on a length of film immediately preceding and 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: Each person approved and briefed for APEX access is responsible for reporting any possible security violations or compromises of APEX information to his/her APEX Security Officer. Such reporting must be done immediately to keep damage to an absolute minimum. An investigation is to be conducted immediately if there is a probability that a compromise has occurred. The cognizant government agency ASO is to be notified both of the incident and investigative results in timely fashion.

b. Investigative Responsibility: Contractor and cognizant government Agency ASO's 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, what damage resulted, and offer conclusions as to whether culpability was apparent in allowing the violation or compromise to occur. Penalties will be assessed as prescribed by the cognizant government Program Managers. These violations will be administered

by the ASO and punitive action taken will be recorded in contractor and cognizant government agency security files.

When it is determined that material has, in fact, been revealed improperly or accidentally to an unauthorized U.S. national, the contractor will immediately advise the cognizant Government ASO of the incident and will secure an agreement of secrecy on the inadvertent exposure.

If the inadvertent exposure has been made to a non-U.S. citizen, the contractor ASO will obtain guidance from the cognizant Government agency ASO whether or not to seek an inadvertent disclosure statement.

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

If personnel to whom inadvertent exposure has been made have been investigated to DCID 1/14 standards, have executed an inadvertent exposure oath and can reasonably be expected to honor their obligation to maintain APEX security, 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 contractor ASO when identifying such basic flaws, to initiate corrective action. The corrective action recommended will be incorporated in the investigative report to the cognizant Government Agency ASO.

XIV. SECURITY EDUCATION

Security education is a continuing program which must be formally provided at the time of initial indoctrination, periodically while in approved status and at the time of termination of access. At all times both ASO's and all indoctrinated personnel must continually maintain and increase security awareness on the part of all approved individuals through day-to-day vigilance and reinforcement of basic security principles.

a. Initial Indoctrination: Upon the granting of initial access, personnel are to be indoctrinated by an ASO. The indoctrination will, at a minimum, include the following:

1. The need for , purpose, 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 United States 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 to include classification/declassification, decompartmentation and sanitization guidelines and marking requirements.

5. The criminal penalties for espionage and unauthorized disclosure in the appropriate sections of Titles 18 (e.g., Sections 792-798) and 50, U.S. Code, relative to APEX information.

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

7. A review of the techniques employed by foreign intelligence organizations in attempting to obtain national security information.

8. A review of individual security responsibilities to include, at a minimum,

(a) the prohibition against disclosing any classified information over either non-secure telephones or in non-secure places,

(b) the need and method to determine that prospective recipients are approved for access, truly need information to perform their official duties and can provide proper protection to the information in question,

(c) administrative reporting requirements such as non-official foreign travel, contacts with foreign nationals, attempts by unauthorized persons to obtain APEX information, possible loss or compromise of APEX material, physical security deficiencies or probable personnel security concerns which would impact adversely on APEX security.

b. Periodic Reindoctrination: 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 a. In addition, as personnel grow in understanding of the APEX Security Control System by being exposed to it, should develop ~~themes~~ THEMES on a more sophisticated level appropriate to the specific types of APEX activity involved (e.g., vulnerability of operational activities to countermeasures, need to protect identity of human sources for purposes of their individual safety, etc.). Such reindoctrinations should reinforce responsibilities of the individual and this opportunity should be used to encourage suggestions for better security within the system.

c. Termination of Access: When it has been determined that individuals no longer require access to any type of APEX information, they should be scheduled for a debriefing and provided with final instructions and guidelines on the protection of APEX information and their personal responsibilities. At a minimum, this debriefing will include:

1. A reminder of the appropriate sections of Titles 18 and 50 of the U.S. 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 acknowledgement of individual responsibility to report to appropriate U.S. 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 review of travel restrictions and reporting requirements, if required.

At the time of debriefing, the person terminating should again be encouraged to provide any comments pertinent to enhanced APEX security.